SPECTEROPS

Security Boundaries within an Active Directory Forest

Jonas Bülow Knudsen

SpecterOps

Rasta Mouse @_RastaMouse · Jan 27

Trick question, there are no security boundaries 🤪

> **SpecterOps** @SpecterOps · Jan 27
>
> Where are the security boundaries in a multi-domain forest? 🤔
>
> Join @Jonas_B_K at #SOCON2025 as he uncovers the boundaries within an Active Directory forest and explores the attack techniques that can compromise them....
> Show more

Microsoft: AD forest is a security boundary

Forests as Security Boundaries

Each forest is a single instance of the directory, the top-level Active Directory container, and a security boundary for all objects that are located in the forest. This security boundary defines the scope of authority of the administrators. In general, a security boundary is defined by the top-level container for which no administrator external to the container can take control away from administrators within the container. As shown in the following figure, no administrators from outside a forest can control access to information inside the forest unless first given permission to do so by the administrators within the forest.

A forest is the only component of the Active Directory logical structure that is a security boundary. By contrast, a domain is not a security boundary because it is not possible for administrators from one domain to prevent a malicious administrator from another domain within the forest from accessing data in their domain. A domain is, however, the administrative boundary for managing objects, such as users, groups, and computers. In addition, each domain has its own individual security policies and trust relationships with other domains.

.. and the domain is not

https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759073(v=ws.10)#forests-as-security-boundaries

Security Boundaries within an Active Directory Forest

None

(credit: RastaMouse)

No boundaries would mean ..

... AD is not designed to prevent arbitrary users from having full control of everything in the forest

That would be absurd..

So where are the boundaries?

Outline

AD domains and forests 101

Where are the boundaries then?

How security boundaries are violated

Audit for security boundary violations in BloodHound

Whoami

```
PS C:\> Get-ADUser jbk -Properties * | Select Name,Title,Company,City,co


Name    : Jonas Bülow Kundsen
Title   : Manager, Research
Company : SpecterOps
City    : Copenhagen
co      : Denmark
```

@jonas-bk.bsky.social

@Jonas-BK

@JonasBK

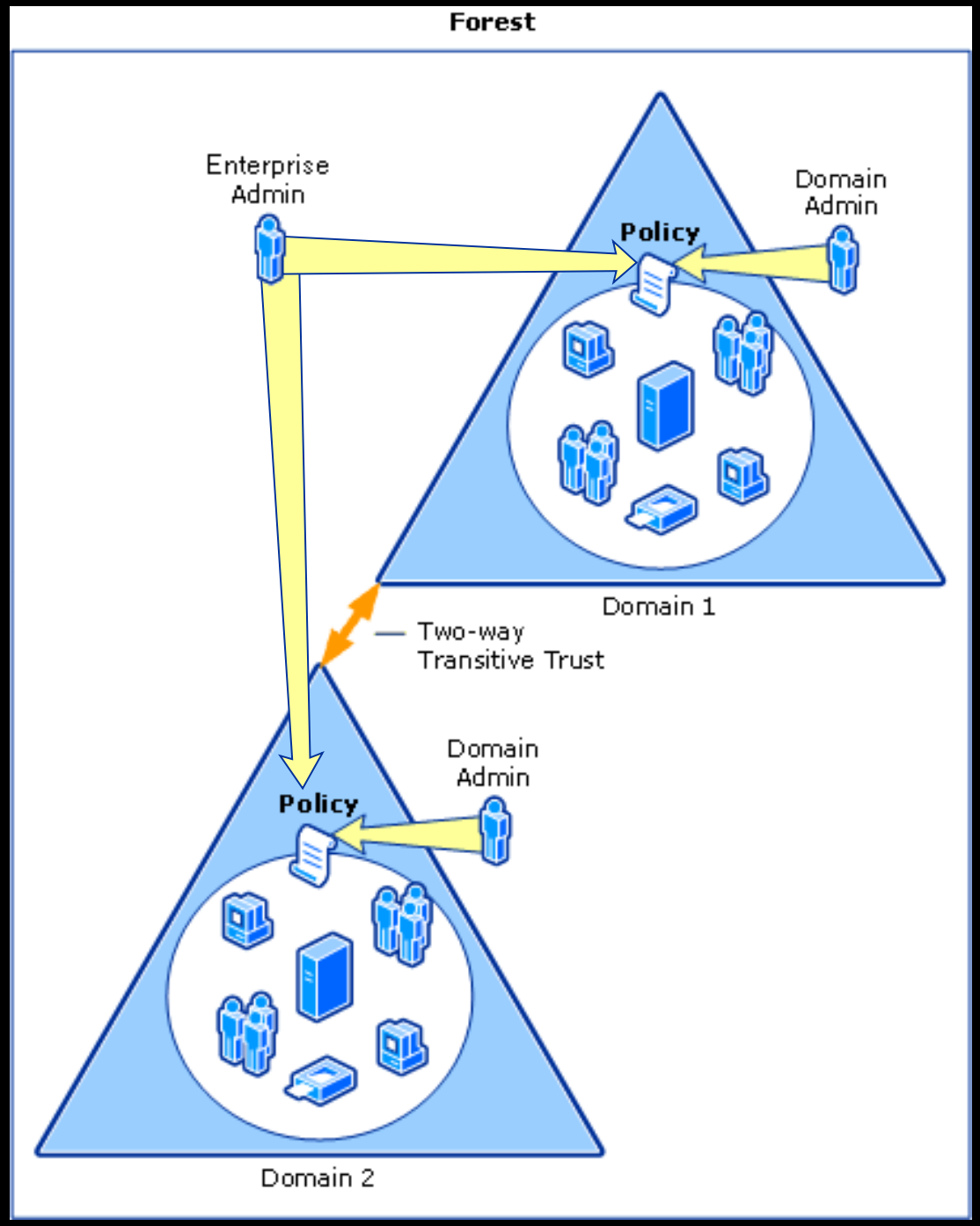
@Jonas_B_K

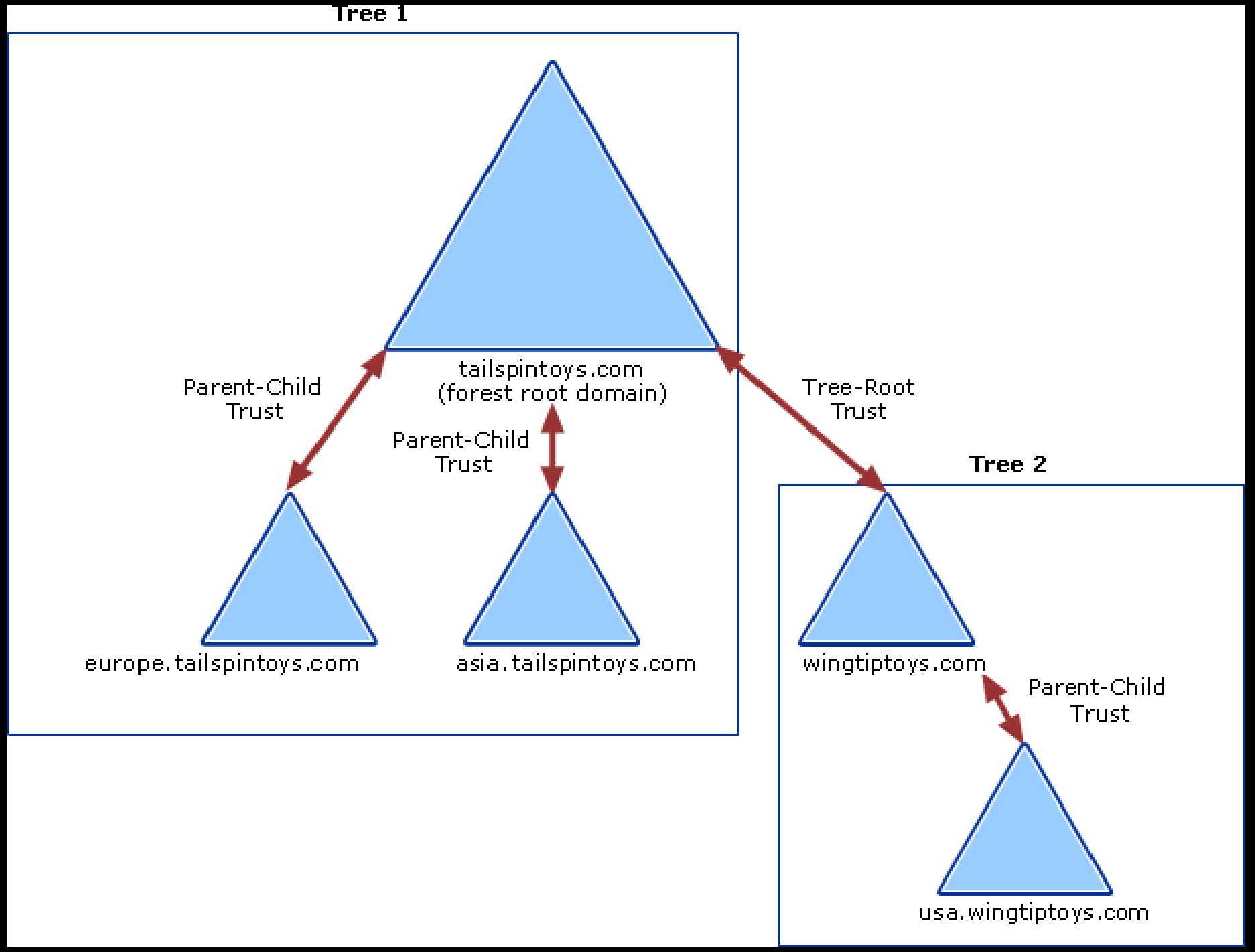
AD domains and forests 101

Where are the boundaries then?

How security boundaries are violated

Audit for security boundary violations in BloodHound


Forest
Enterprise Admin
Domain Admin
Policy
Domain 1
Two-way Transitive Trust
Domain Admin
Policy
Domain 2

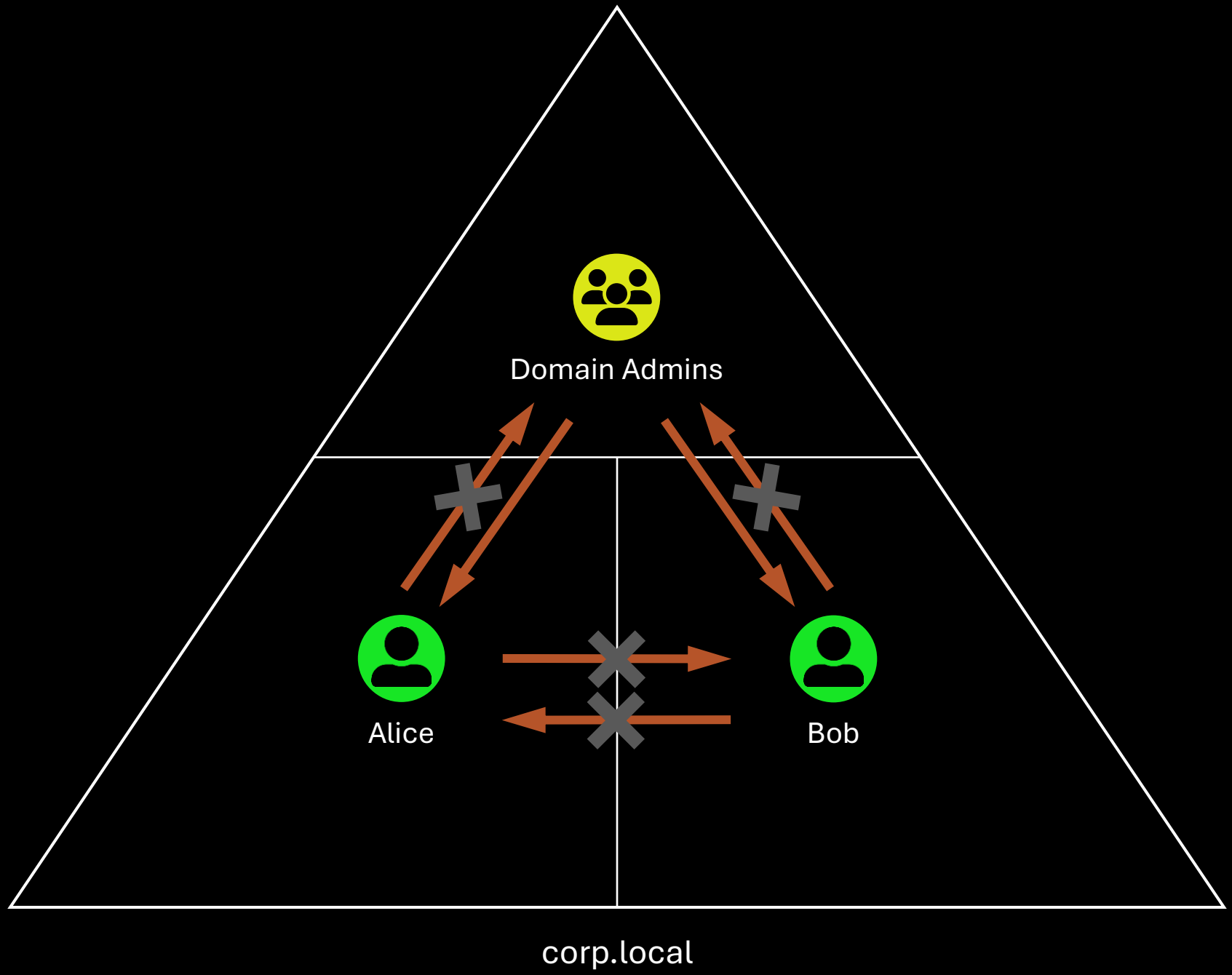

Tree 1
tailspintoys.com
(forest root domain)
Parent-Child
Trust
Parent-Child
Trust
Tree-Root
Trust
europe.tailspintoys.com
asia.tailspintoys.com
Tree 2
wingtiptoys.com
Parent-Child
Trust
usa.wingtiptoys.com

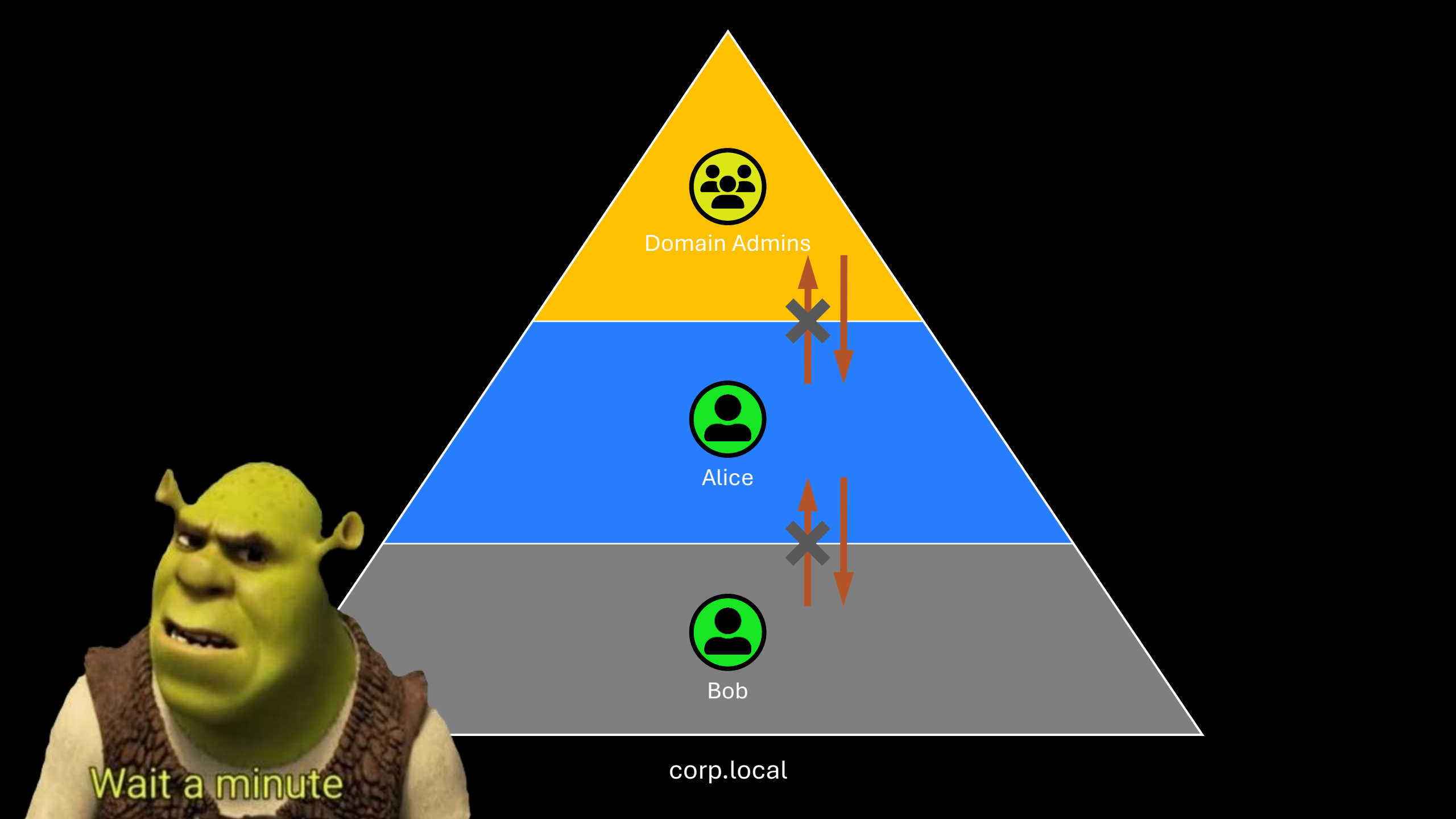
AD domains and forests 101

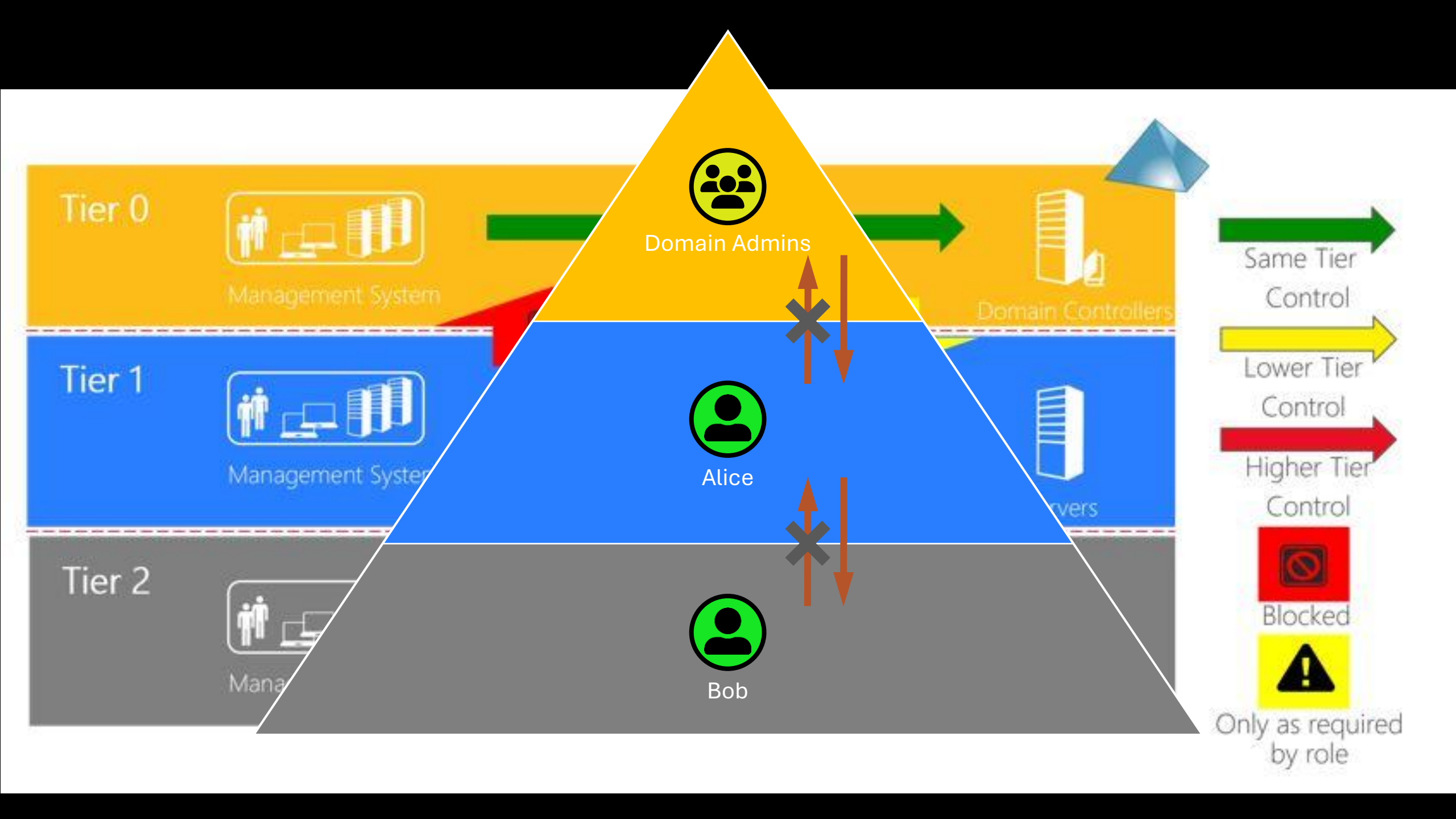
Where are the boundaries then?

