
SBA
Research

COMET

Competence Centers for
Excellent Technologies

Vertrauen ist gut, Pentests sind besser

Sicherheitsprobleme in Active Directory Forests (Star Wars Edition)

Bundesministerium Verkehr, Innovation und Technologie

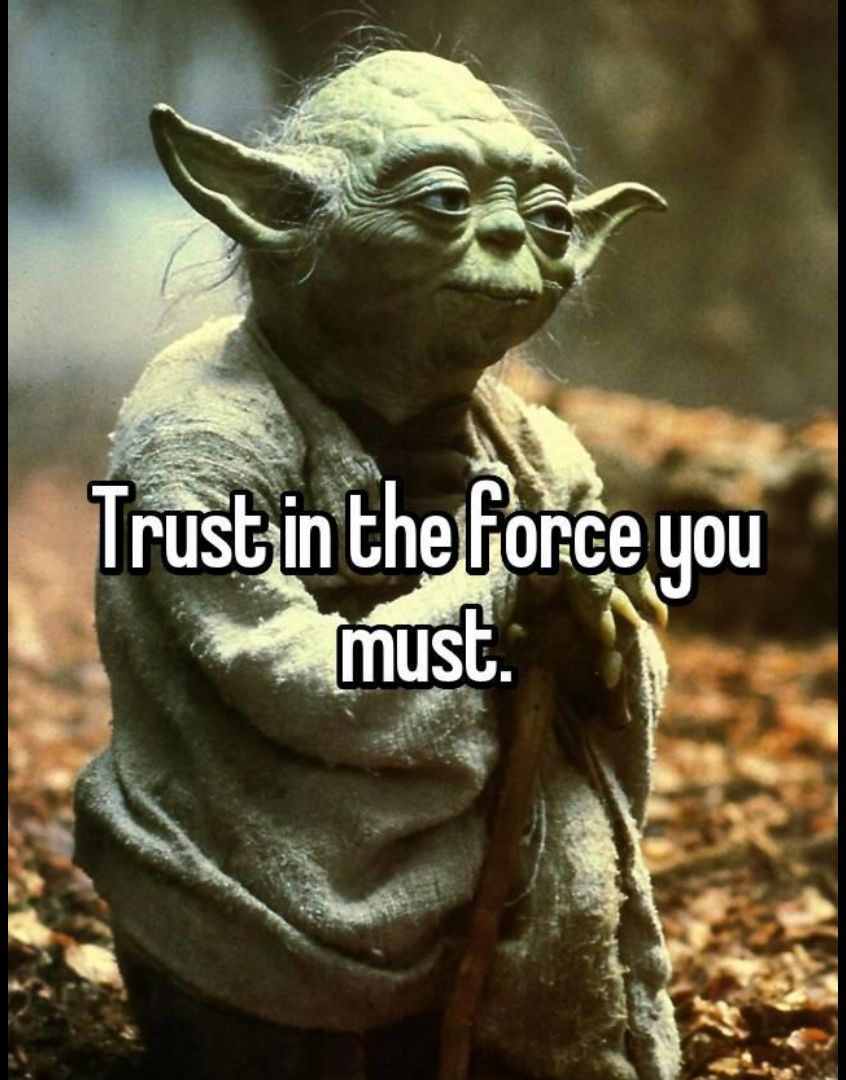
Bundesministerium Digitalisierung und Wirtschaftsstandort

FFG Forschung wirkt.

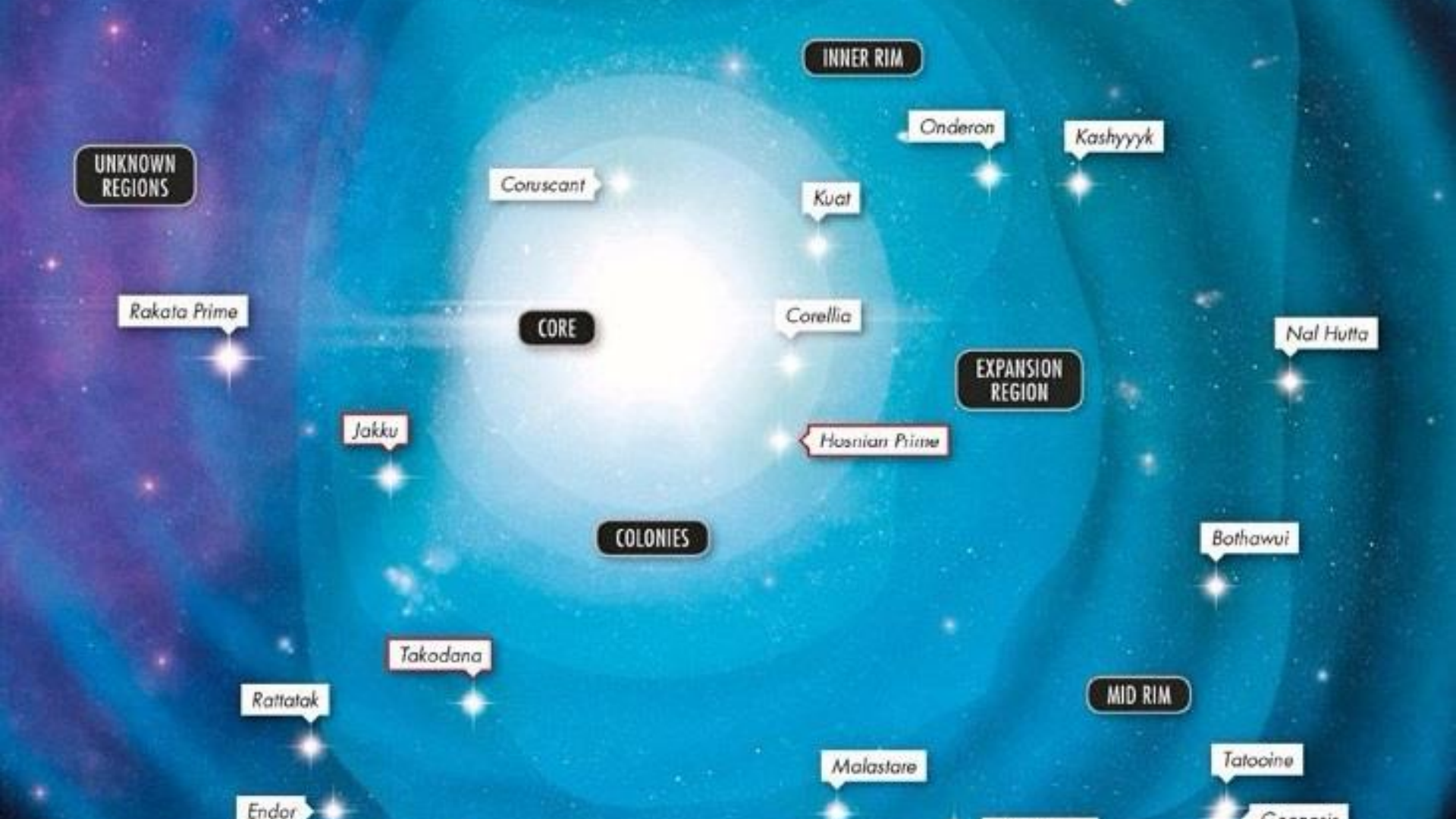
wirtschaftsagentur wien Ein Fonds der Stadt Wien

FWF Der Wissenschaftsfonds.