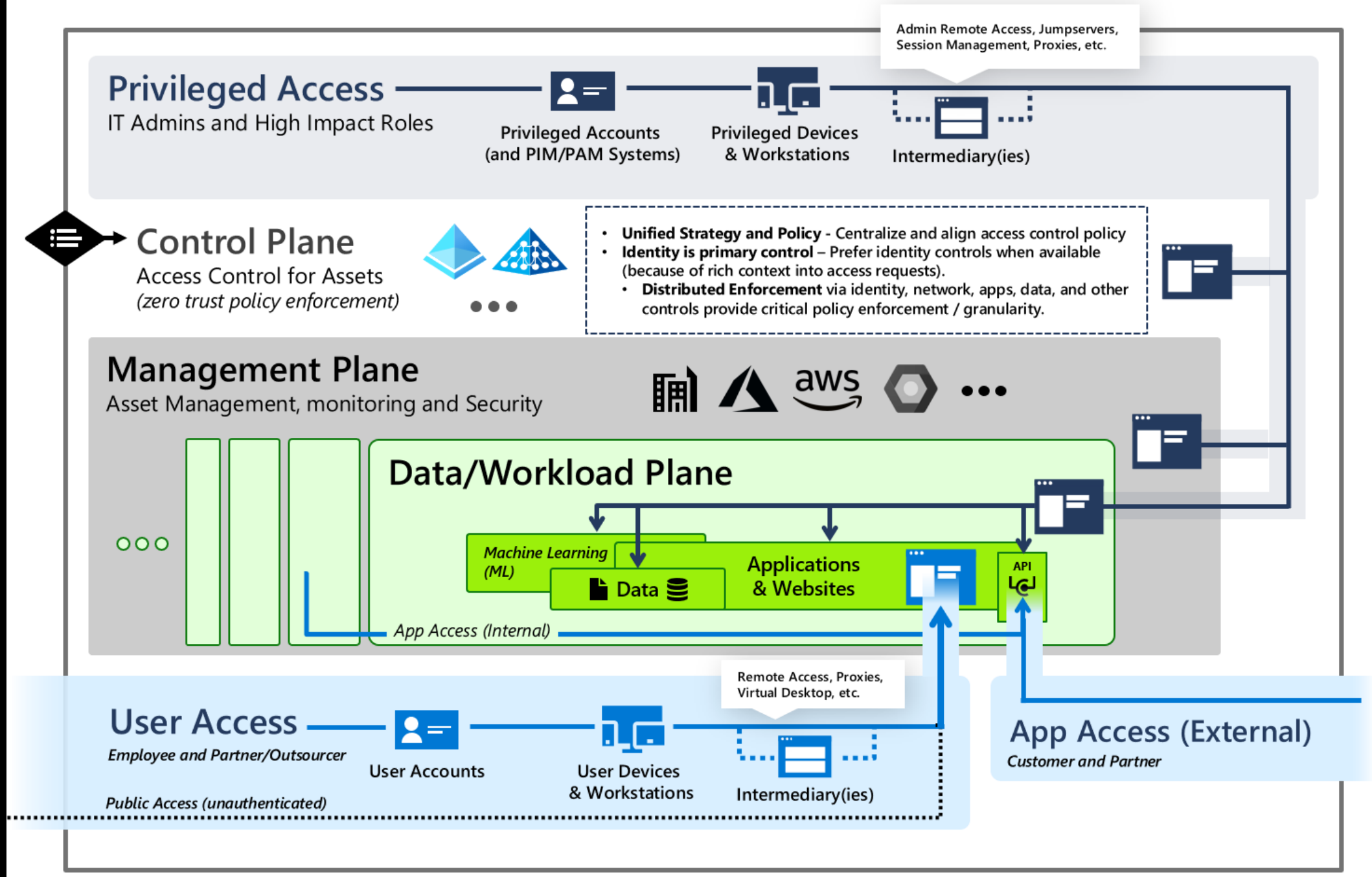
How security boundaries are violated

Audit for security boundary violations in BloodHound


Domain Admins
Alice
Bob
corp.local

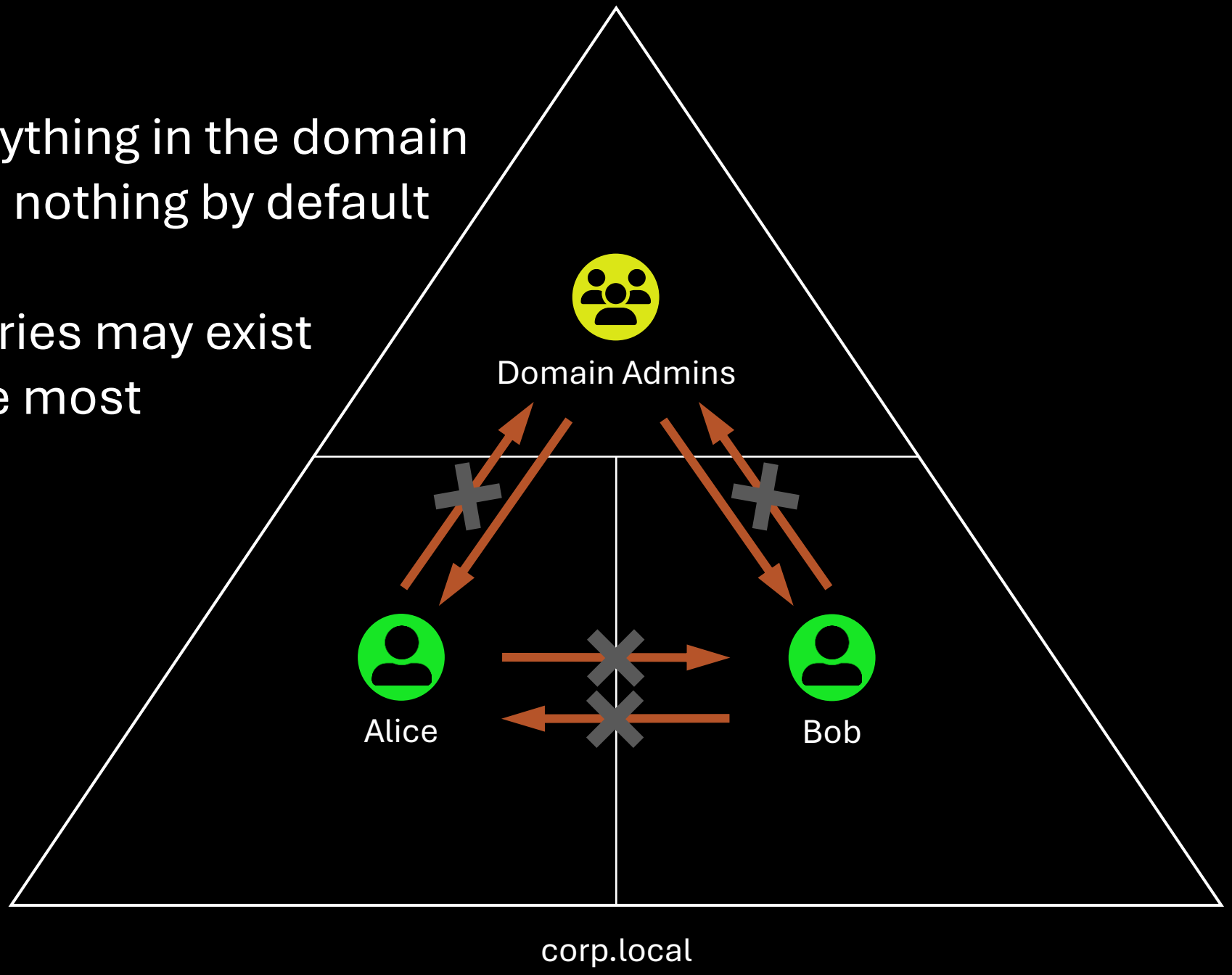

Domain Admins
Alice
Bob
corp.local
Wait a minute


Tier 0
Management System
Domain Controllers
Tier 1
Management Syste
vers
Tier 2
Mana
Domain Admins
Alice
Bob
Same Tier Control
Lower Tier Control
Higher Tier Control
Blocked
Only as required by role

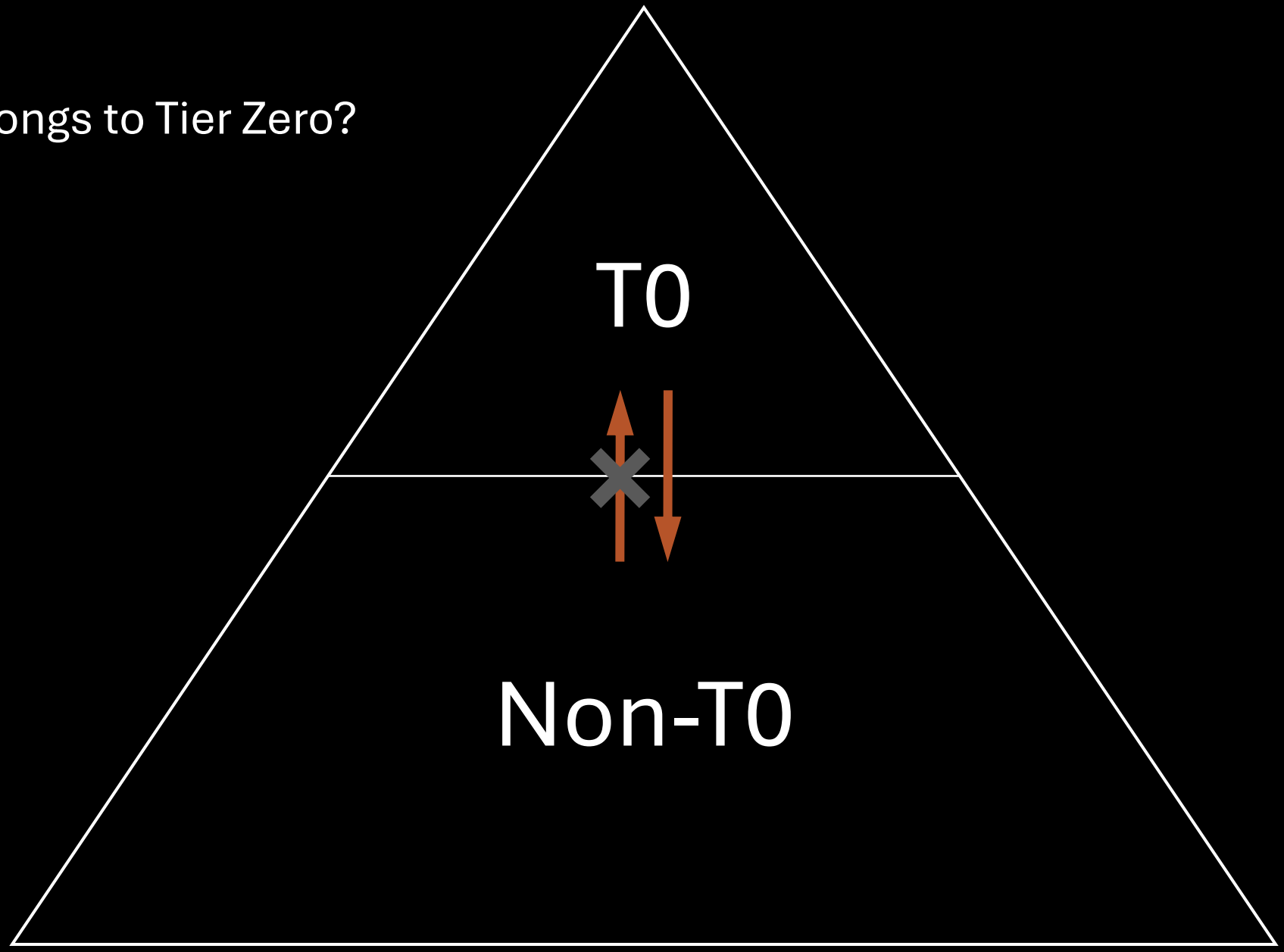

Admin Remote Access, Jumpservers, Session Management, Proxies, etc.
Privileged Access
IT Admins and High Impact Roles
Privileged Accounts (and PIM/PAM Systems)
Privileged Devices & Workstations
Intermediary(ies)
Control Plane
Access Control for Assets
(zero trust policy enforcement)
• Unified Strategy and Policy - Centralize and align access control policy
• Identity is primary control – Prefer identity controls when available (because of rich context into access requests).
• Distributed Enforcement via identity, network, apps, data, and other controls provide critical policy enforcement / granularity.
Management Plane
Asset Management, monitoring and Security
aws
Data/Workload Plane
Machine Learning (ML)
Data
Applications & Websites
API
App Access (Internal)
Remote Access, Proxies, Virtual Desktop, etc.
User Access
Employee and Partner/Outsourcer
User Accounts
User Devices & Workstations
Intermediary(ies)
Public Access (unauthenticated)
App Access (External)
Customer and Partner

Tier Zero controls everything in the domain
Non-Tier Zero controls nothing by default

Many security boundaries may exist
.. but let's focus on the most essential one



What belongs to Tier Zero?



What belongs to Tier Zero?

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 configuration
Account Operators	DC group	Active Directory	SID: S-1-5-32-548	The Account Operators group grants limited account creation privileges to a user. Members of this group... Read more	YES - Takeover	N/A - Compr default
Administrators	DC group	Active Directory	SID: S-1-5-32-544	Members of the Administrators group have complete and unrestricted access to the computer. If the... Read more	YES - Takeover	N/A - Compr default
Backup Operators	DC group	Active Directory	SID: S-1-5-32-551	Members of the Backup Operators group can back up and restore all files on a computer, regardless of the... Read more	YES - Takeover	N/A - Compr default
Cryptographic Operators	DC group	Active Directory	SID: S-1-5-32-569	Members of this group are authorized to perform cryptographic operations. This security	NO	NO

TierZeroTable Public

Edit Pins · Unwatch 7

main · 1 Branch · 0 Tags · Go to file t · Add file · Code

JonasBK Update TierZeroTable.csv ✓ 793eb01 · 2 months ago · 28 Commits

.github/workflows	Create cla.yml	2 years ago
LICENSE	Create LICENSE	2 years ago
README.md	Update README.md - Part 4	4 months ago
TierZeroTable.csv	Update TierZeroTable.csv	2 months ago
index.html	make table ux better	4 months ago

README · GPL-3.0 license

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

https://github.com/SpecterOps/TierZeroTable

What belongs to Tier Zero?

TierZeroTable Public

Edit Pins | Unwatch 7

main | 1 Branch | 0 Tags | Go to file t | Add file | Code

JonasBK Update TierZeroTable.csv ✓ 793eb01 · 2 months ago 28 Commits

ate cla.yml	2 years ago
ate LICENSE	2 years ago
date README.md - Part 4	4 months ago
date TierZeroTable.csv	2 months ago
ke table ux better	4 months ago

ong to Tier Zero.

erZeroTable

Blog posts:

- What is Tier Zero - Part 1

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://gith

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

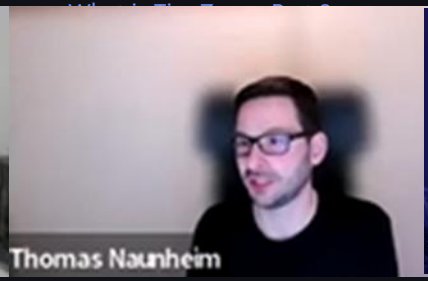
Search...