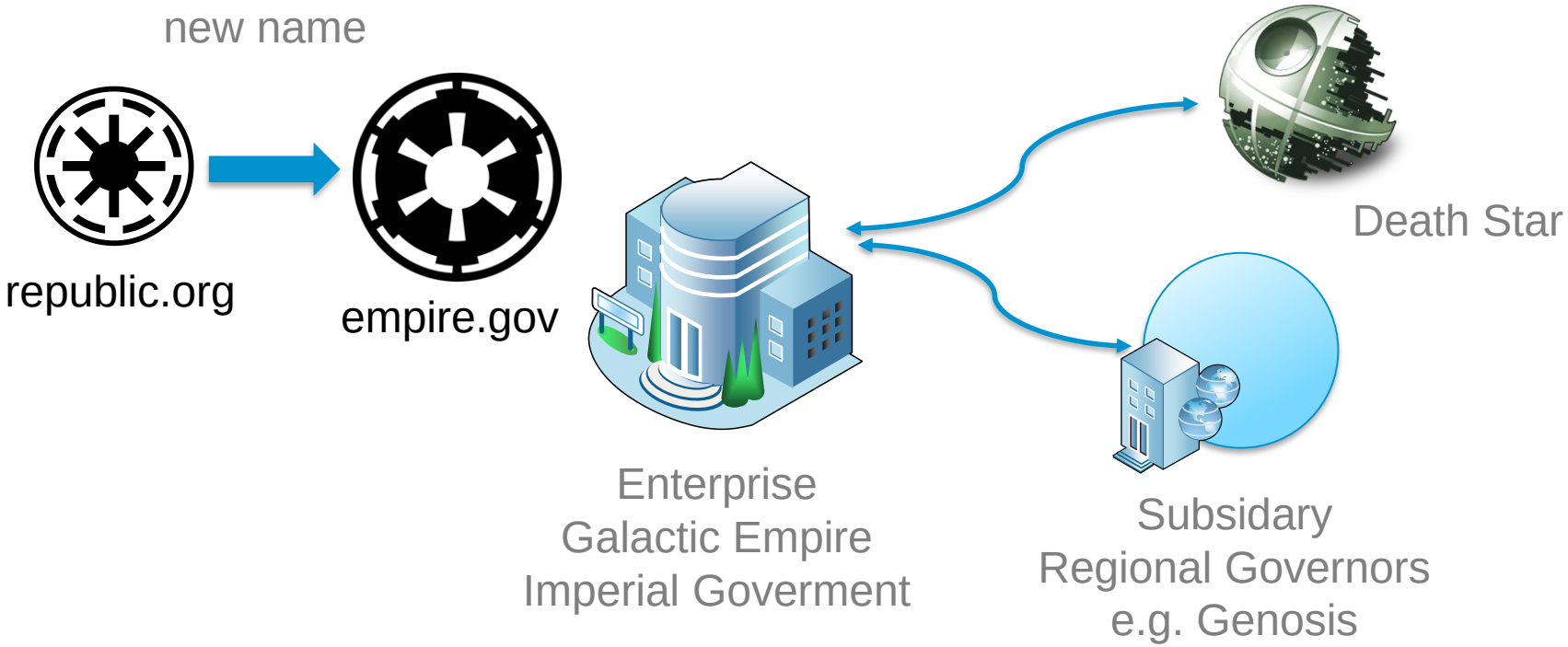
netidee OPEN INNOVATIONS


Trust in the force you must.

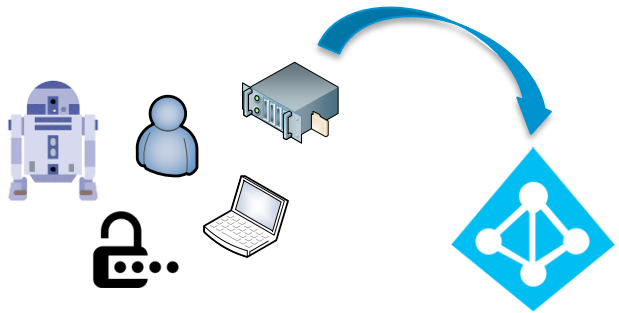
20th Century Fox ; Lucasfilm Ltd. ; written and directed by George Lucas ; produced by Rick McCallum. Star Wars. Episode III, Revenge of the Sith. Beverly Hills, Calif. :20th Century Fox Home Entertainment, 2013.

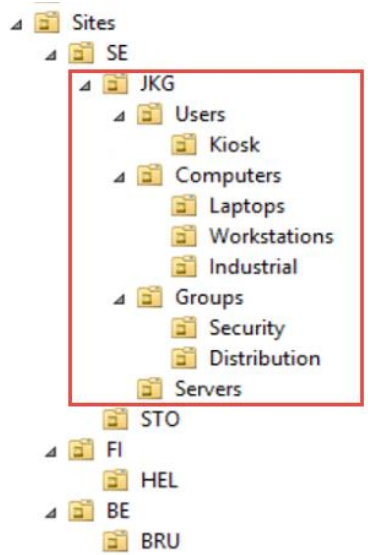

INNER RIM
Onderon
Kashyyyk
UNKNOWN REGIONS
Coruscant
Kuat
Rakata Prime
CORE
Corellia
Nal Hutta
EXPANSION REGION
Jakku
Hosnian Prime
COLONIES
Bothawui
Takodana
Rattatak
MID RIM
Malastare
Tatooine
Endor