Name	Type	IdP	Ide
Account Operators	DC group	Active Directory	SID
Administrators	DC group	Active Directory	SID
Backup Operators	DC group	Active Directory	SID: S-1-5-32-551

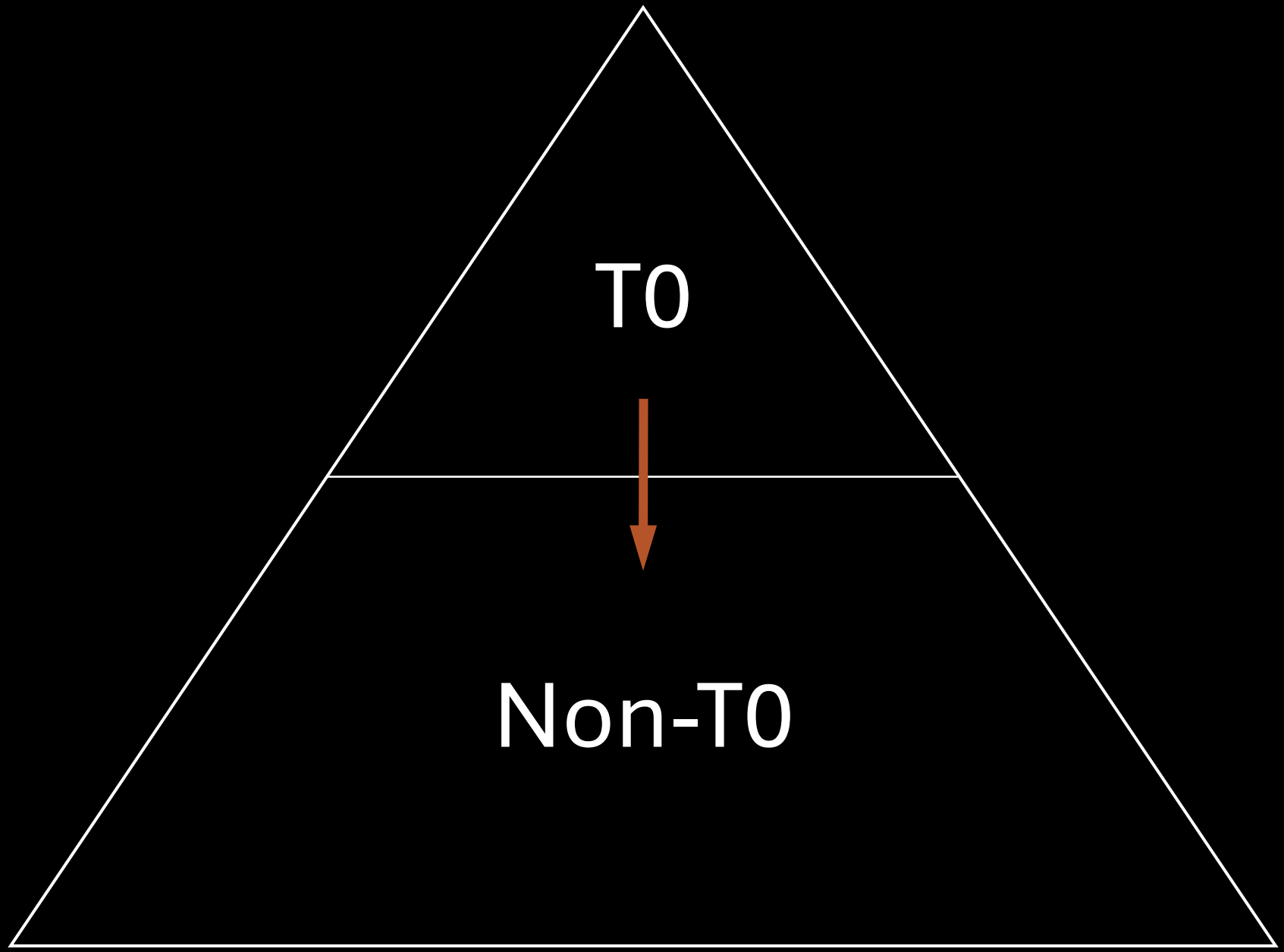
Members of the Backup Operators group can back up and restore all files on a computer, regardless of the... Read more

YES - Takeover

N/A - Compr default



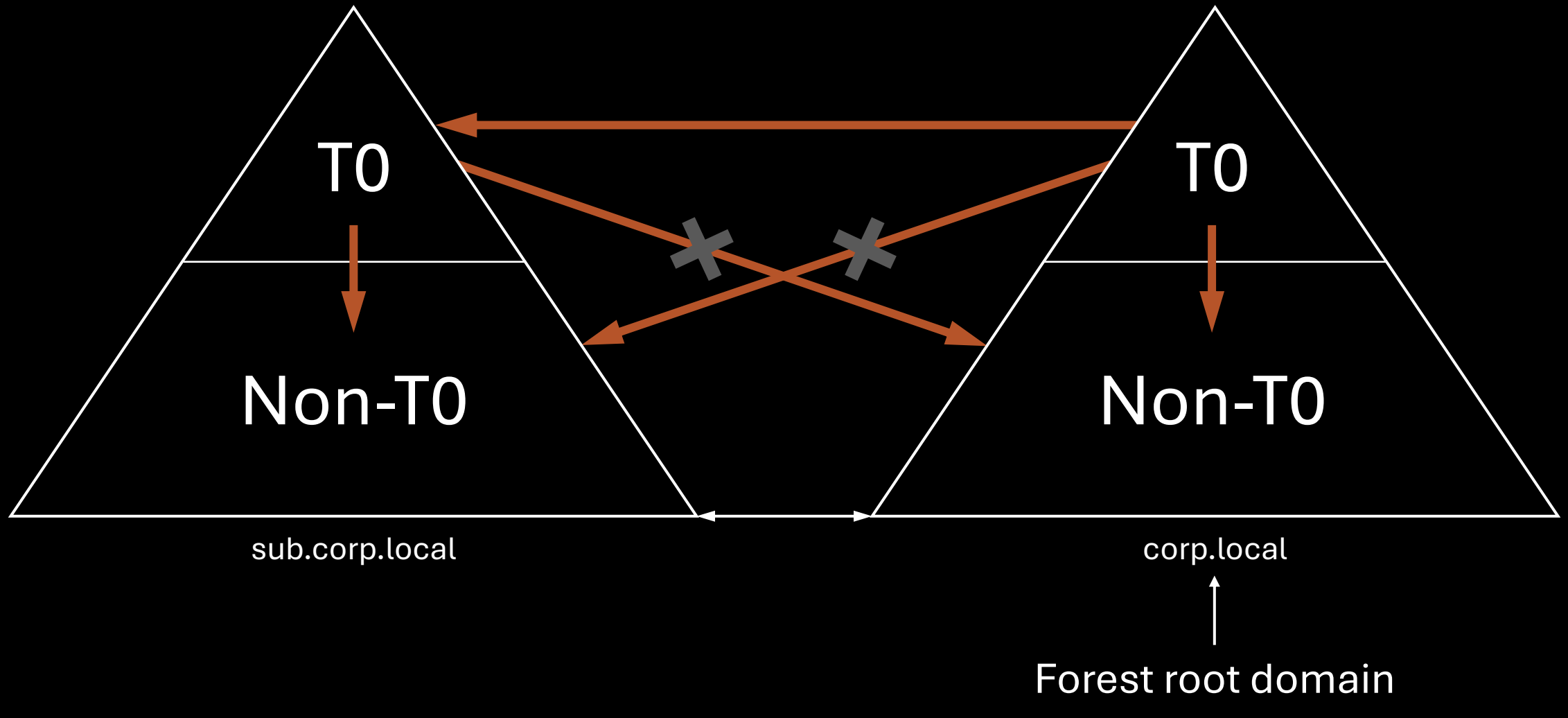
https://github.com/SpecterOps/TierZeroTable



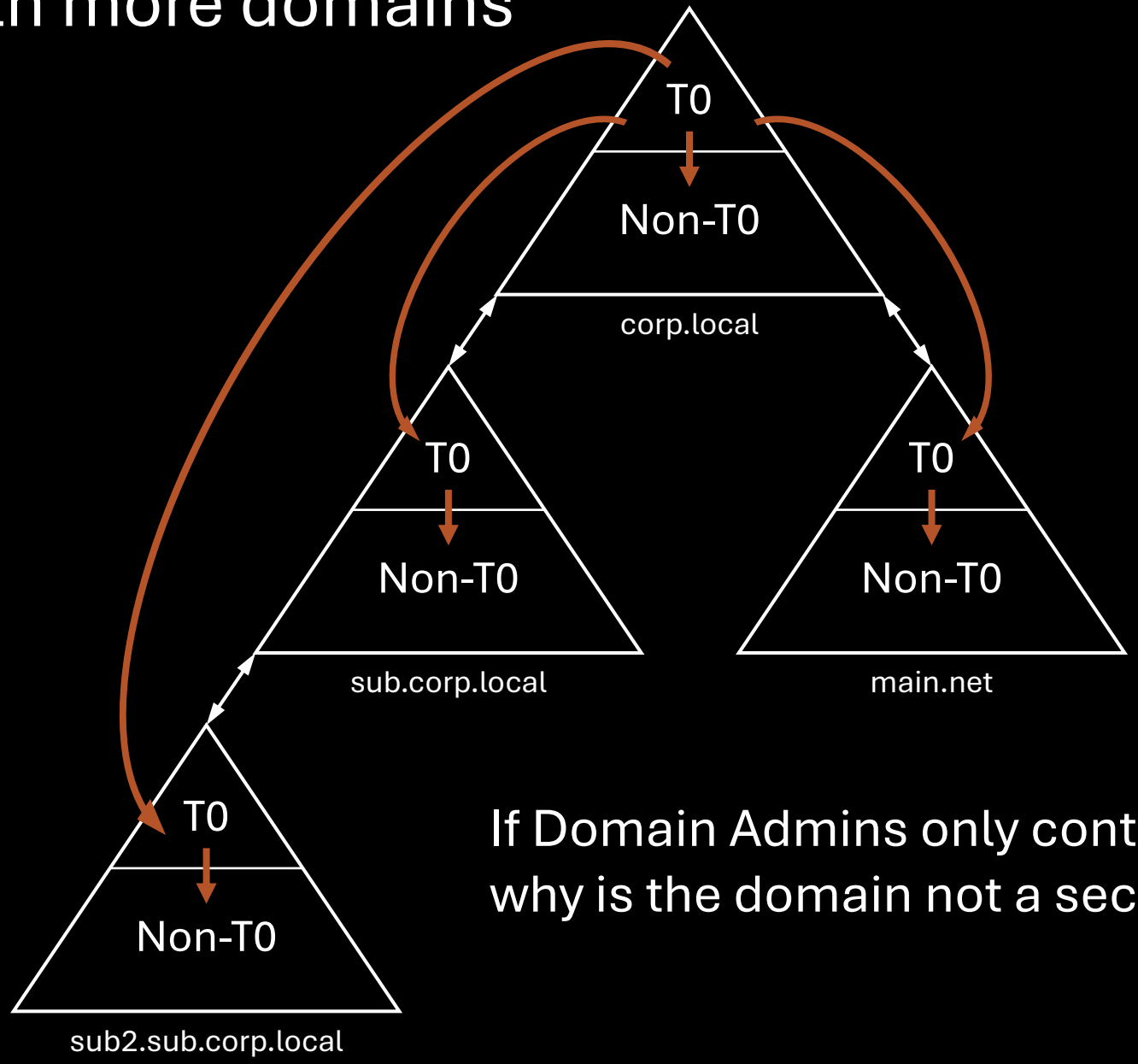
corp.local

Forest with two domains

Domain Admins control their own domain - only
Enterprise Admins control the entire forest



Forest with more domains



If Domain Admins only control their own domain, why is the domain not a security boundary then?

If Domain Admins only control their own domain,
why is the domain not a security boundary then?

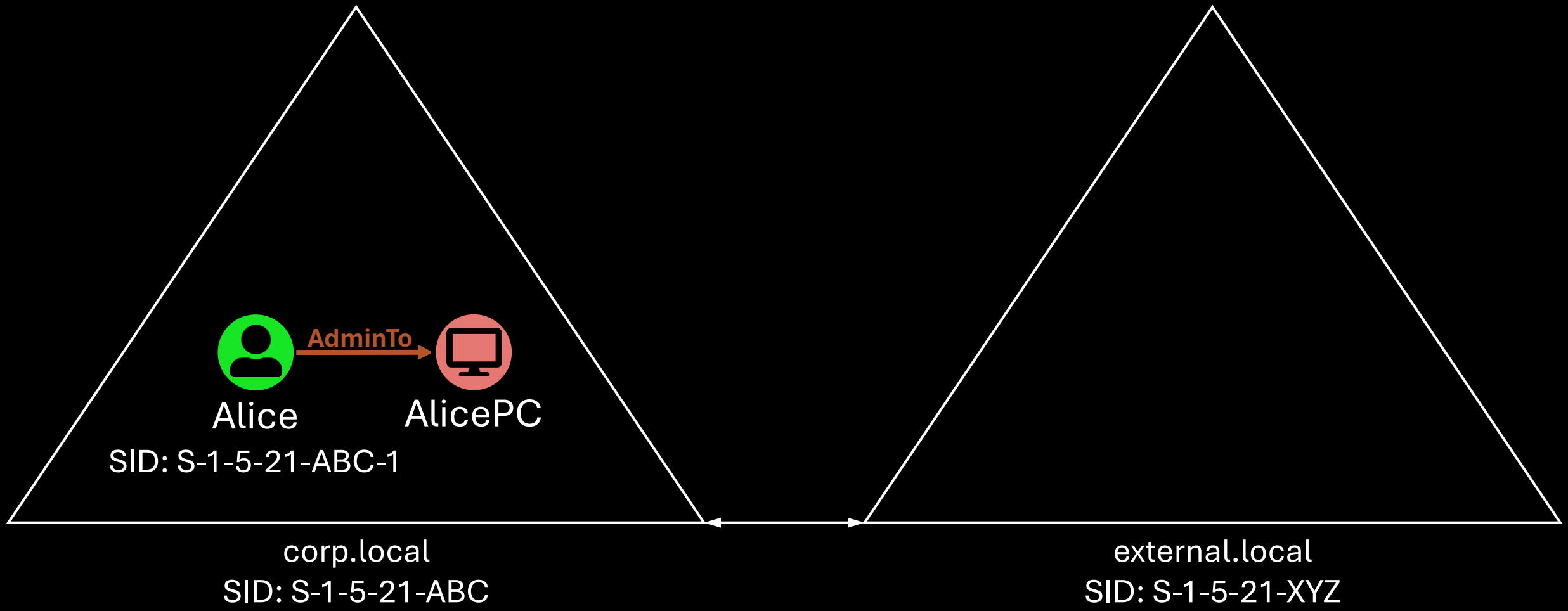
A forest is the only component of the Active Directory logical structure that is a security boundary. By contrast, a domain is not a security boundary because it is not possible for administrators from one domain to prevent a malicious administrator from another domain within the forest from accessing data in their domain. A domain is, however, the

Domain Admins can compromise other domains within the forest

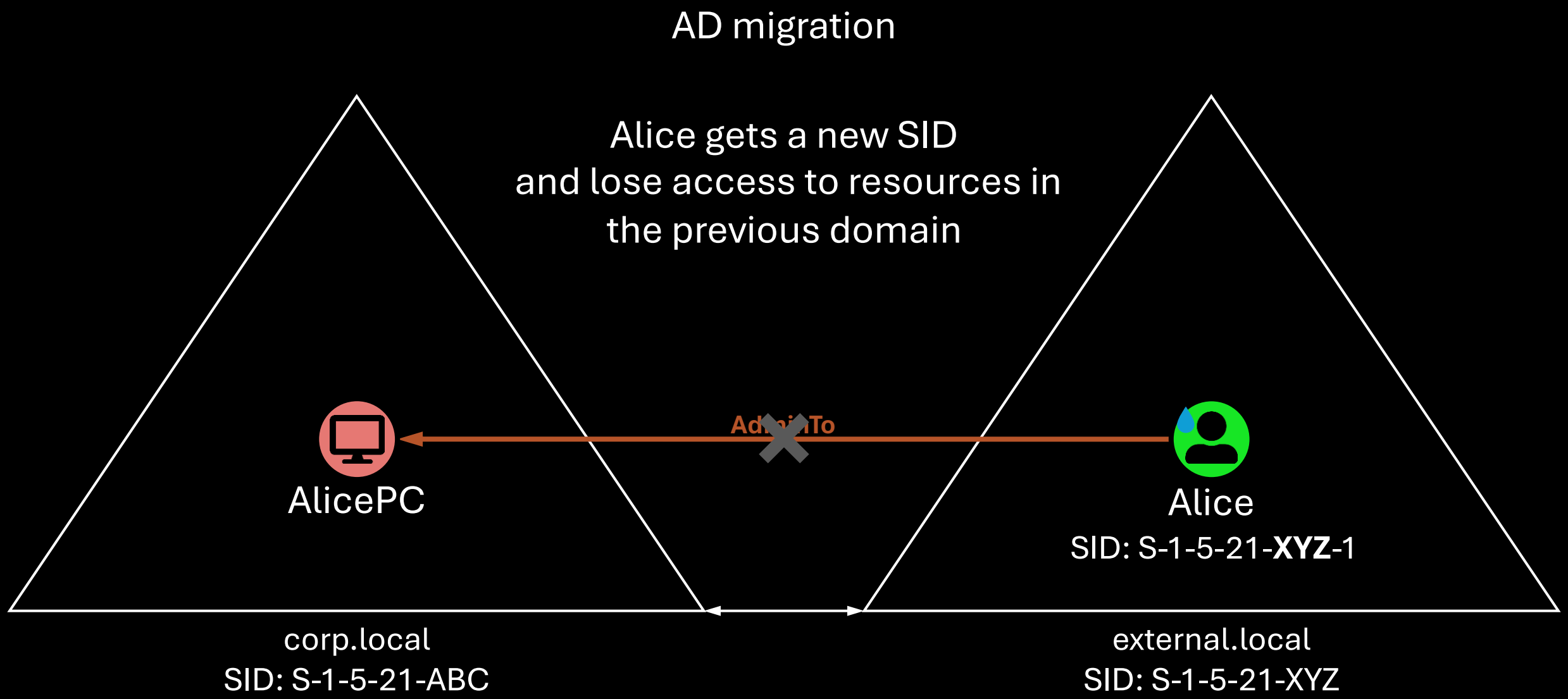
1. Trusts within a forest has a weak configuration by default
    a. Weak SID filtering configuration – enables SID History Spoofing