Merger: Sharing Ressources



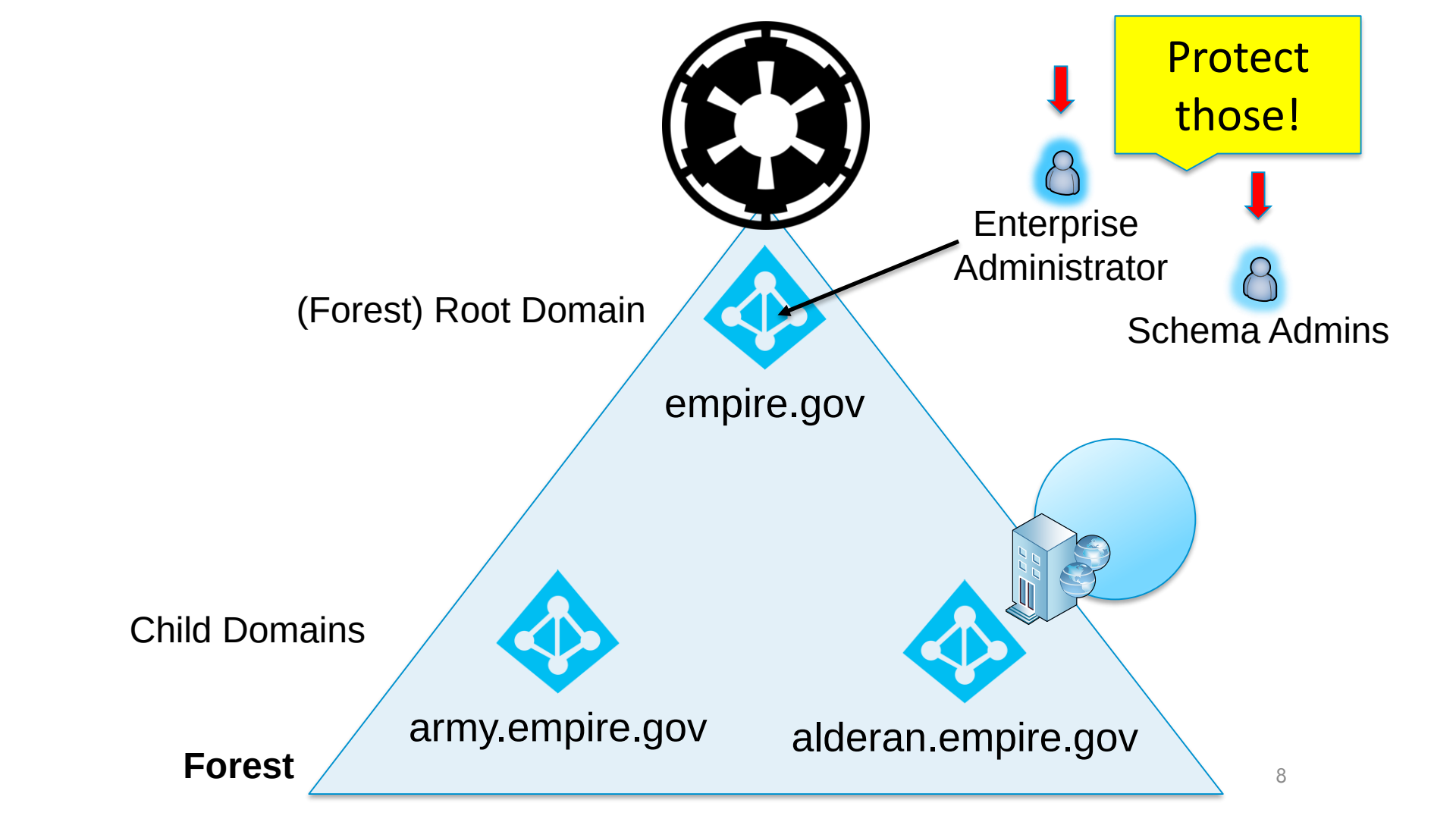
Domain

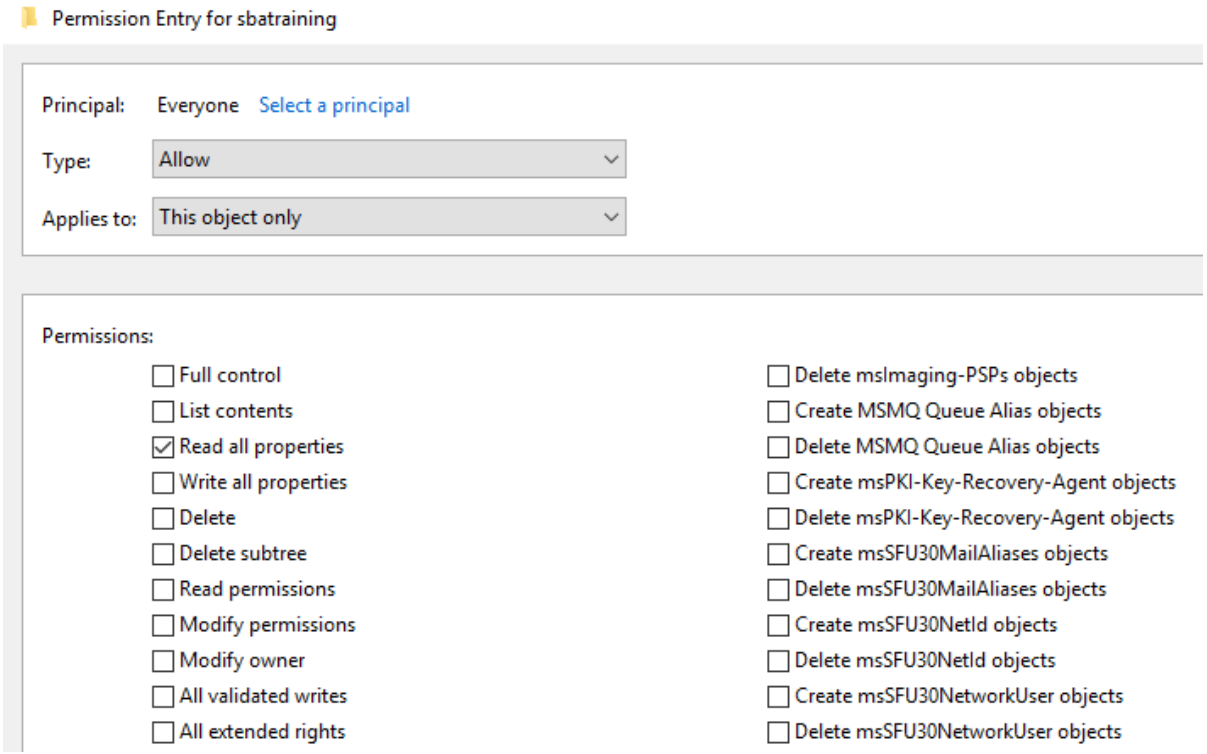




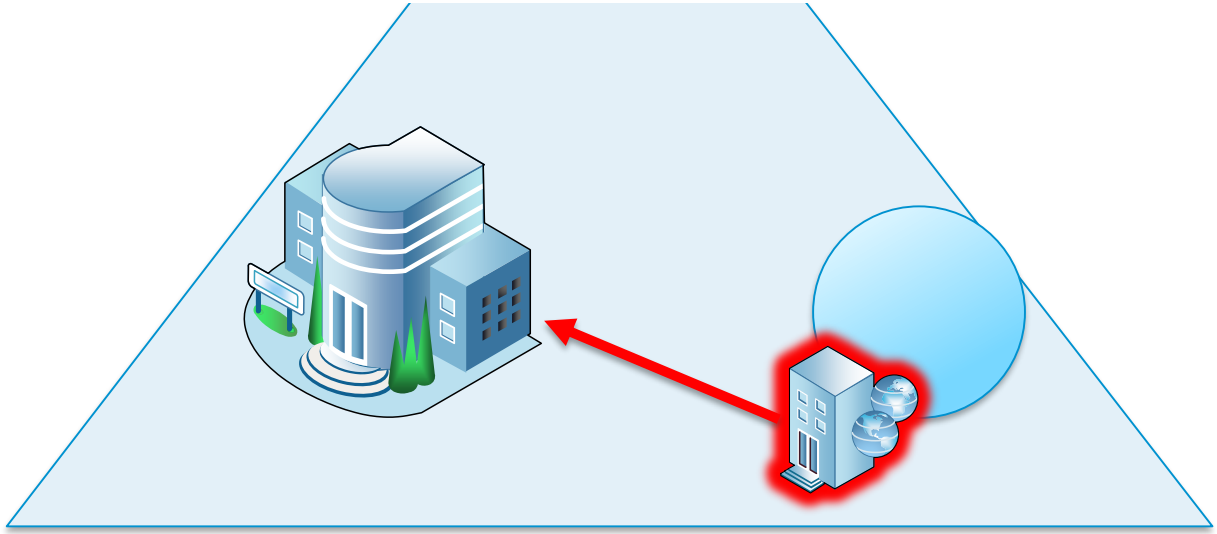
Domains are container objects. Domains are a collection of administratively defined objects that share a common directory database

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759073(v=ws.10)

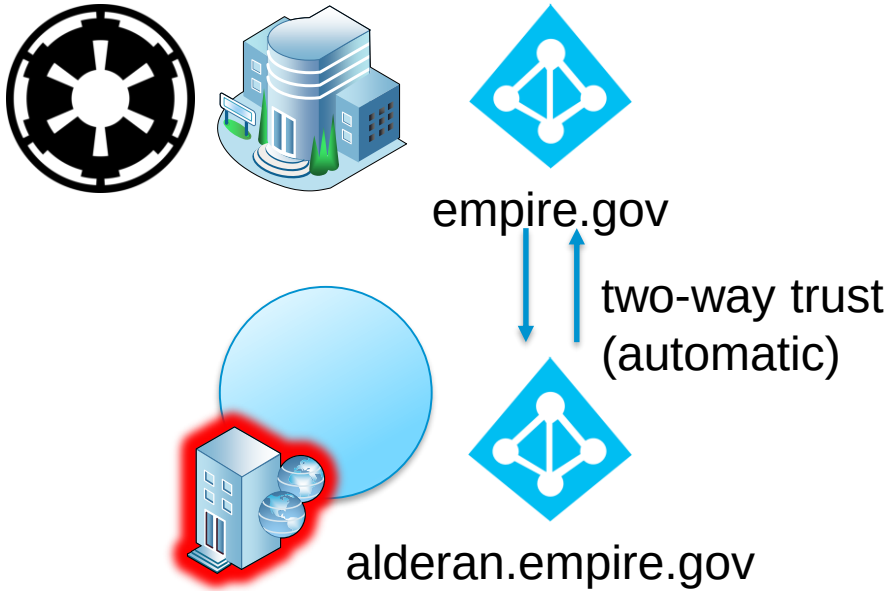

Protect those!
Enterprise Administrator
Schema Admins
(Forest) Root Domain
empire.gov
Child Domains
army.empire.gov
alderan.empire.gov
Forest

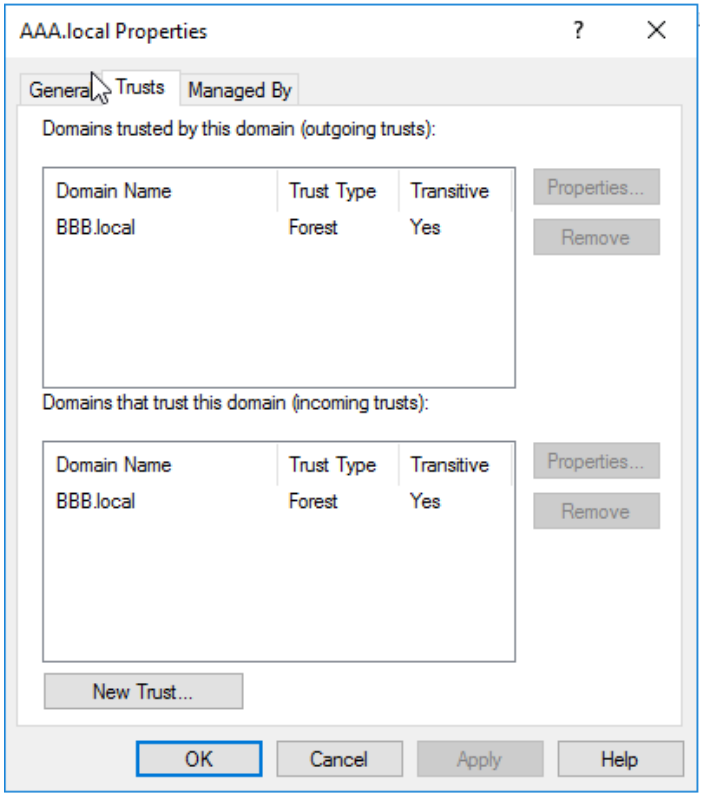

Permission Entry for sbatraining
Principal: Everyone Select a principal
Type: Allow
Applies to: This object only
Permissions:
Full control
List contents
Read all properties
Write all properties
Delete
Delete subtree
Read permissions
Modify permissions
Modify owner
All validated writes
All extended rights
Delete msImaging-PSPs objects
Create MSMQ Queue Alias objects
Delete MSMQ Queue Alias objects
Create msPKI-Key-Recovery-Agent objects
Delete msPKI-Key-Recovery-Agent objects
Create msSFU30MailAliases objects
Delete msSFU30MailAliases objects
Create msSFU30NetId objects
Delete msSFU30NetId objects
Create msSFU30NetworkUser objects
Delete msSFU30NetworkUser objects

Threat model: Subdomain Compromized, is the Root Domain in Danger?