Weak SID filtering configuration – enables SID History Spoofing

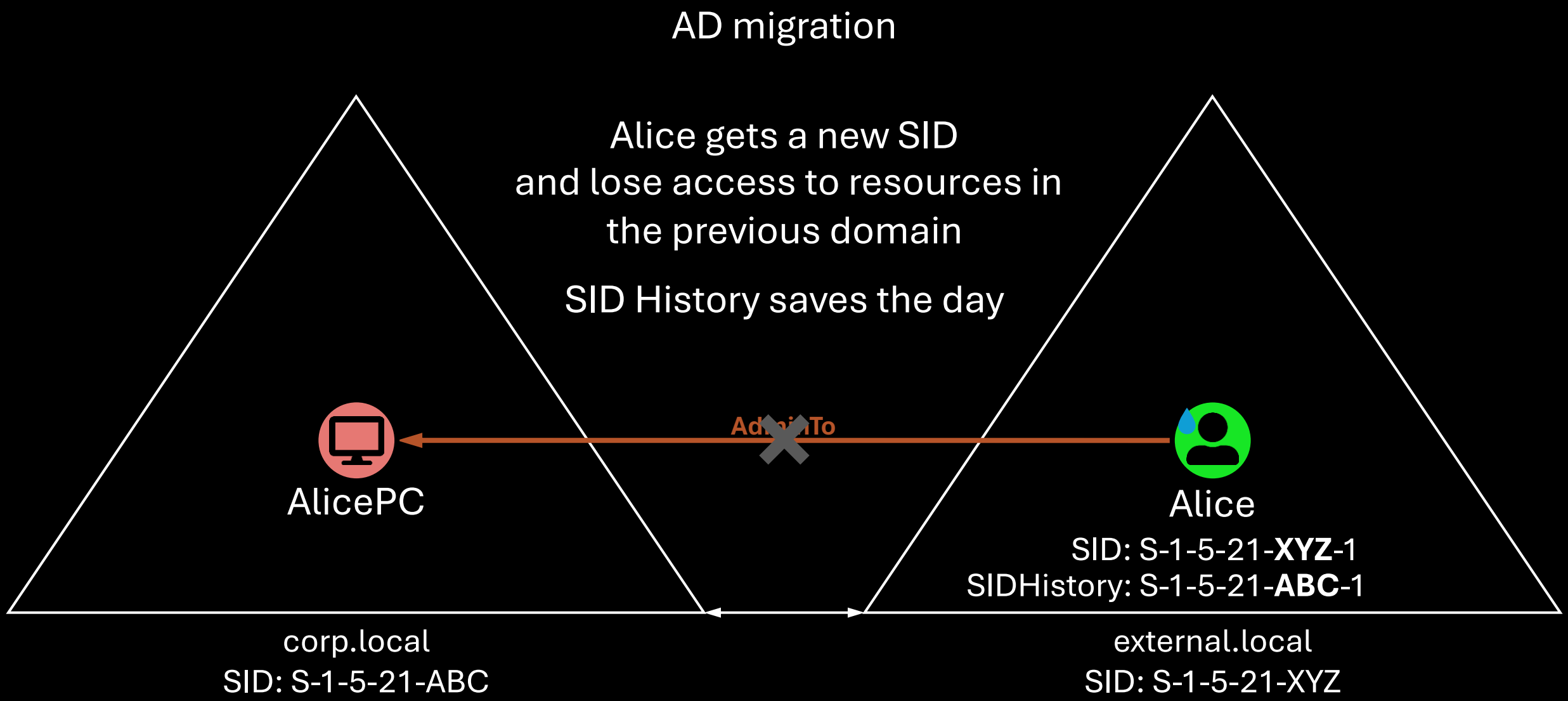
AD migration



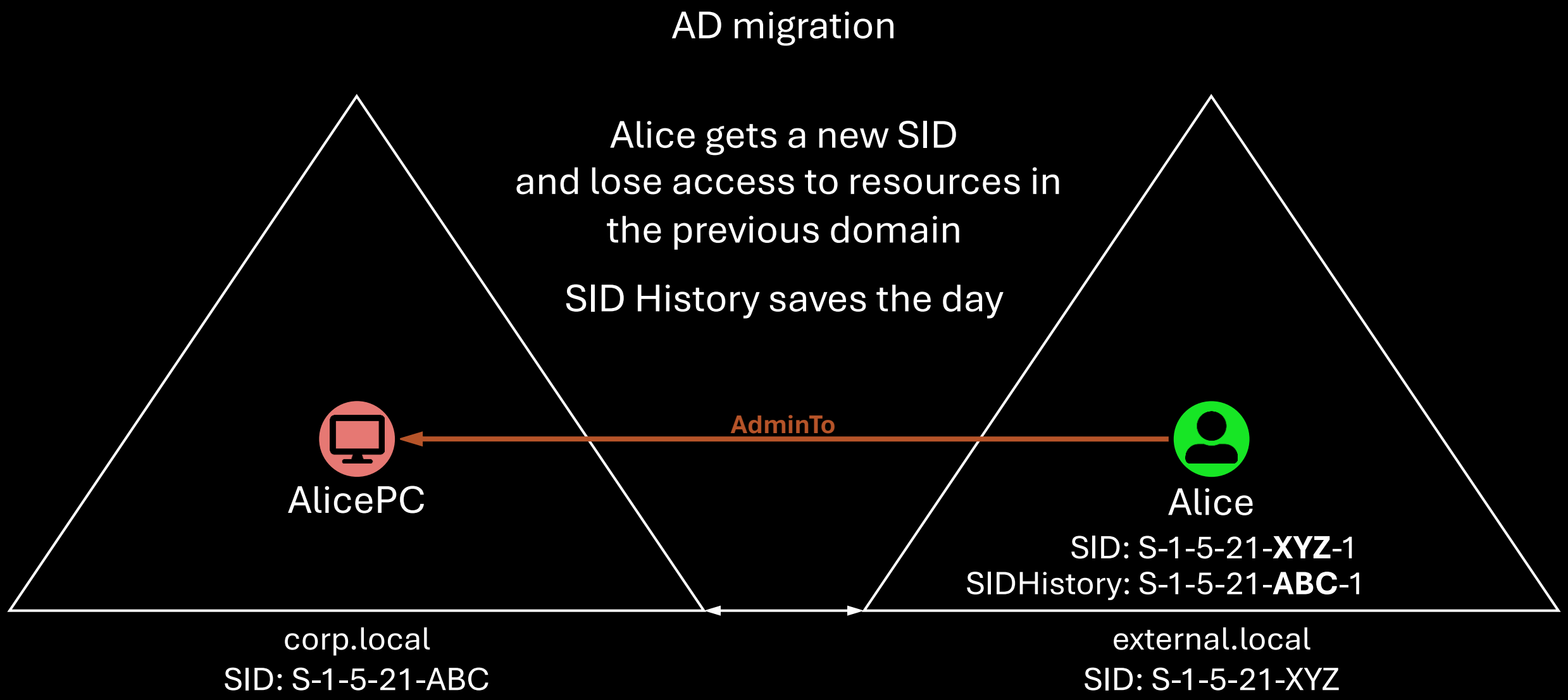
Weak SID filtering configuration – enables SID History Spoofing



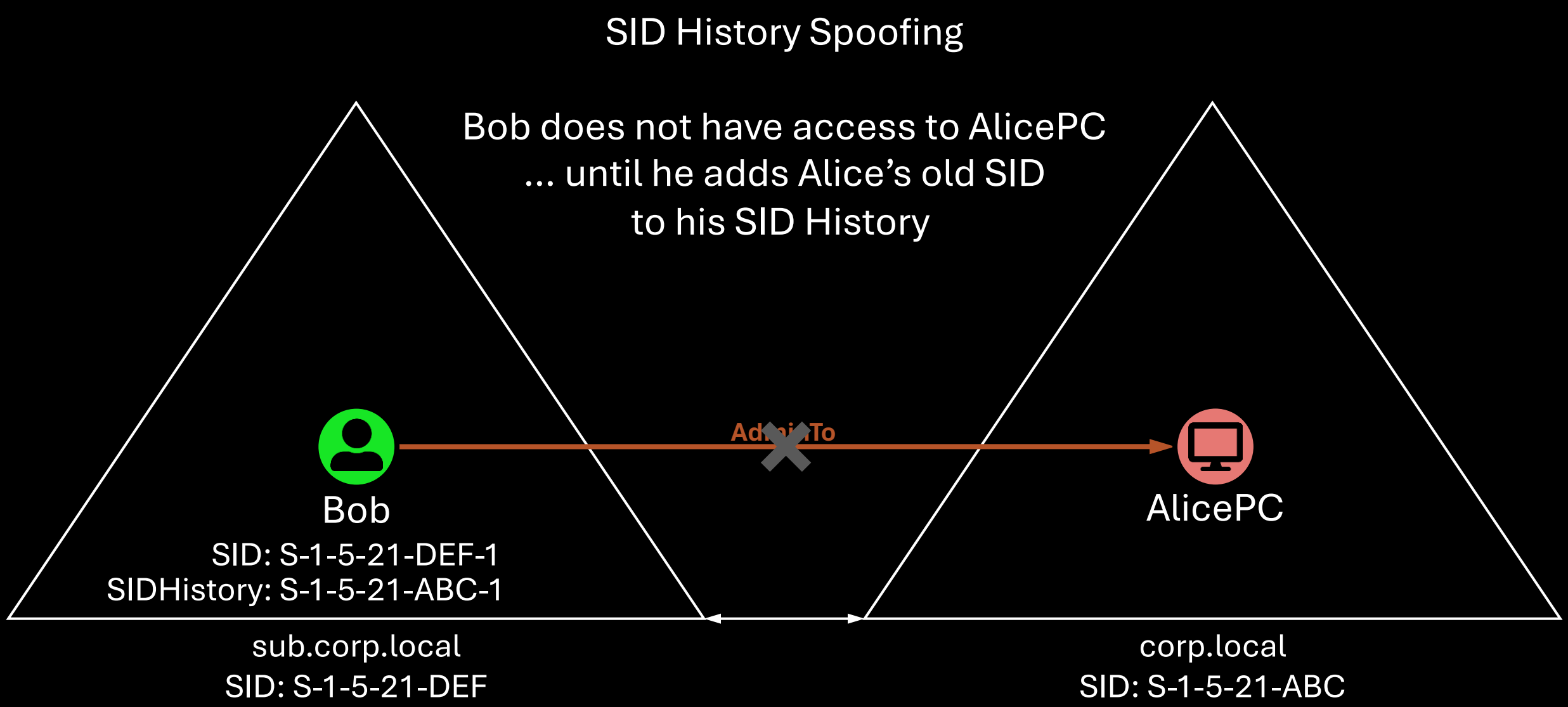
Weak SID filtering configuration – enables SID History Spoofing



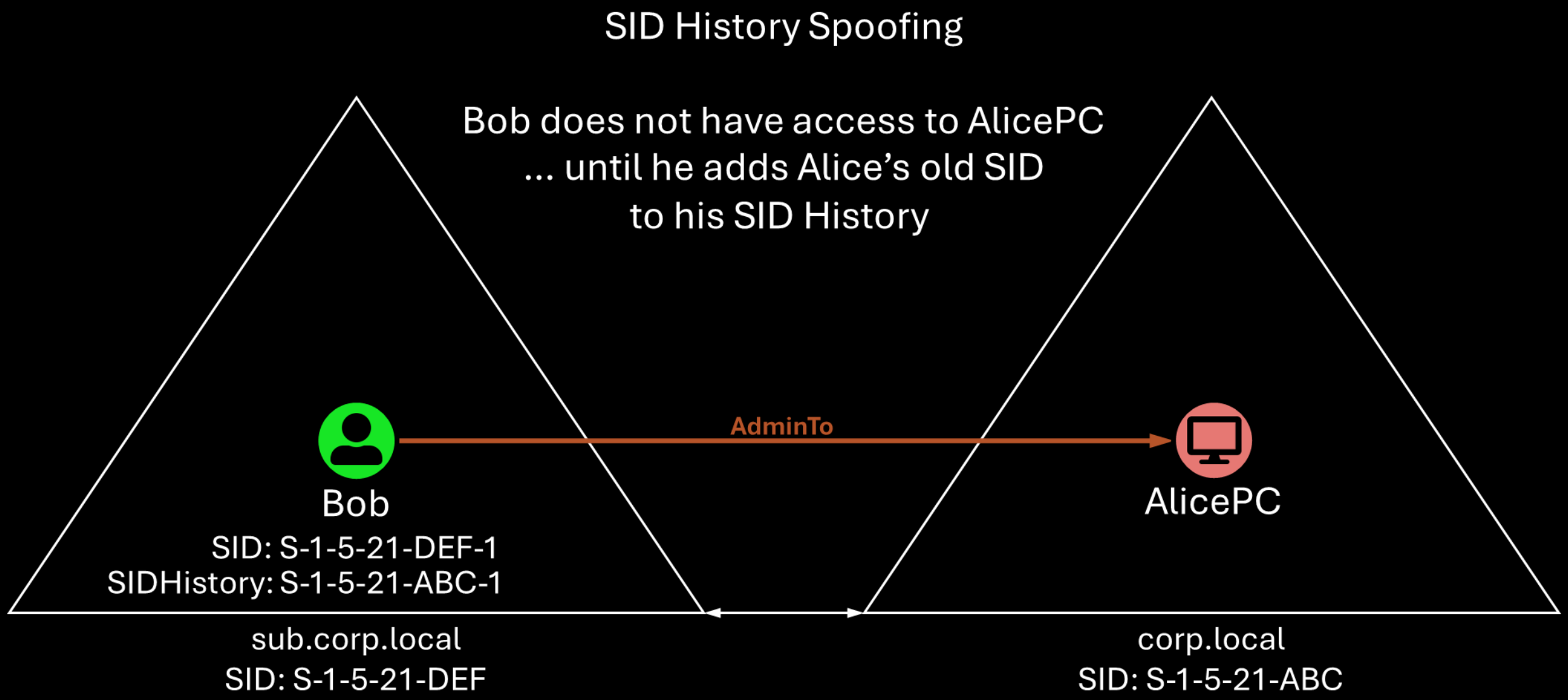
Weak SID filtering configuration – enables SID History Spoofing



Weak SID filtering configuration – enables SID History Spoofing

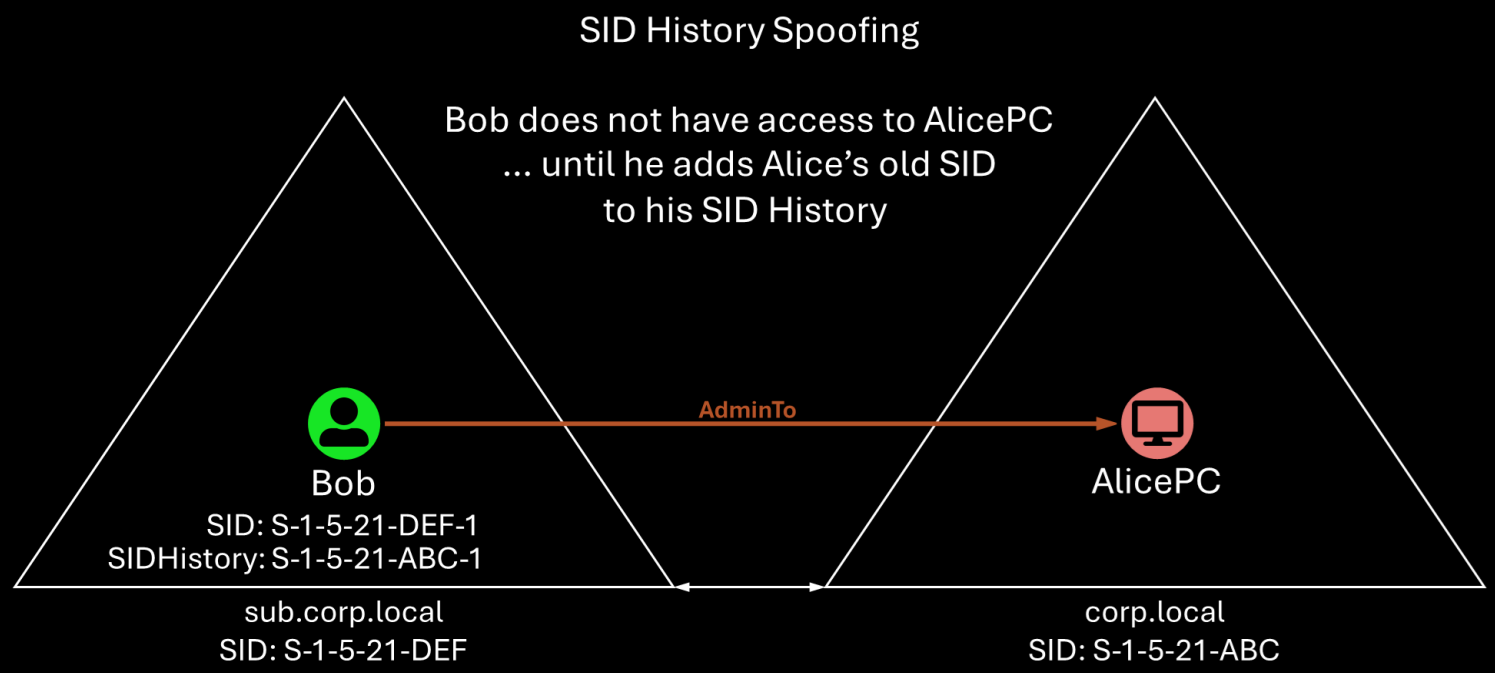


Weak SID filtering configuration – enables SID History Spoofing



Weak SID filtering configuration – enables SID History Spoofing

The SID History SID does **not** have to be a migrated user's – it can even be the Enterprise Admins SID

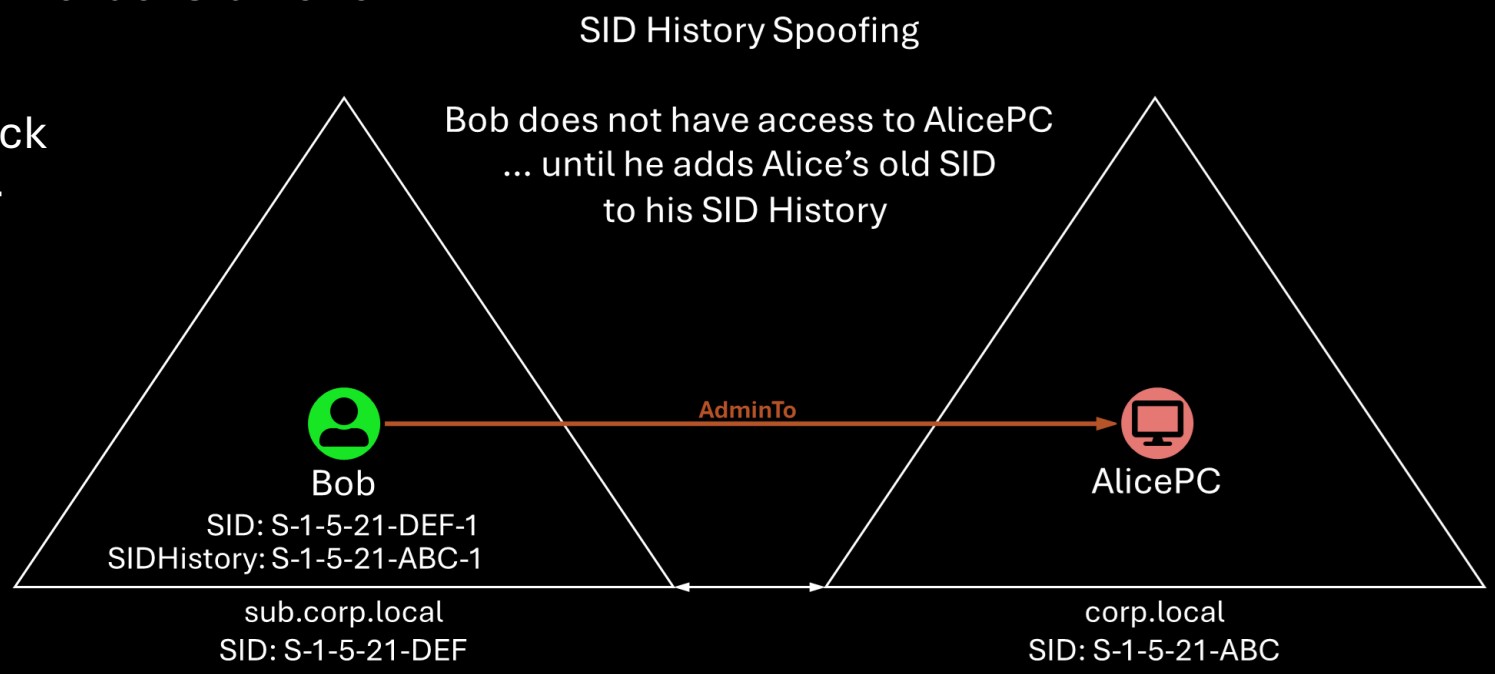


Weak SID filtering configuration – enables SID History Spoofing

The SID History SID does **not** have to be a migrated user's – it can even be the Enterprise Admins SID

Requires admin rights on a DC to modify SID History

1. Directly in the AD attribute
   DSInternals: Add-ADDBSidHistory by Michael Grafnetter
2. In the user's TGT
   Rubeus: golden/diamond by GhostPack
3. In the user's inter-realm TGT
   Rubeus: silver by GhostPack