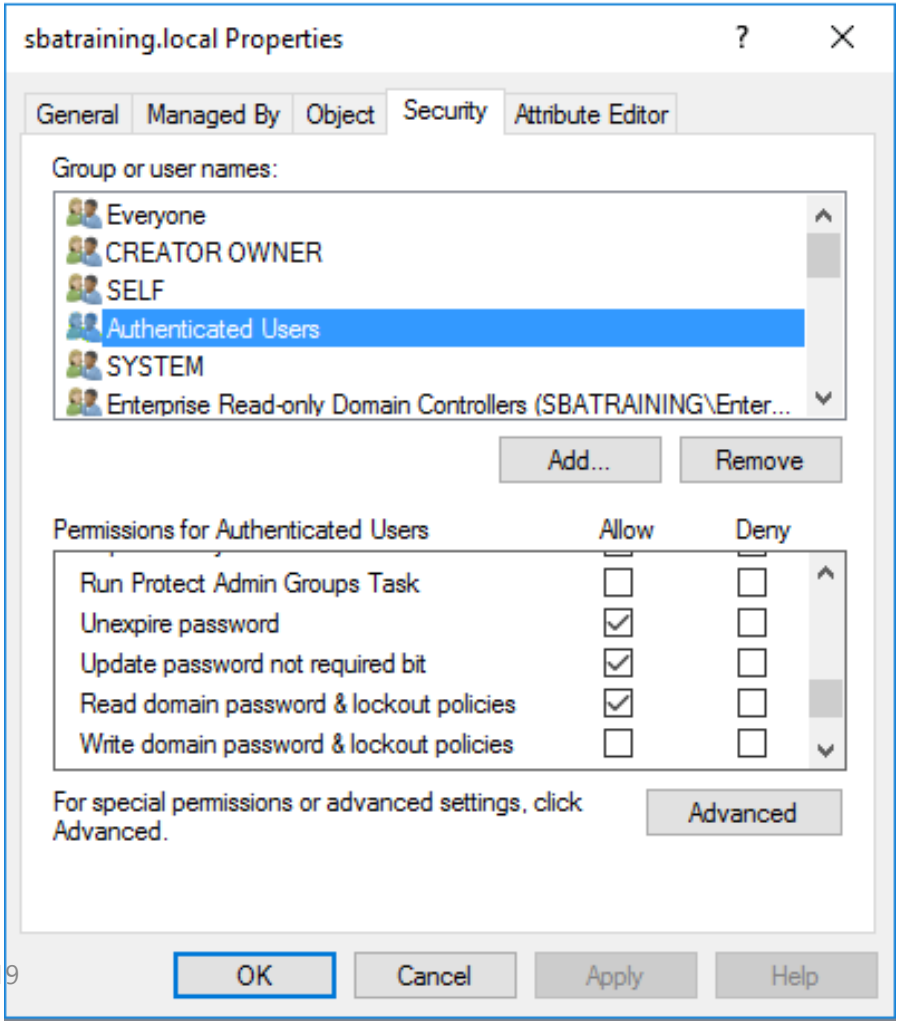
Subdomain Trust Relation



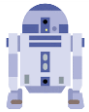


"Each time you create a new domain container in a forest, a two-way, transitive trust relationship is automatically created between the new domain and its parent domain."

empire.gov


sbatraining.local Properties
?
General
Managed By
Object
Security
Attribute Editor
Group or user names:
Everyone
CREATOR OWNER
SELF
Authenticated Users
SYSTEM
Enterprise Read-only Domain Controllers (SBATRAINING\Enter...
Add...
Remove
Permissions for Authenticated Users
Allow
Deny
Run Protect Admin Groups Task
Unexpire password
Update password not required bit
Read domain password & lockout policies
Write domain password & lockout policies
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply
Help

S-1-5-21-124525095-708259637-1543119021-2097



Kerberos Ticket

Subject

User's Access Token

- User SID
- Group SIDs
- List of Privileges
- Other Access Information

Object

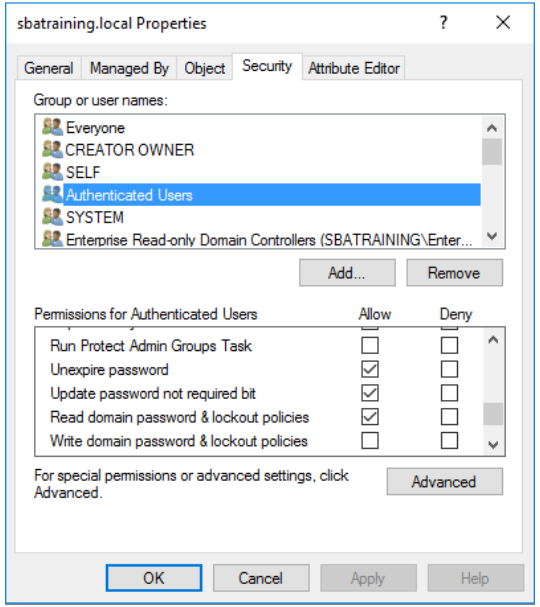
Object's Security Descriptor

- Object Owner SID
- Group SID
- SACL
  - System ACL
  - ACE
  - ACE
  - ACE
- DACL
  - ACE
  - ACE
  - ACE
  - ACE
  - .
  - .

System performs access check

Each ACE is examined until a match is found

Access decision is made



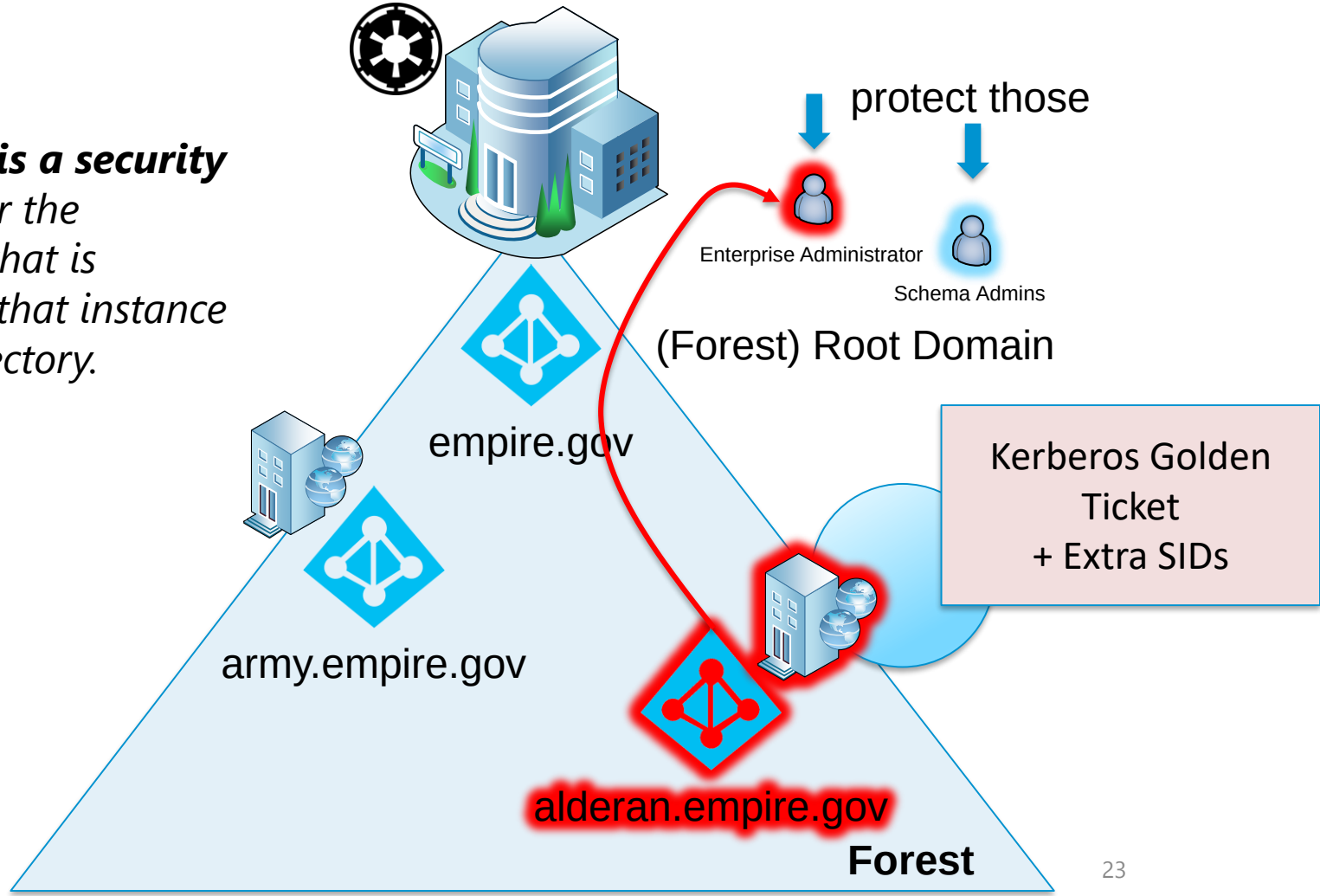
https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/security-principals

Active Directory Migration: SidHistory

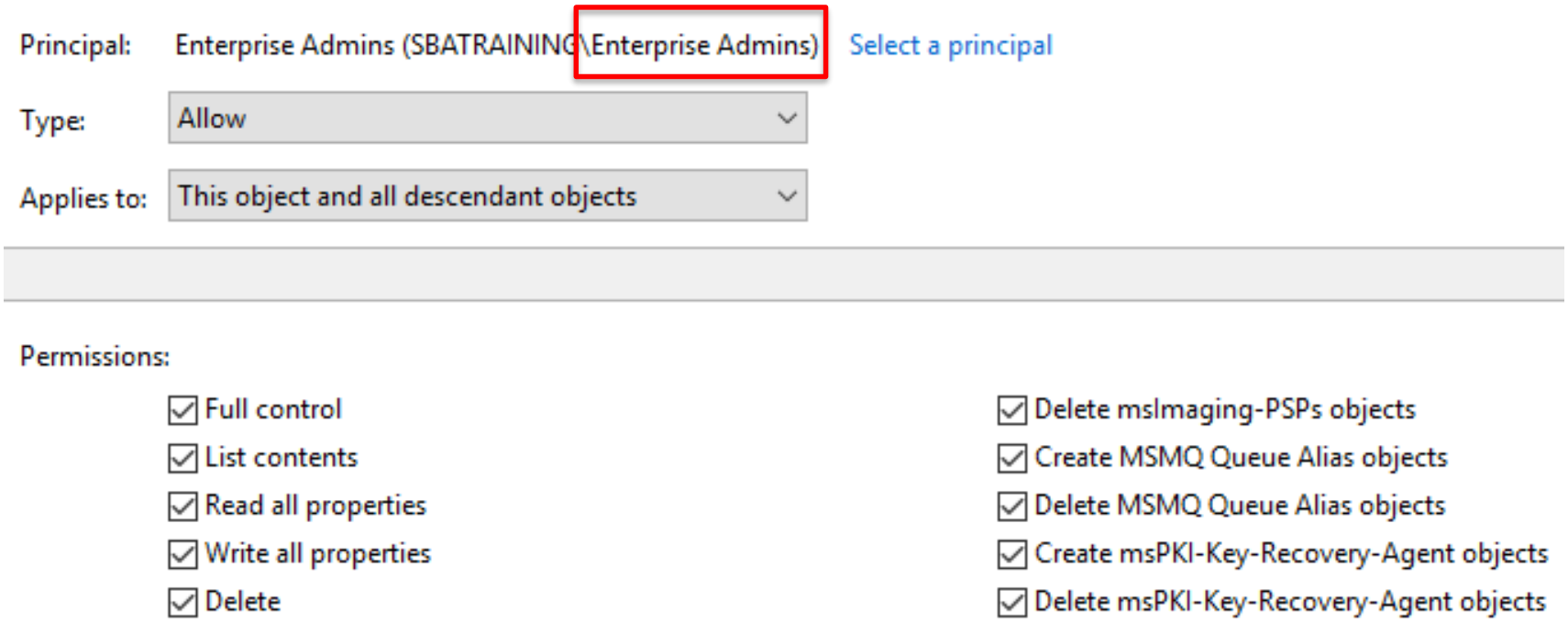
Objects are migrated into the new domain.
Not yet migrated users have access using the old SIDs.