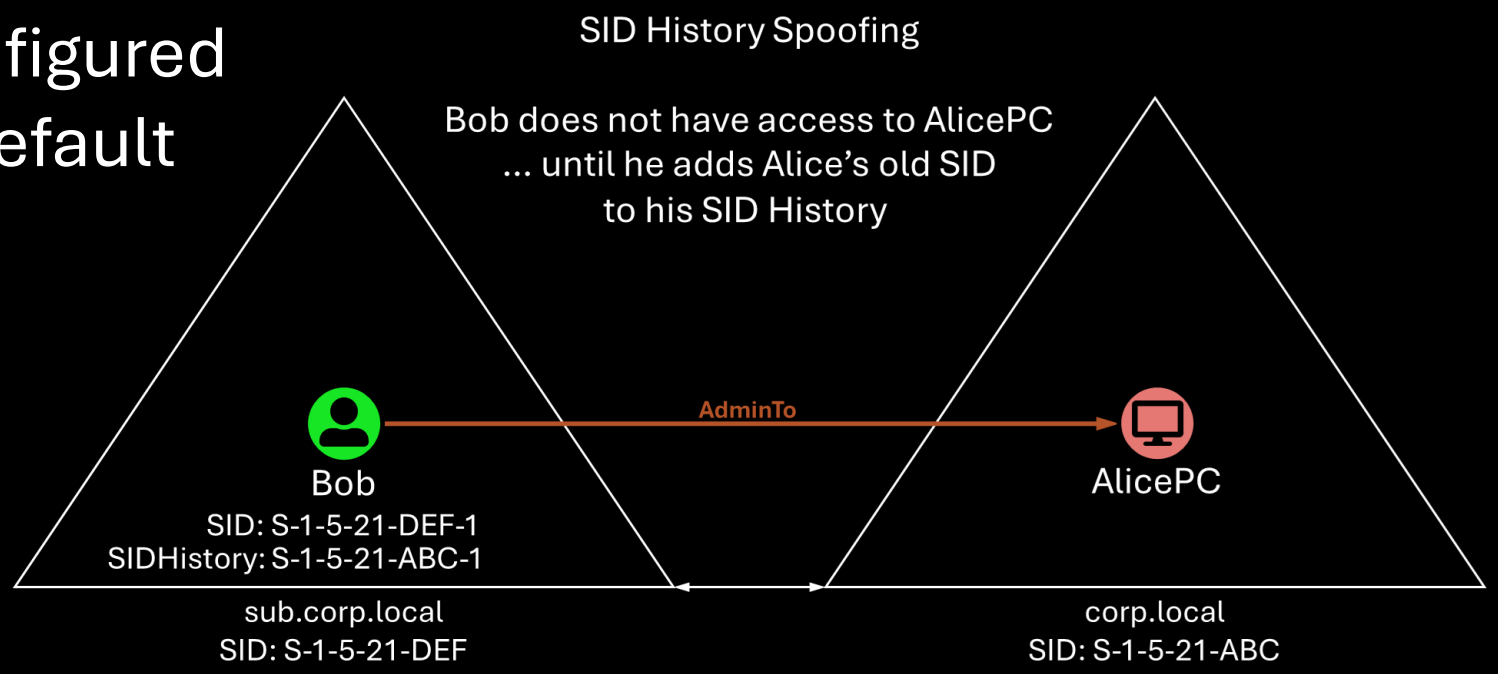
Weak SID filtering configuration – enables SID History Spoofing

SID History usage requires weak SID filtering

- Rejects built-in SIDs (e.g. S-1-5-32-544) but not domain SIDs

Strong SID filtering rejects SIDs from outside the source domain

Trusts within a forest is configured with weak SID filtering by default

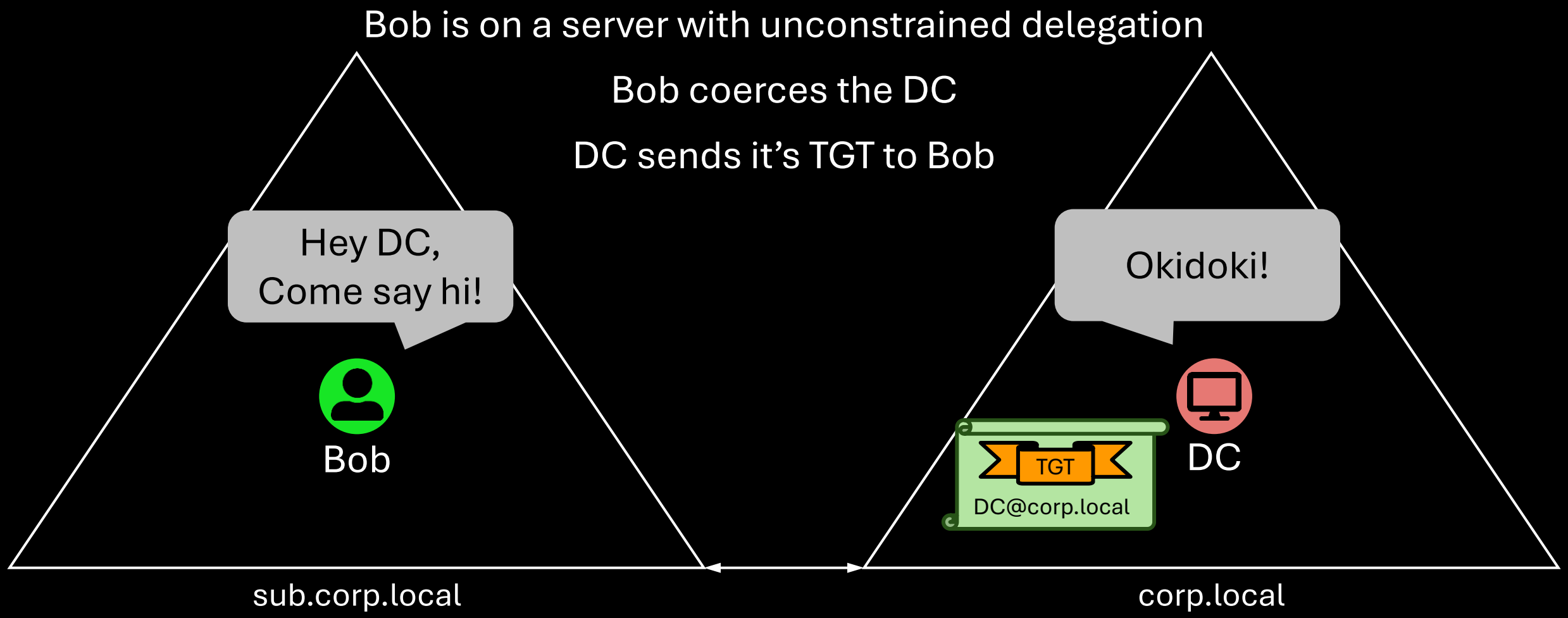


If Domain Admins only control their own domain,
why is the domain not a security boundary then?

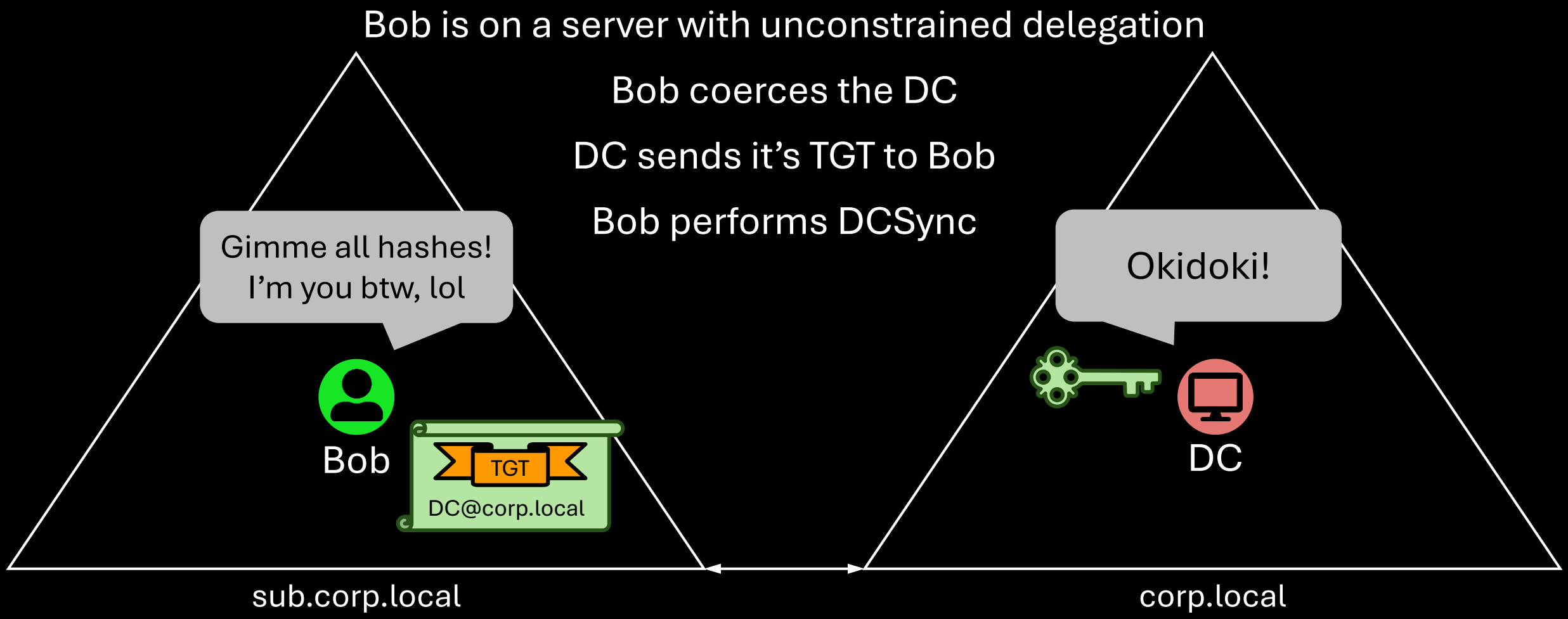
Domain Admins can compromise other domains within the forest

1. Trusts within a forest has a weak configuration by default
    a. Weak SID filtering configuration – enables SID History Spoofing
    b. TGT delegation enabled – coerce T0 server and get it’s TGT

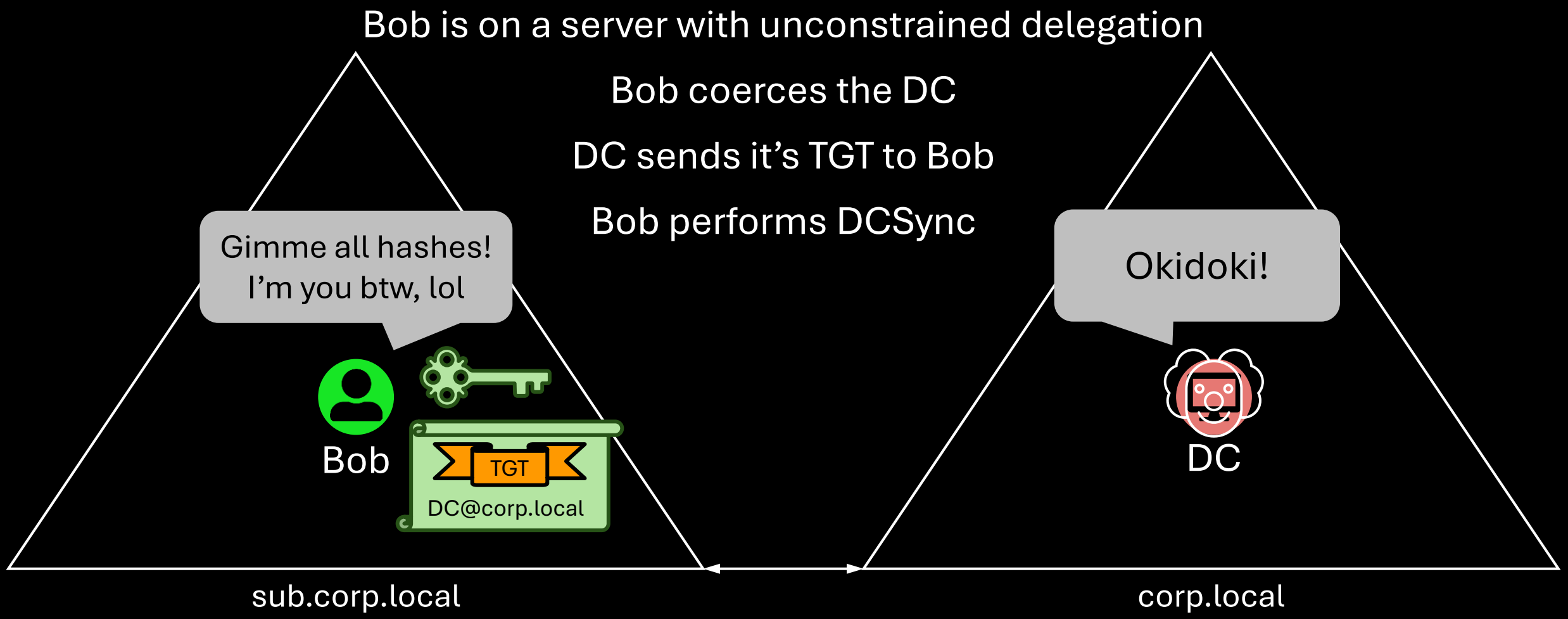
TGT delegation enabled – coerce T0 server and get it's TGT



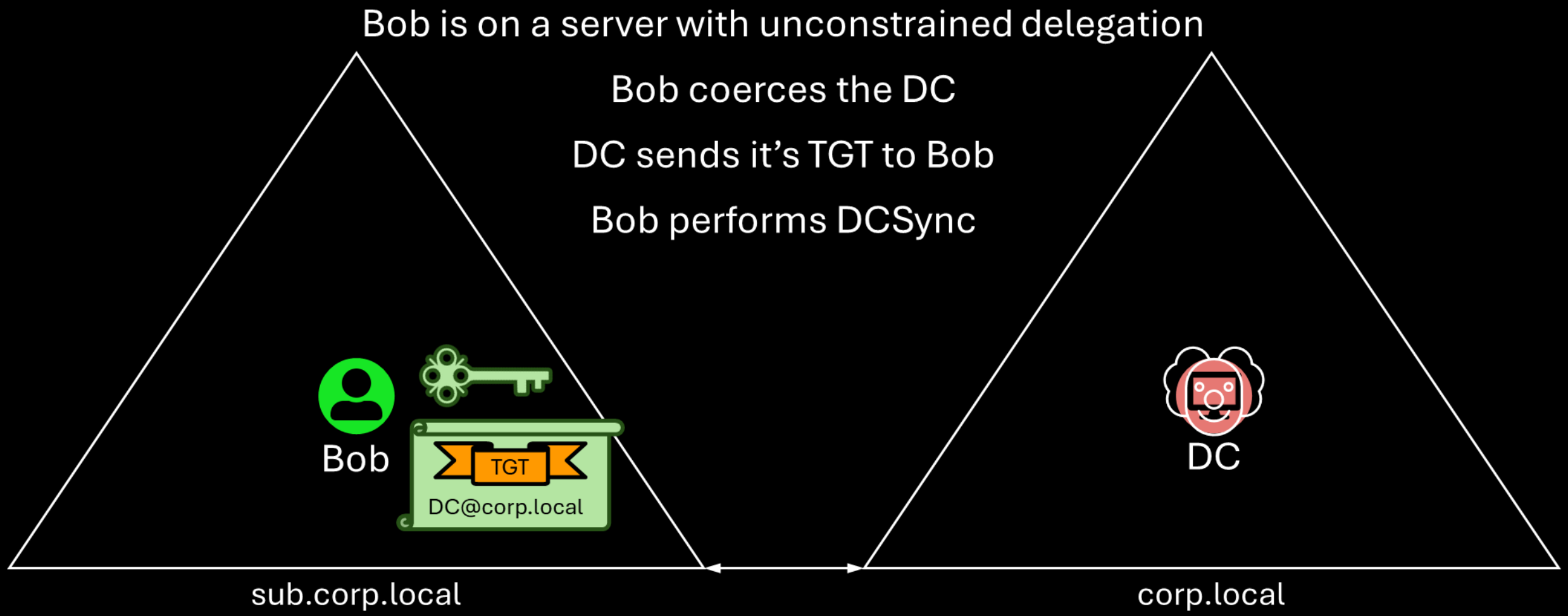
TGT delegation enabled – coerce T0 server and get it's TGT



TGT delegation enabled – coerce T0 server and get it's TGT



TGT delegation enabled – coerce T0 server and get it's TGT



TGT delegation enabled – coerce T0 server and get it's TGT

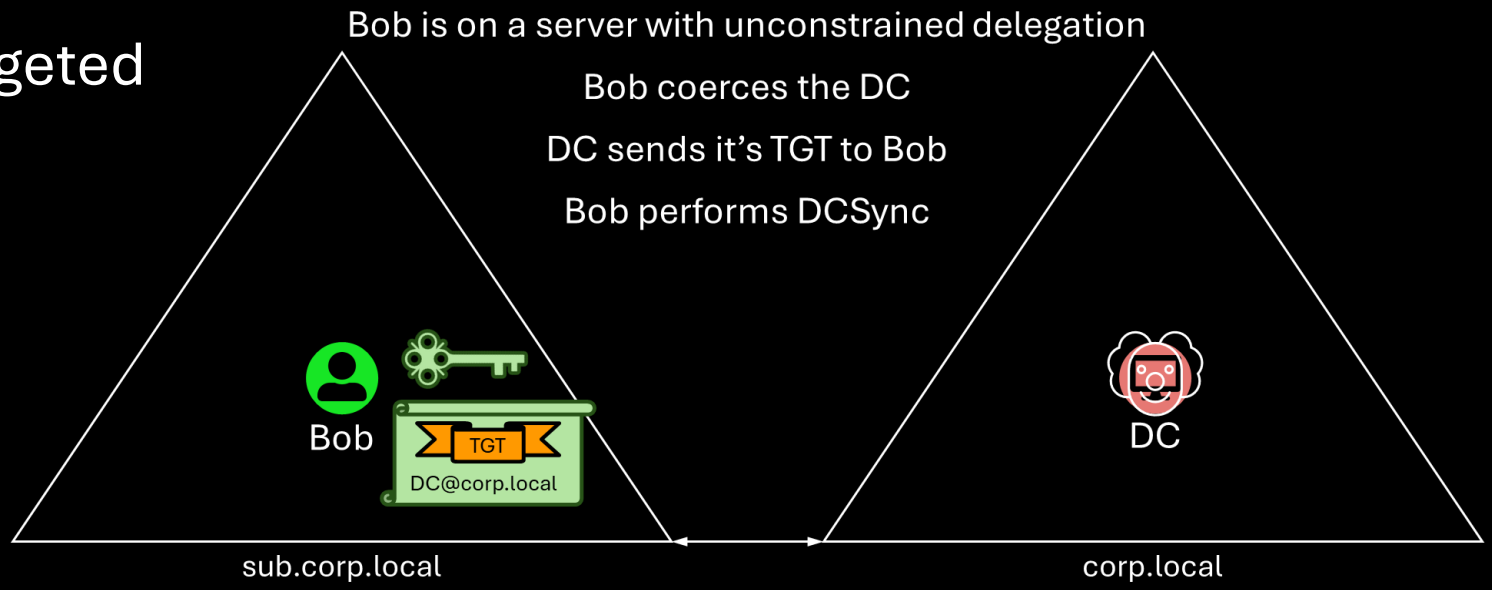
Requires compromise of a DC or another server/user with unconstrained delegation

Many coercion techniques exist

Windows Coerced Authentication Methods by p0dalirius

Any Windows server can be targeted
- not only DCs

Trusts within a forest allow
TGT delegation by default



If Domain Admins only control their own domain,
why is the domain not a security boundary then?

Domain Admins can compromise other domains within the forest

1. Trusts within a forest has a weak configuration by default
    a. Weak SID filtering configuration – enables SID History Spoofing
    b. TGT delegation enabled – coerce T0 server and get it's TGT

    Trust in quarantine mode prevents the attacks
    - Strong SID filtering - rejects SIDs from outside the source domain
    - TGT delegation disabled

If Domain Admins only control their own domain,
why is the domain not a security boundary then?