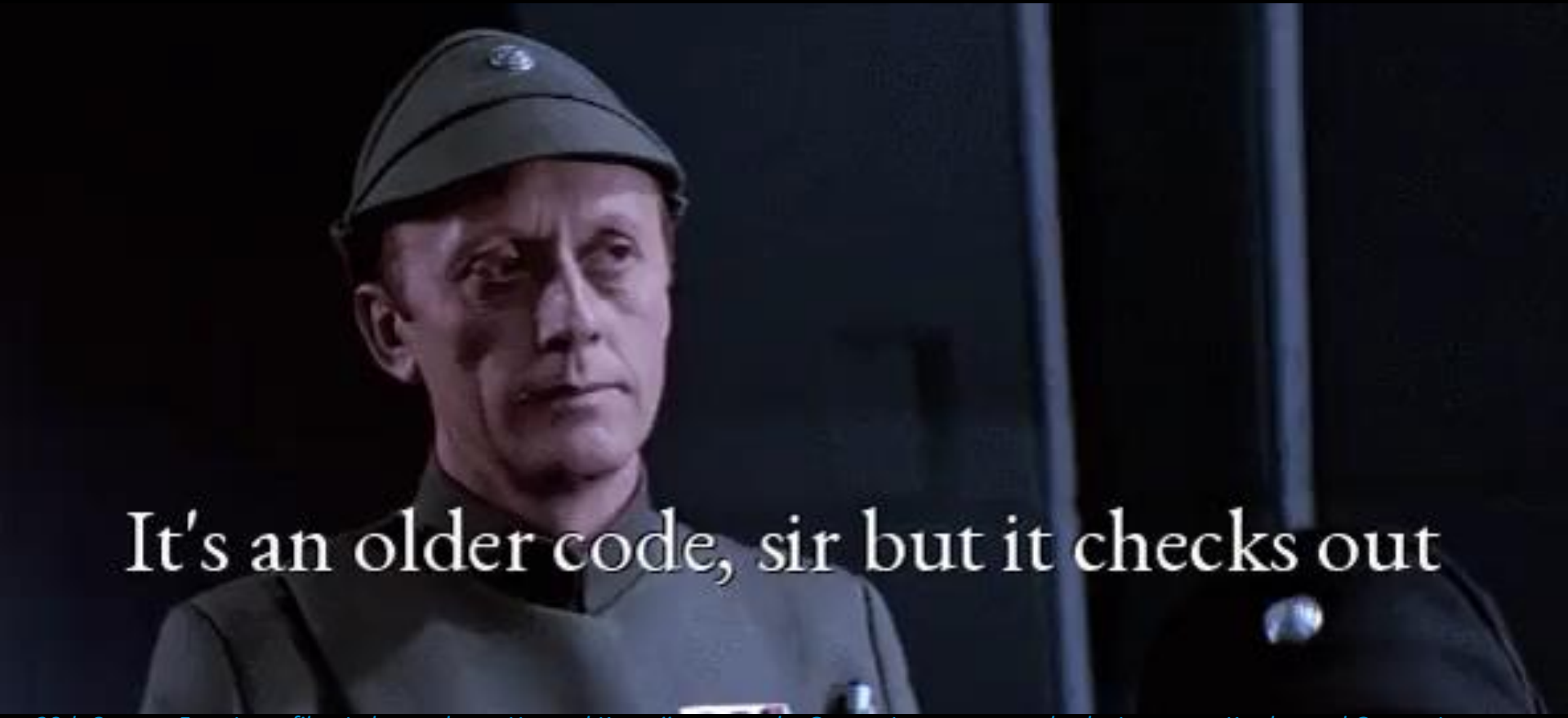
→ **You can add arbitrary groups (SIDs) to the TGT.**

*… the **forest is a security boundary** for the information that is contained in that instance of Active Directory.*
- MSDN