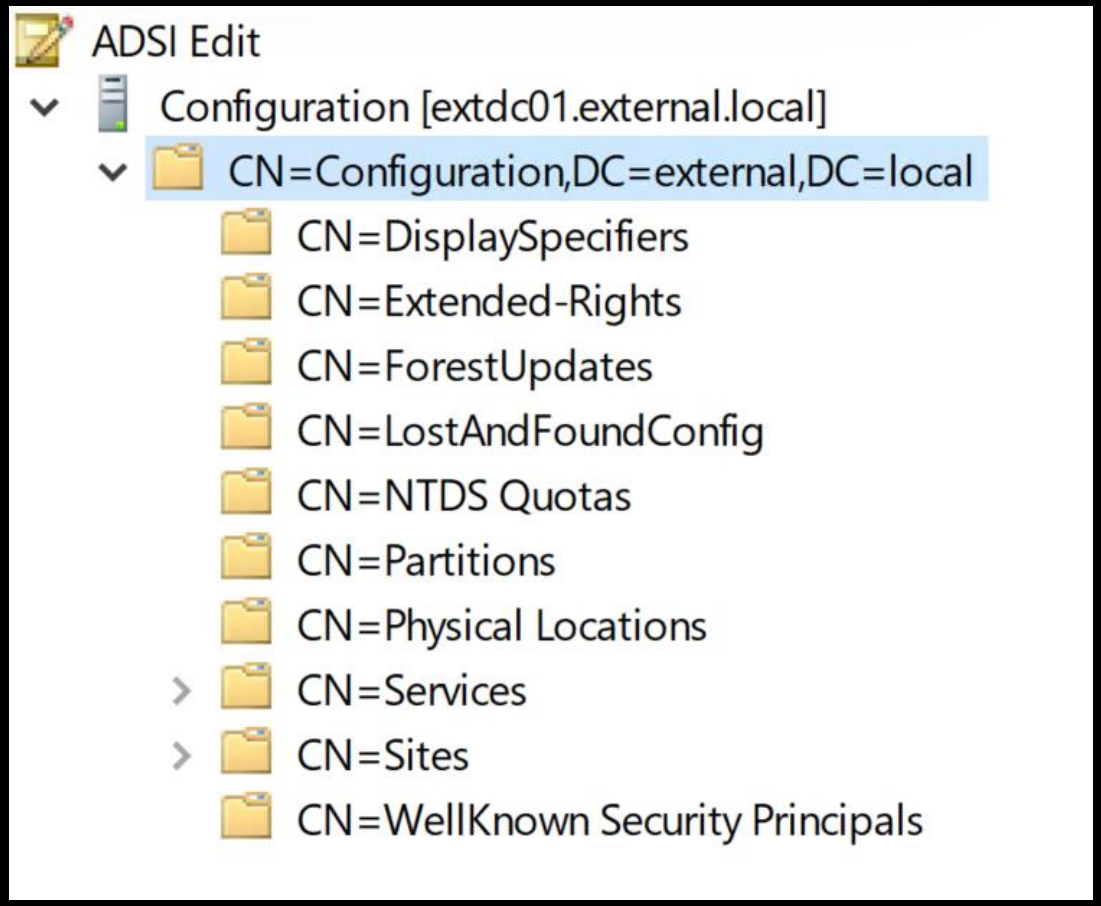
1. Trusts within a forest has a weak configuration by default
    a. Weak SID filtering configuration – enables SID History Spoofing
    b. TGT delegation enabled – coerce T0 server and get it's TGT
2. Configuration NC is writeable from any writeable DC in the forest

Configuration NC is writeable from any writeable DC in the forest

Holds forest-wide configurations

Domain Admins of a child domain has no write access

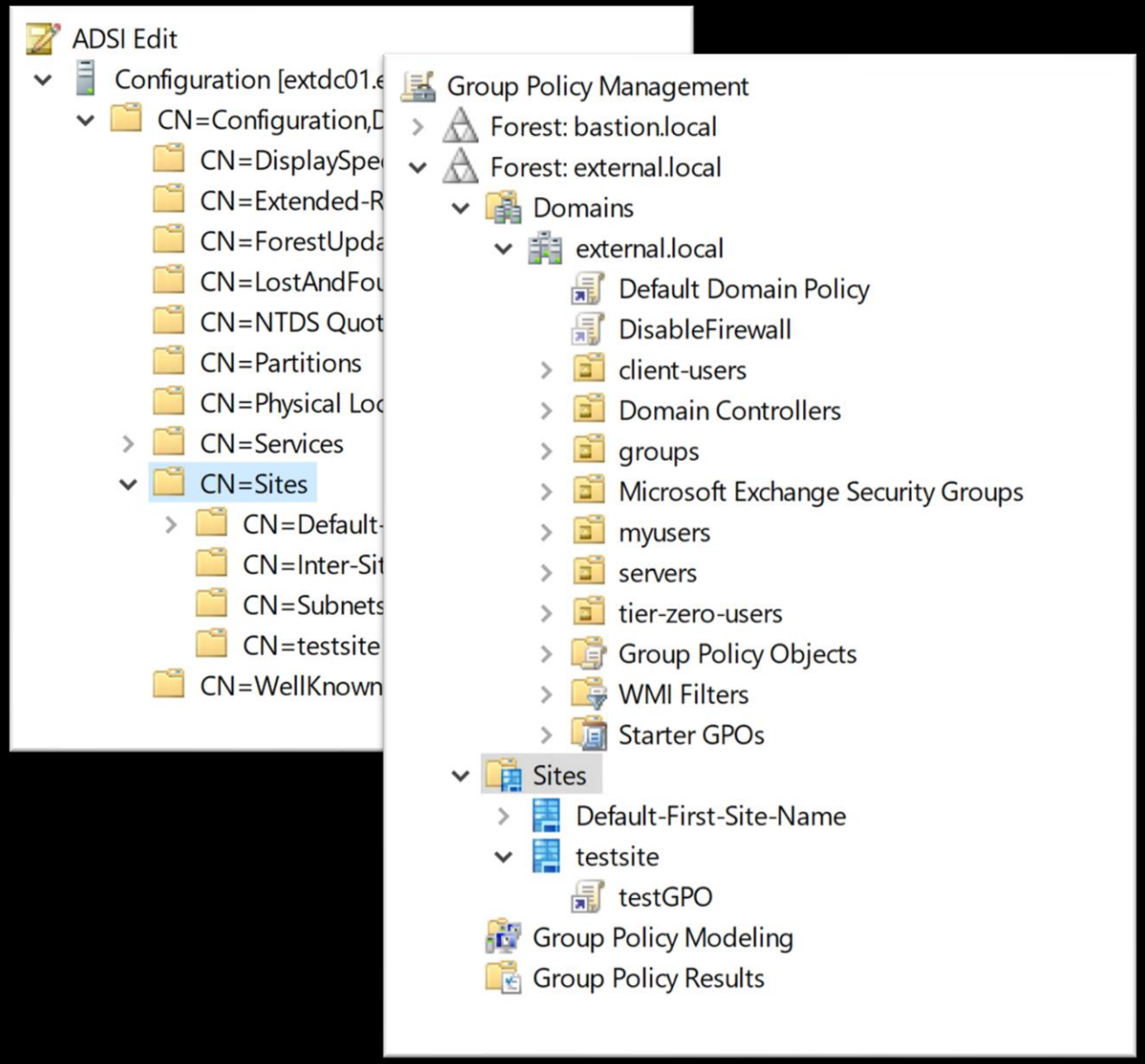
But run as SYSTEM on a DC and you can write to most objects



If Domain Admins only control their own domain,
why is the domain not a security boundary then?

1. Trusts within a forest has a weak configuration by default
    a. Weak SID filtering configuration – enables SID History Spoofing
    b. TGT delegation enabled – coerce T0 server and get it's TGT
2. Configuration NC is writeable from any writeable DC in the forest
    a. GPO linked on site

GPO linked on site



Sites contains DCs

GPOs can be linked to sites

Applies to the DCs and all computers and users connecting to the DCs

Attack: Create and link a GPO that gives to admin to the site of any DC within the forest

If Domain Admins only control their own domain,
why is the domain not a security boundary then?

1. Trusts within a forest has a weak configuration by default
    a. Weak SID filtering configuration – enables SID History Spoofing
    b. TGT delegation enabled – coerce T0 server and get it’s TGT
2. Configuration NC is writeable from any writeable DC in the forest
    a. GPO linked on site
    b. ADCS ESC5

ADCS ESC5

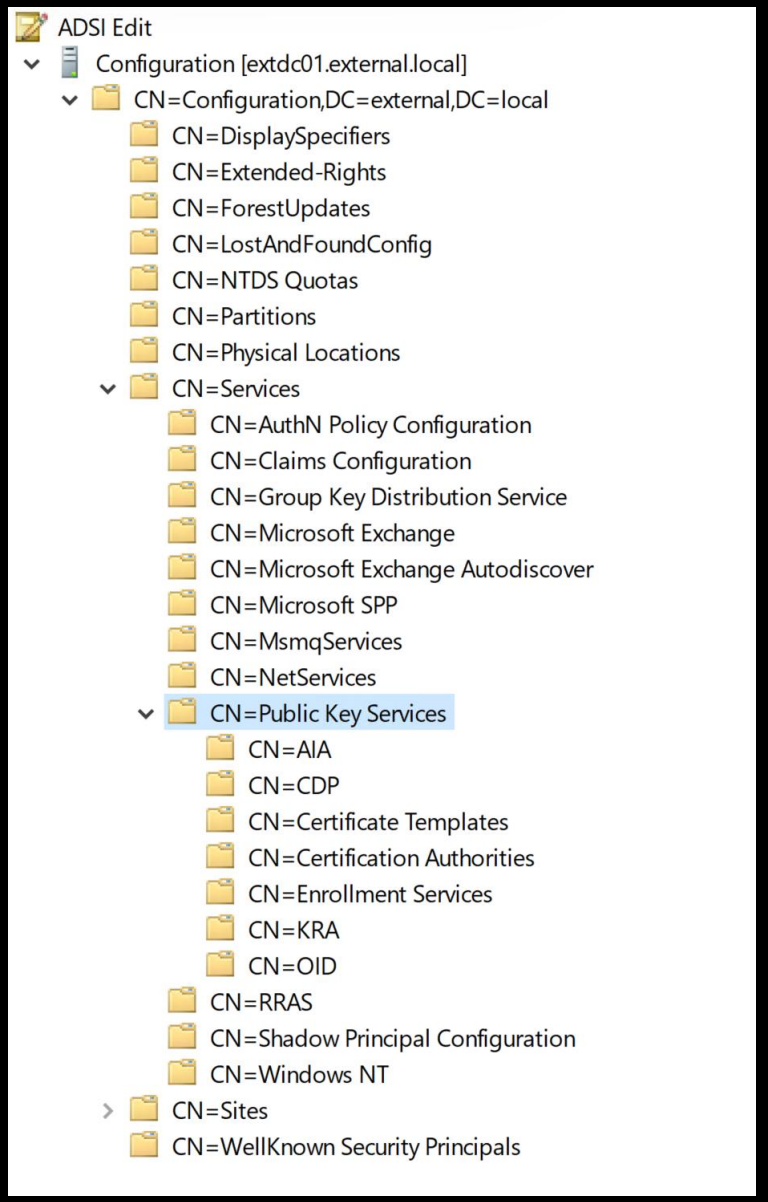
Attack steps:

1. Create a certificate template enabling ESC1
2. Publish the certificate template
3. Enroll the certificate as target user
4. Authenticate as target

From DA to EA with ESC5 by Andy Robbins

No ADCS? Deploy ADCS first

Escalating from child domain's admins to enterprise admins in 5 minutes by abusing AD CS, a follow up by Vadims Podāns



If Domain Admins only control their own domain,
why is the domain not a security boundary then?

1. Trusts within a forest has a weak configuration by default
    a. Weak SID filtering configuration – enables SID History Spoofing
    b. TGT delegation enabled – coerce T0 server and get it's TGT

2. Configuration NC is writeable from any writeable DC in the forest
    a. GPO linked on site
    b. ADCS ESC5

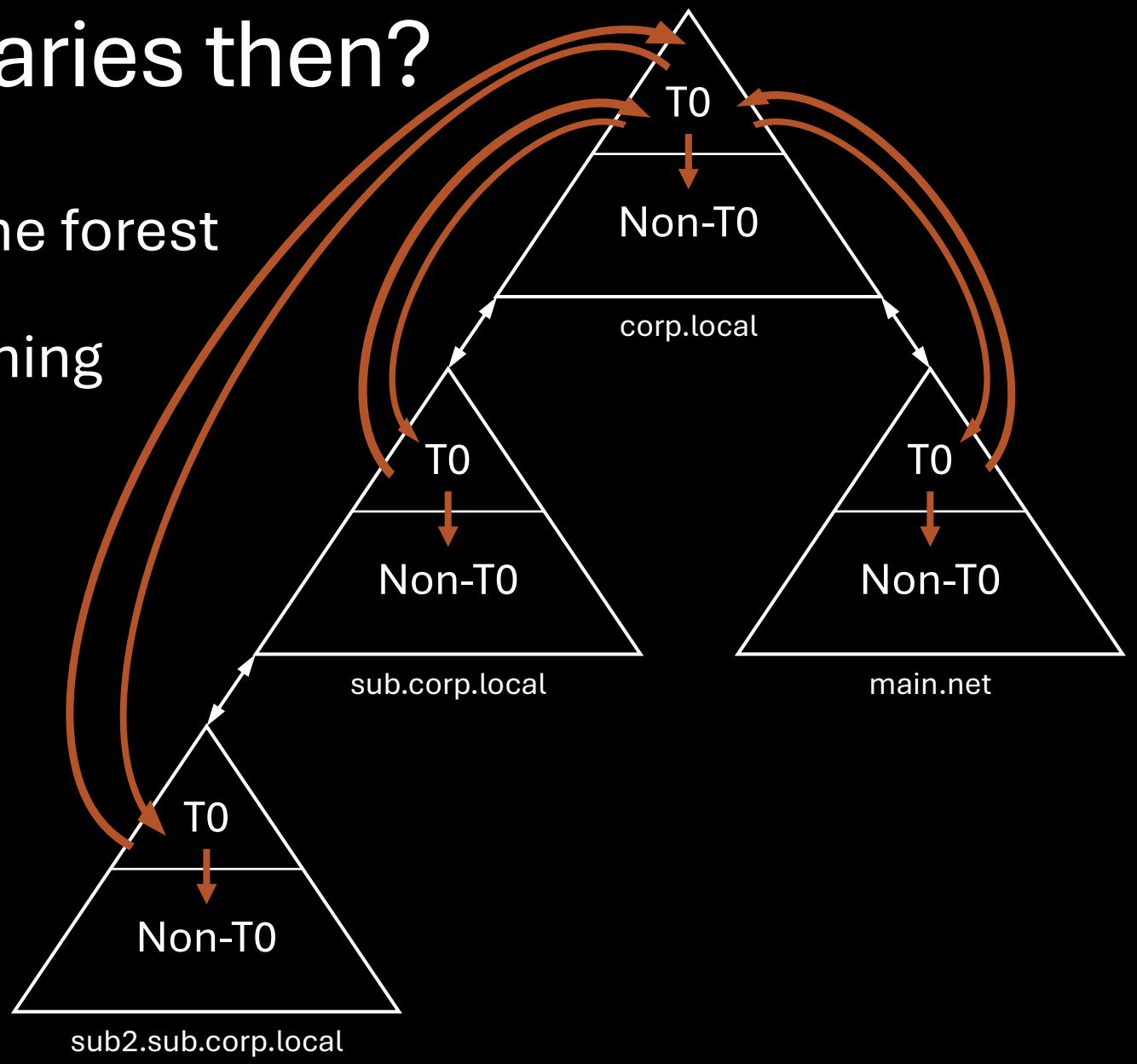
    Not feasible to prevent

Where are the boundaries then?

Tier Zero in any domain controls the forest

Non-Tier Zero cannot control anything by default

The forest should be seen as a unified whole, rather than as separate domains



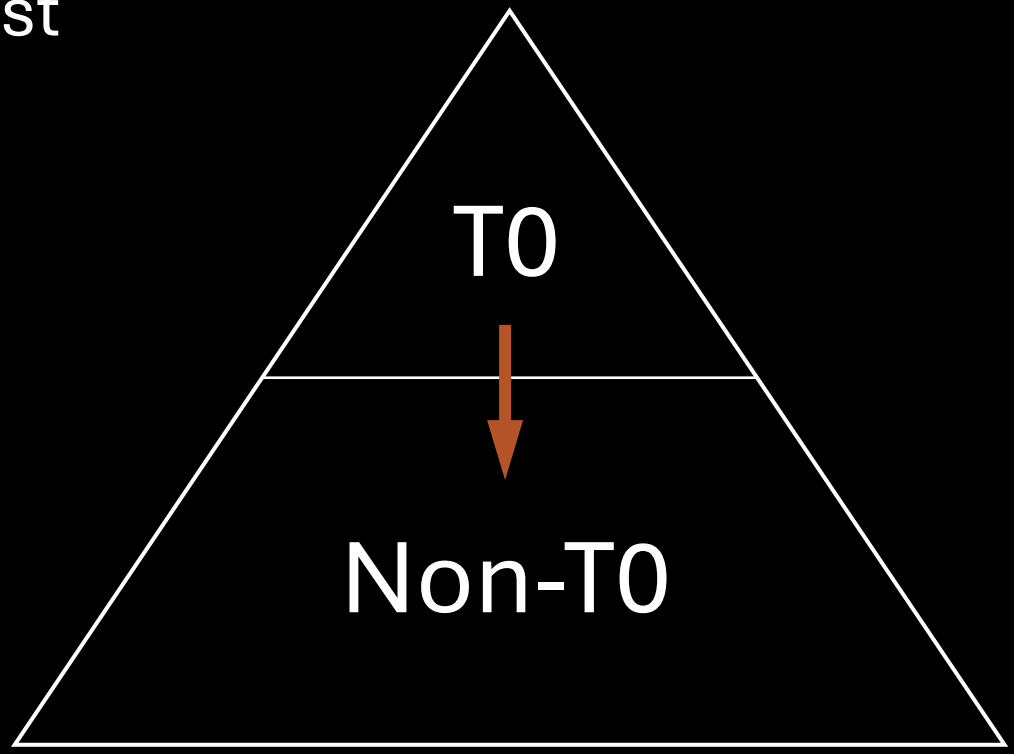
Where are the boundaries then?

Tier Zero in any domain controls the forest

Non-Tier Zero cannot control anything by default

The forest should be seen as a unified whole, rather than as separate domains

There can be endless Non-Tier Zero boundaries protecting objects from each other



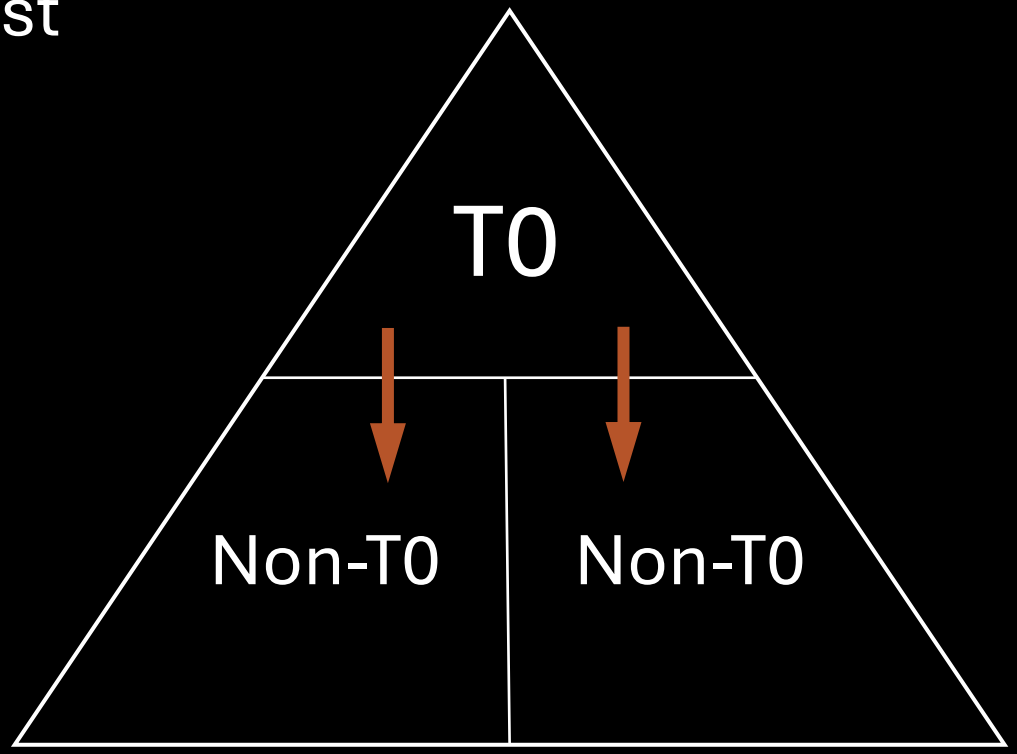
Where are the boundaries then?

Tier Zero in any domain controls the forest

Non-Tier Zero cannot control anything by default

The forest should be seen as a unified whole, rather than as separate domains

There can be endless Non-Tier Zero boundaries protecting objects from each other



AD domains and forests 101

Where are the boundaries then?

How security boundaries are violated

Audit for security boundary violations in BloodHound

How security boundaries are violated

Delegation of control

Indirect control - often not on purpose

- Linking a GPO to T0 computer
- Promoting a computer to DC
- Logging in with a T0 user on Non-T0 computer
- Usage of *AD Special Identities*

AD Special Identities

Common examples:

- Authenticated Users
- Everyone

Grants access to all principals **of the trusted domains**

Coercion + relay attacks 🔥

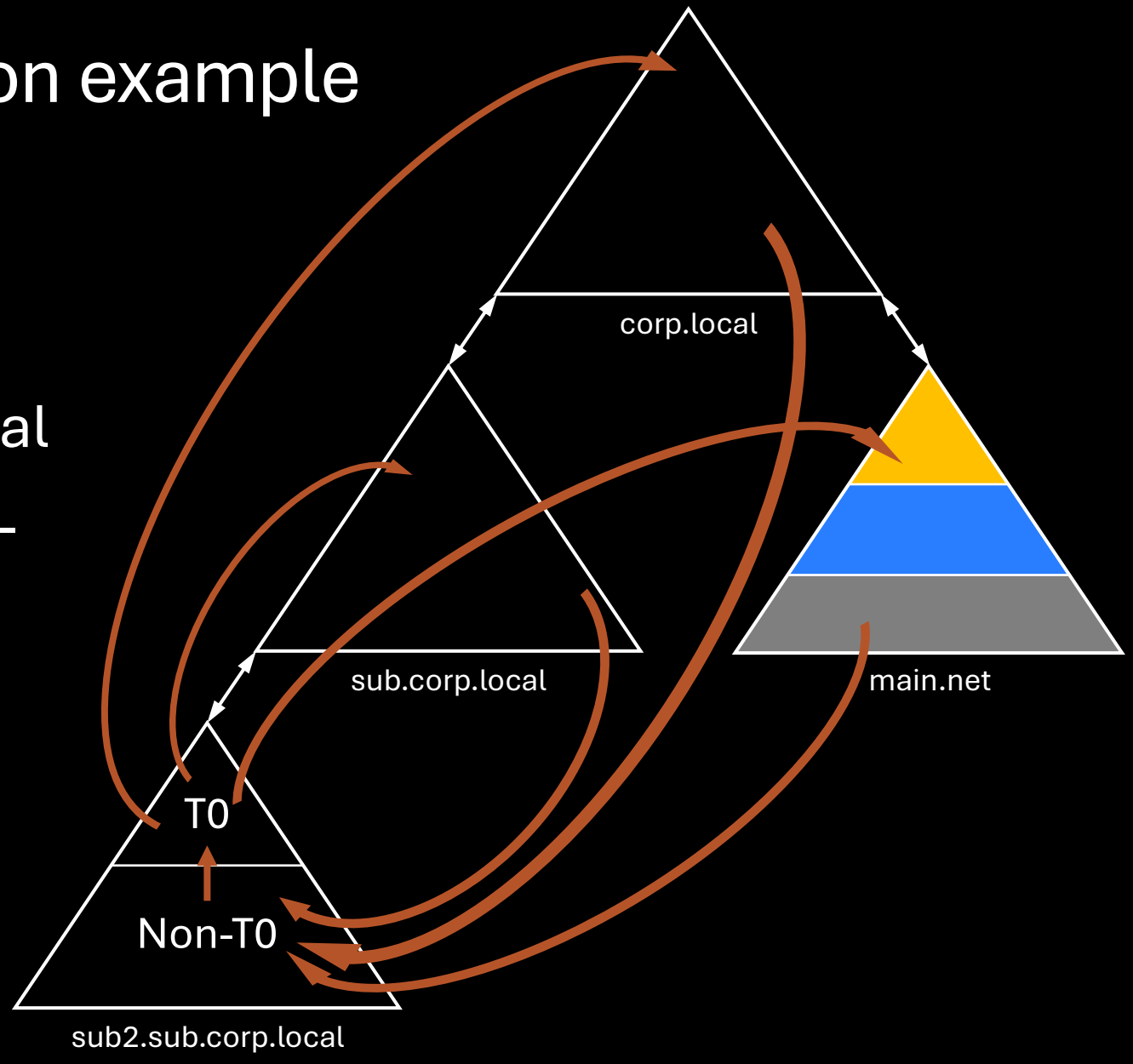
Security boundary violation example

main.net is perfectly tiered

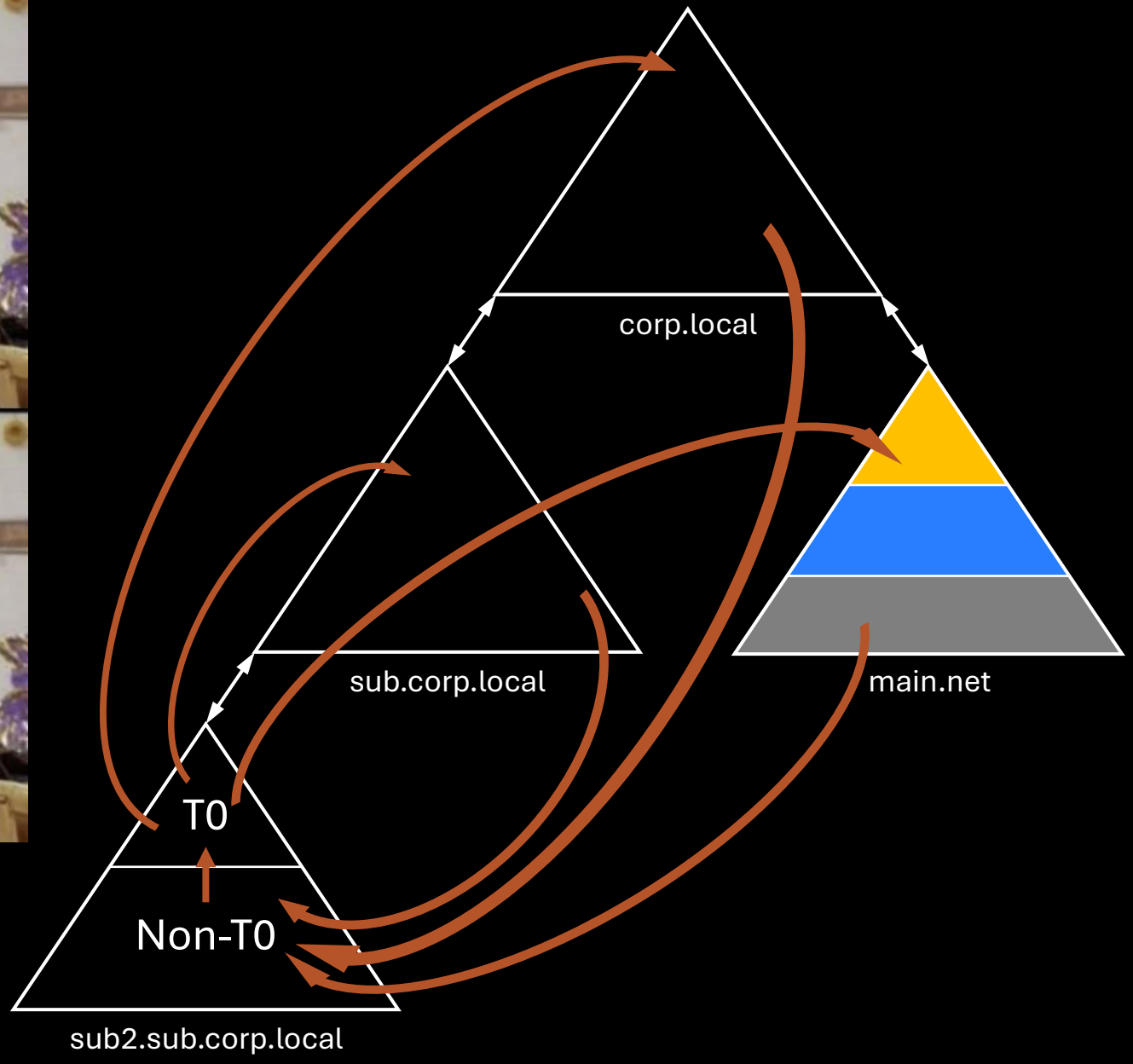
but Everyone has an attack path to Tier Zero in sub2.sub.corp.local

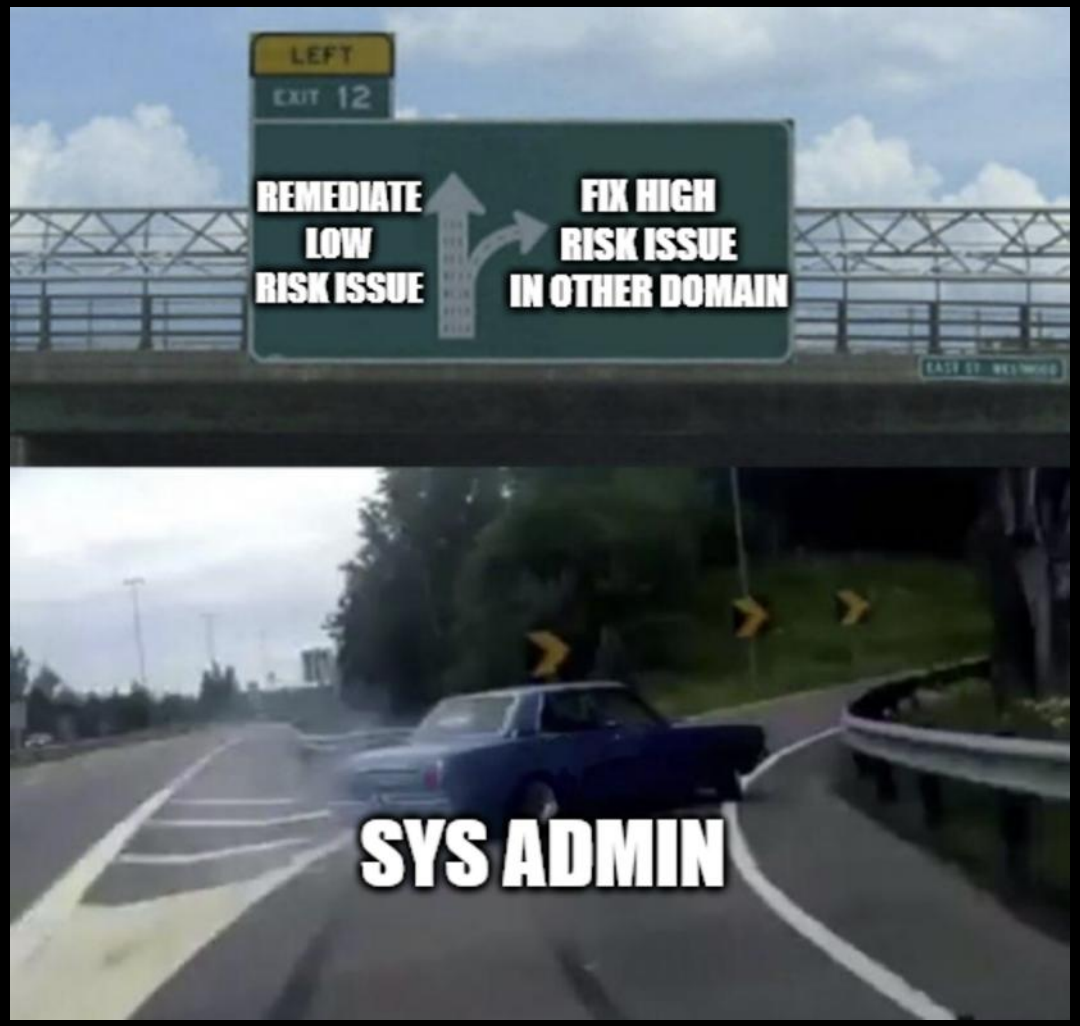
Everyone extends across trusts – 100% of the principals of the forest can compromise 100% of the domain

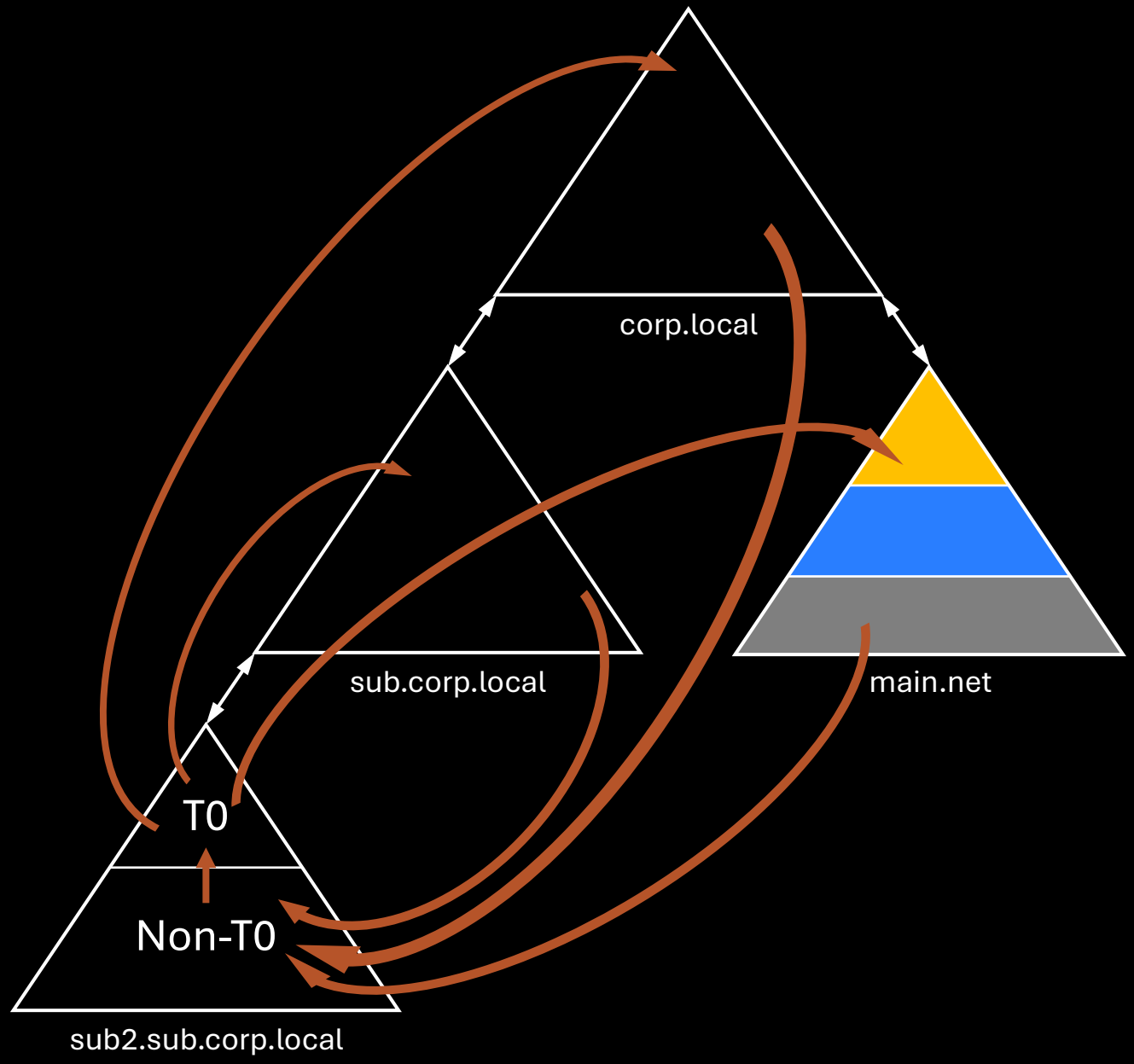
… and the forest




LOOKING AT MY TIERED AD DOMAIN
REALIZING IT CAN BE COMPROMISED BY EVERYONE


corp.local
sub.corp.local
main.net
T0
Non-T0
sub2.sub.corp.local


LEFT
EXIT 12
REMEDIATE LOW RISK ISSUE
FIX HIGH RISK ISSUE IN OTHER DOMAIN
SYS ADMIN


corp.local
sub.corp.local
main.net
T0
Non-T0
sub2.sub.corp.local

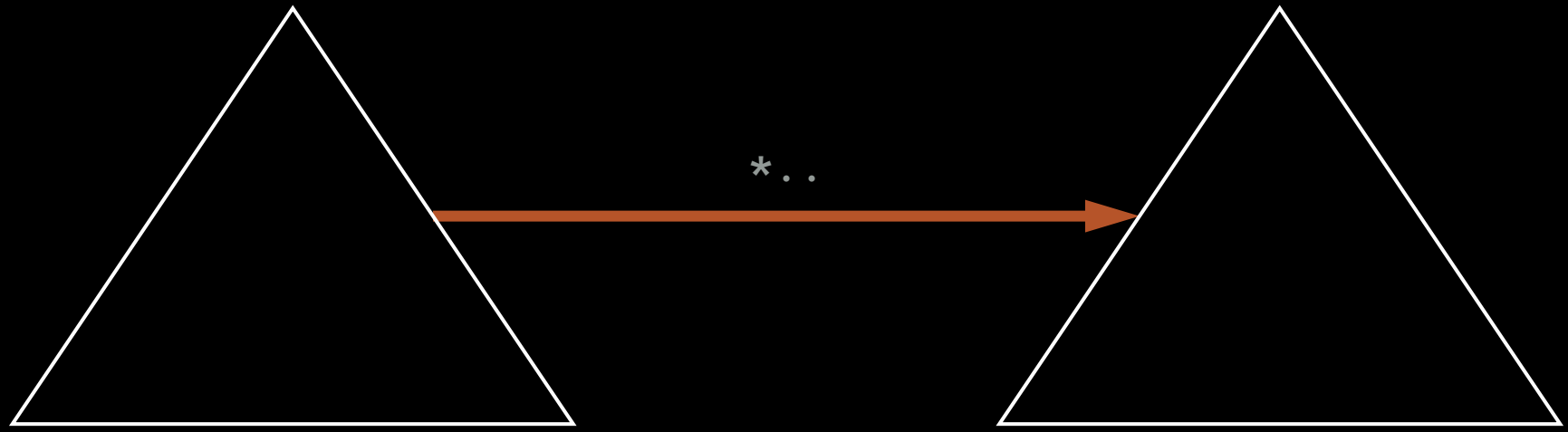
AD domains and forests 101

Where are the boundaries then?

How security boundaries are violated

Audit for security boundary violations in BloodHound

Cross domain paths



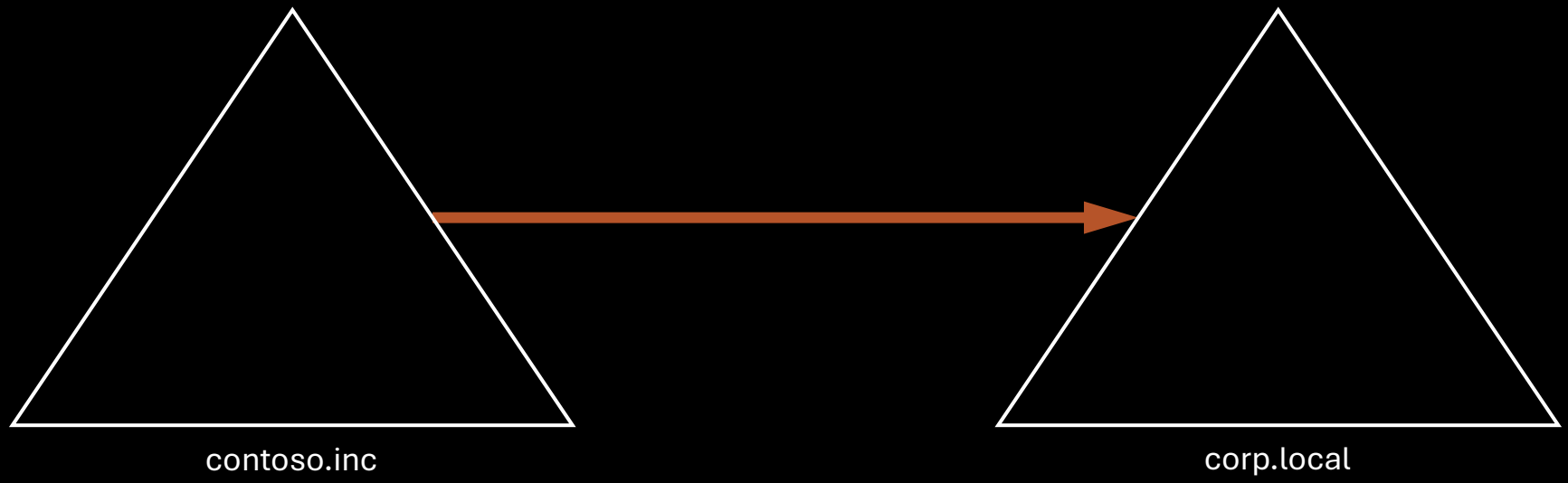

```
MATCH p = (x:Base)                    CKS*..]->(y:Base)
WHERE x.domain <> y.
RETURN p
```

Does not scale

Cross domain edges

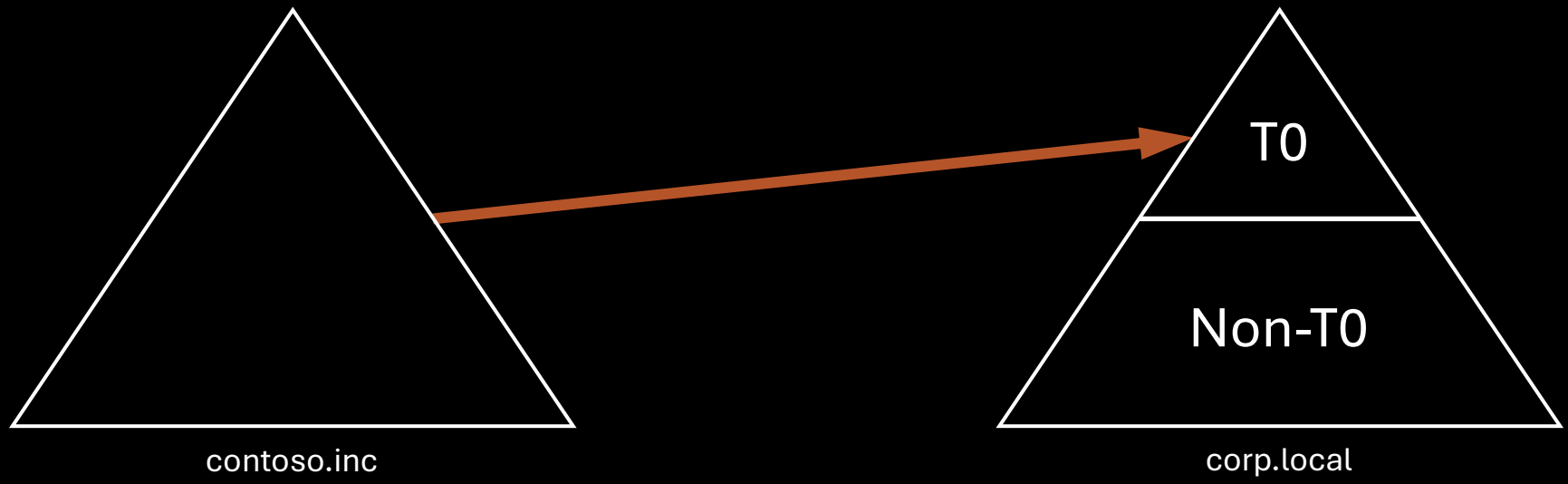
```
MATCH p = (x:Base)-[:AD_ATTACKS]->(y:Base)
WHERE x.domain <> y.domain
RETURN p
```

Cross domain edges



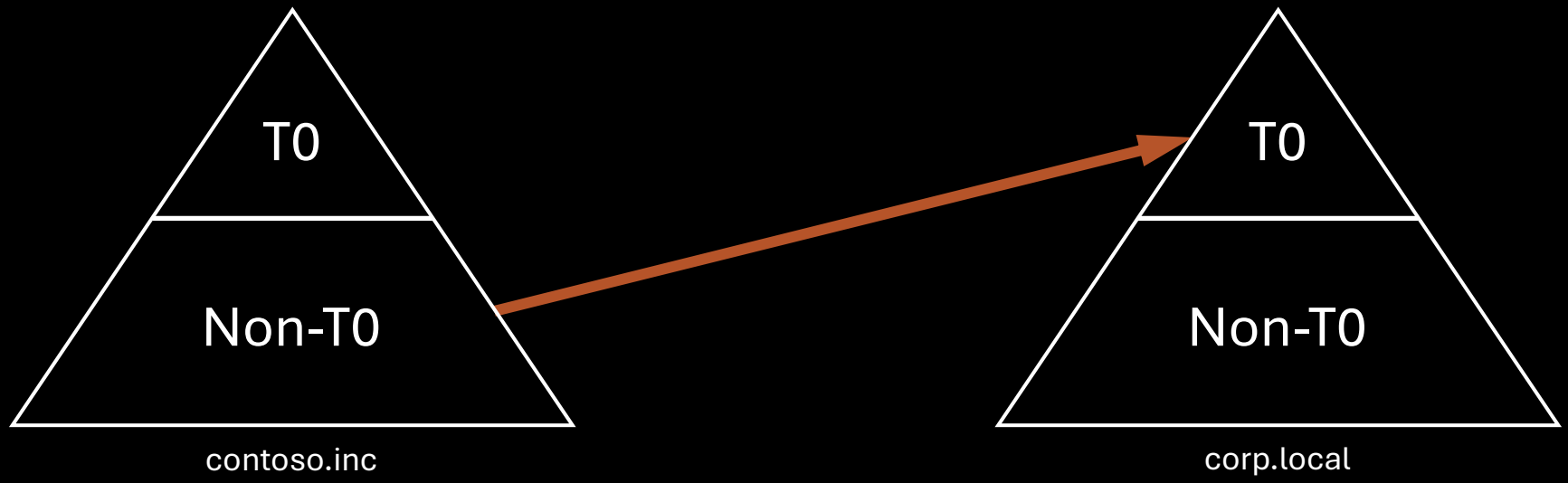

```
MATCH p = (x:Base)-[:AD_ATTACKS]->(y:Base)
WHERE x.domain = 'contoso.inc'
  AND y.domain = 'corp.local'
RETURN p
```

Cross domain edges to Tier Zero



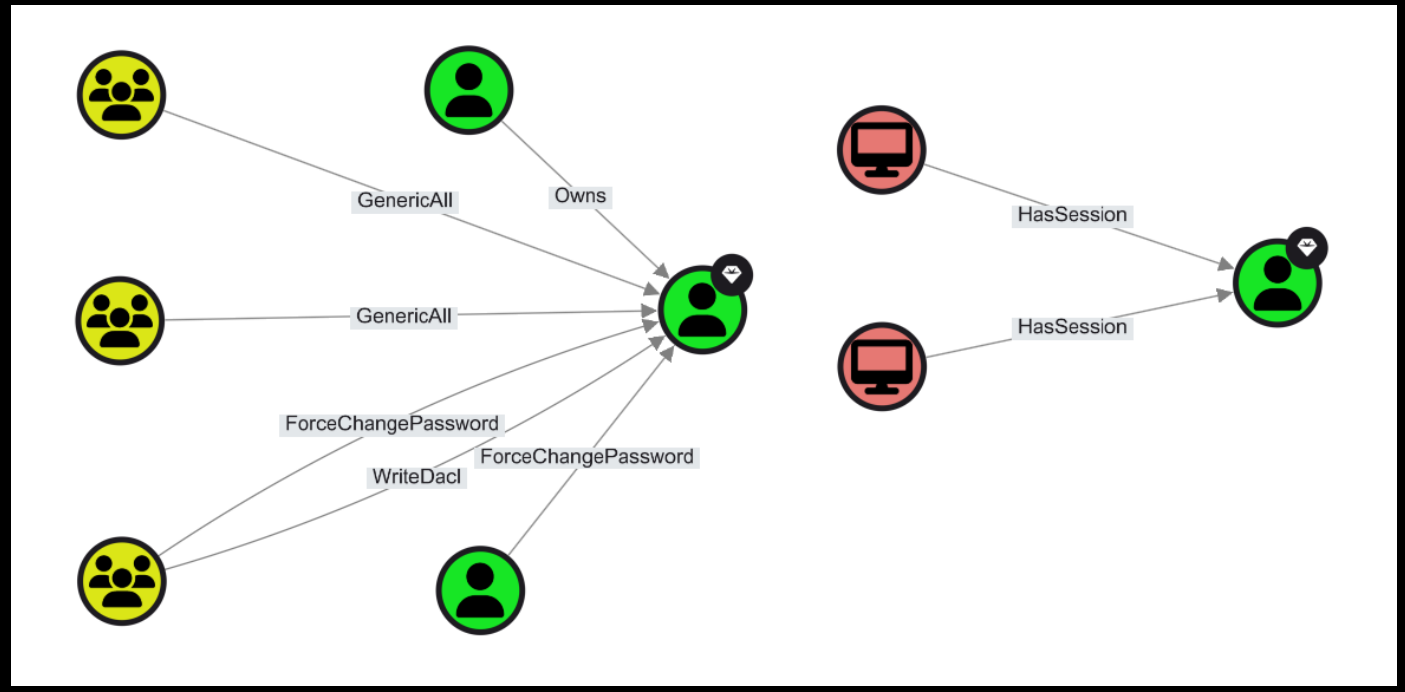

```
MATCH p = (x:Base)-[:AD_ATTACKS]->(y:Base)
WHERE x.domain = 'contoso.inc'
  AND y.domain = 'corp.local'
  AND y.system_tags CONTAINS 'admin_tier_0'
RETURN p
```

Cross domain edges from Non-Tier Zero to Tier Zero



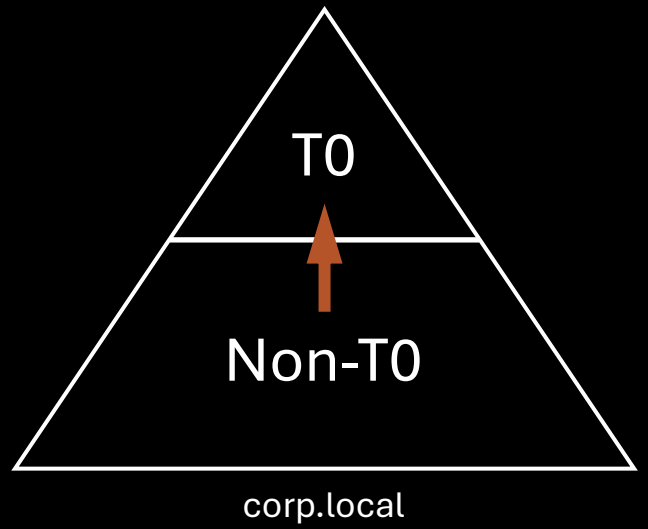
```
MATCH p = (x:Base)-[:AD_ATTACKS]->(y:Base)
WHERE x.domain = 'contoso.inc'
  AND y.domain = 'corp.local'
  AND y.system_tags CONTAINS 'admin_tier_0'
  AND NOT COALESCE(x.system_tags, '') CONTAINS 'admin_tier_0'
RETURN p
```

Cross domain edges from Non-Tier Zero to Tier Zero



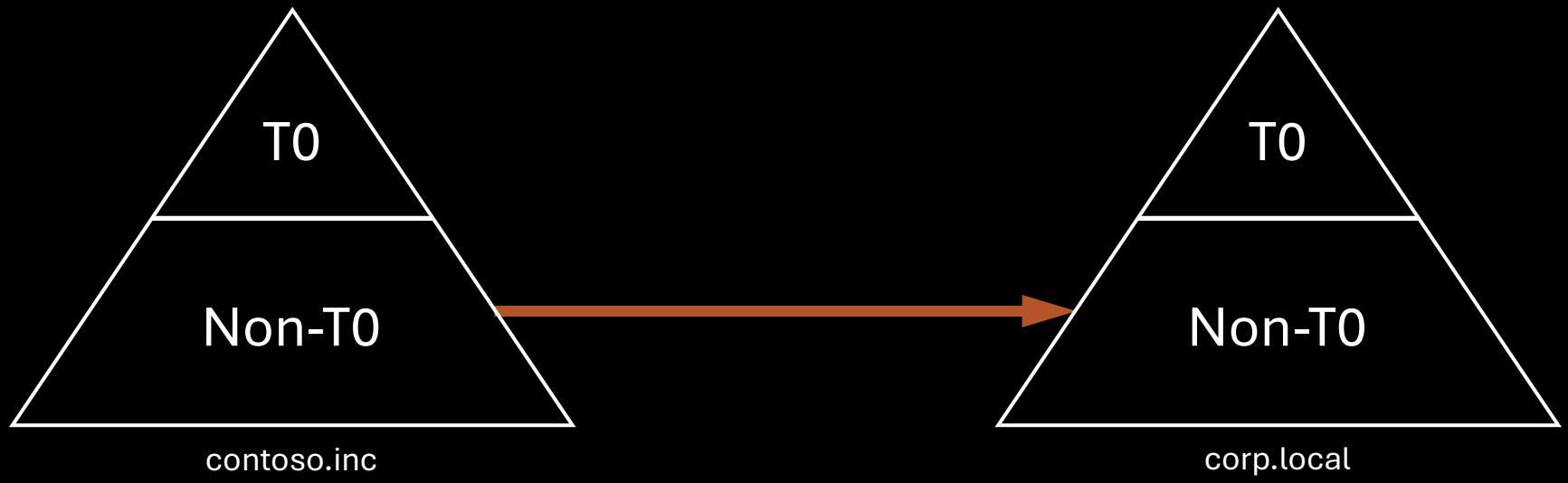
```
MATCH p = (x:Base)-[:AD_ATTACKS]->(y:Base)
WHERE x.domain = 'contoso.inc'
  AND y.domain = 'corp.local'
  AND y.system_tags CONTAINS 'admin_tier_0'
  AND NOT COALESCE(x.system_tags, '') CONTAINS 'admin_tier_0'
RETURN p
```

Local domain edges from Non-Tier Zero to Tier Zero



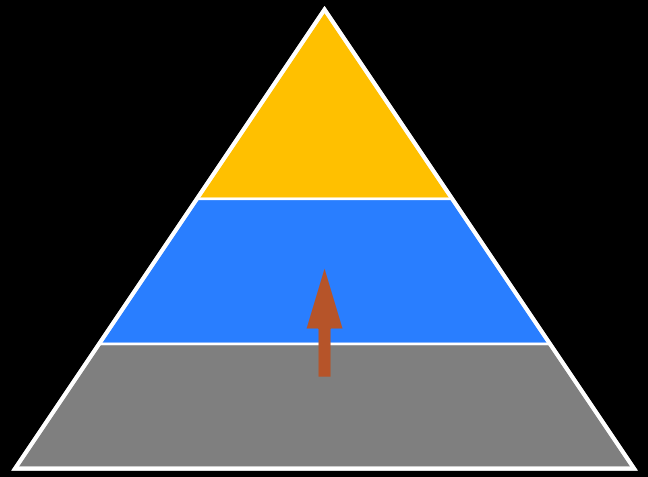
```
MATCH p = (x:Base)-[:AD_ATTACKS]->(y:Base)
WHERE x.domain = 'corp.local'
  AND y.domain = x.domain
  AND y.system_tags CONTAINS 'admin_tier_0'
  AND NOT COALESCE(x.system_tags, '') CONTAINS 'admin_tier_0'
RETURN p
```

Cross domain edges from Non-Tier Zero to Non-Tier Zero



```
MATCH p = (x:Base)-[:AD_ATTACKS]->(y:Base)
WHERE x.domain = 'contoso.inc'
  AND y.domain = 'corp.local'
  AND NOT COALESCE(x.system_tags, '') CONTAINS 'admin_tier_0'
  AND NOT COALESCE(y.system_tags, '') CONTAINS 'admin_tier_0'
RETURN p
```

Edges crossing Non-Tier Zero boundary



```
MATCH p = (x:Base)-[:AD_ATTACKS]->(y:Base)
WHERE x.distinguishedname ENDS WITH 'OU=T2,DC=CORP,DC=LOCAL'
WHERE y.distinguishedname ENDS WITH 'OU=T1,DC=CORP,DC=LOCAL'
RETURN p
```

```
AD_ATTACKS =
Contains|Owns|GenericAll|GenericWrite|WriteOwner|WriteDacl
|MemberOf|ForceChangePassword|AllExtendedRights|AddMember|
HasSession|GPLink|AllowedToDelegate|TrustedBy|AllowedToAct
|AdminTo|CanPSRemote|CanRDP|ExecuteDCOM|HasSIDHistory|AddS
elf|DCSync|ReadLAPSPassword|ReadGMSAPassword|DumpSMSAPassw
ord|SQLAdmin|AddAllowedToAct|WriteSPN|AddKeyCredentialLink
|SyncLAPSPassword|WriteAccountRestrictions|WriteGPLink|Man
ageCA|ManageCertificates|GoldenCert|ADCSESC1|ADCSESC3|ADCS
ESC4|ADCSESC5|ADCSESC6a|ADCSESC6b|ADCSESC7|ADCSESC9a|ADCSE
SC9b|ADCSESC10a|ADCSESC10b|ADCSESC13|DCFor|CoerceToTGT|Coe
rceAndRelayNTLMToSMB|CoerceAndRelayNTLMToADCS|CoerceAndRel
ayNTLMToADCS|CoerceAndRelayNTLMToLDAP|CoerceAndRelayNTLMTo
LDAPS|WriteOwnerLimitedRights|OwnsLimitedRights
```

Key takeaways

Domain Admins of a child domain has indirect control of the entire AD forest – you cannot prevent that

Ensure equal protection of Tier Zero – across all domains

Authenticated Users and Everyone are all principals in the forest

Auditors – Remember to look for paths through other domains

SPECTEROPS

Thank you