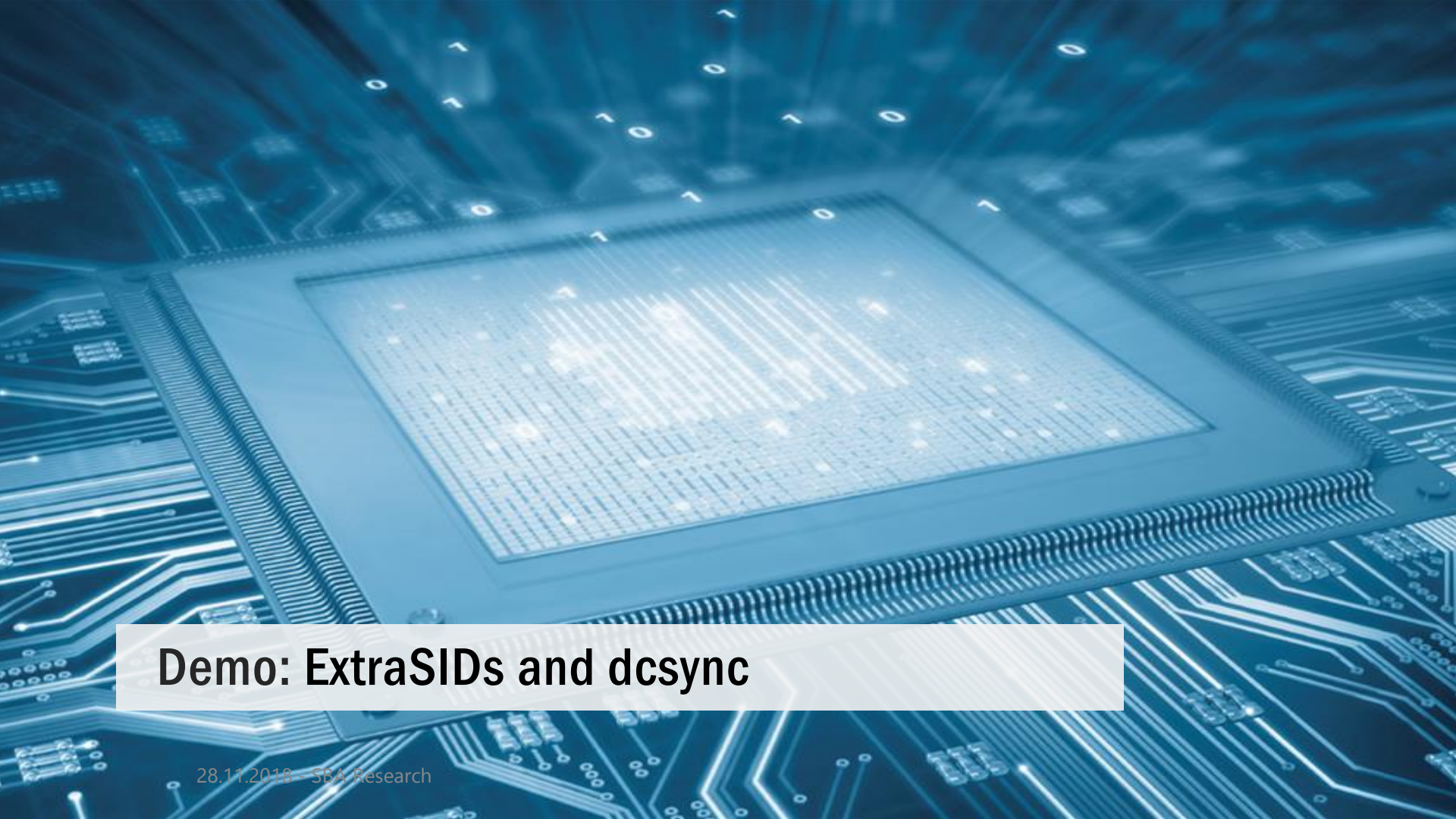


Enterprise Administrators

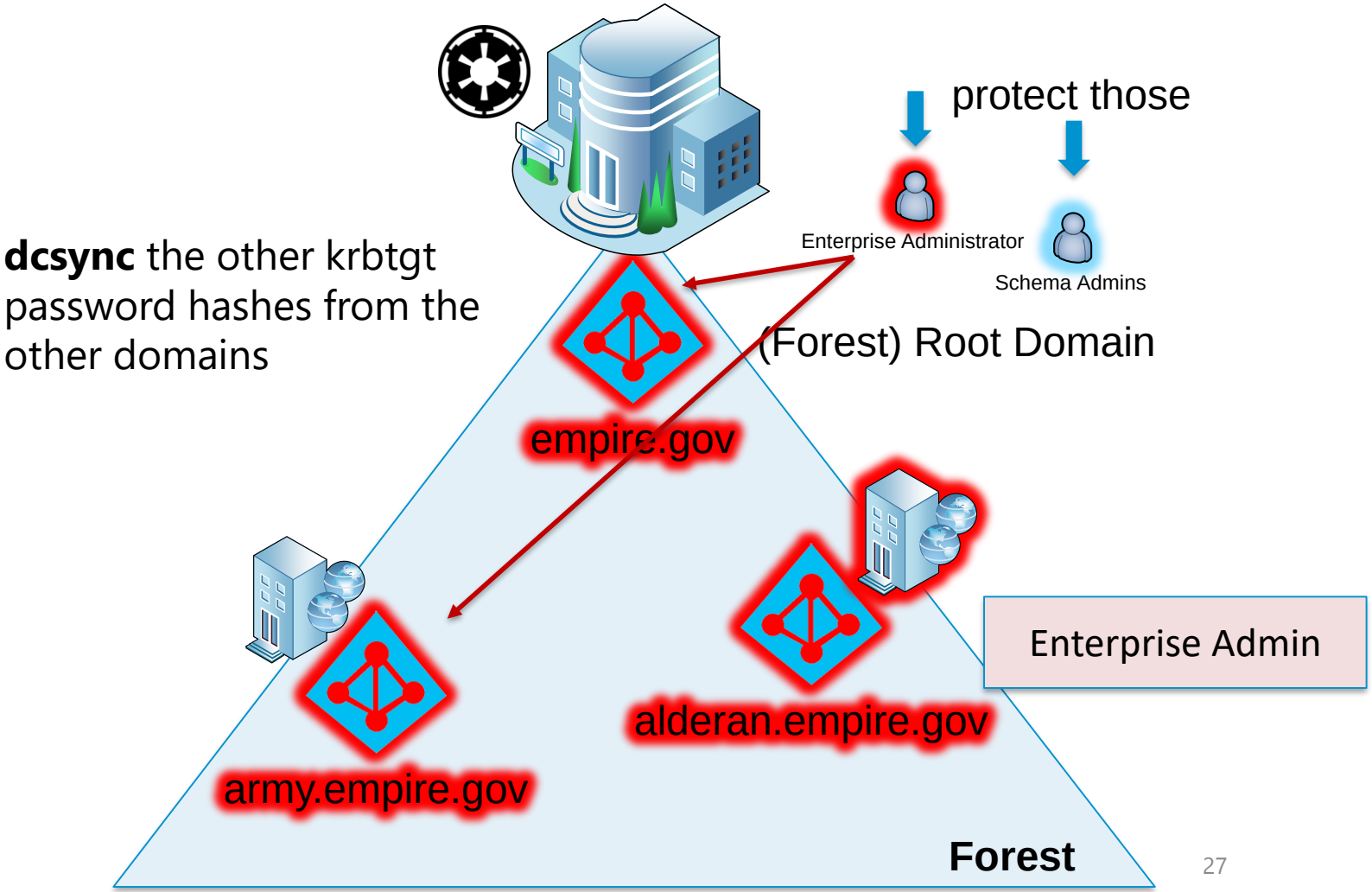




20th Century Fox ; Lucasfilm, Ltd. ; producer, Howard Kazanjian ; story by George Lucas ; screenplay by Lawrence Kasdan and George Lucas ; director, Richard Marquand. Star Wars. Episode VI, Return of the Jedi. Beverly Hills, Calif. :20th Century Fox Home Entertainment, 2013.



Demo: ExtraSIDs and dcsync


protect those
Enterprise Administrator
Schema Admins
dcsync the other krbtgt password hashes from the other domains
(Forest) Root Domain
empire.gov
alderan.empire.gov
army.empire.gov
Enterprise Admin
Forest

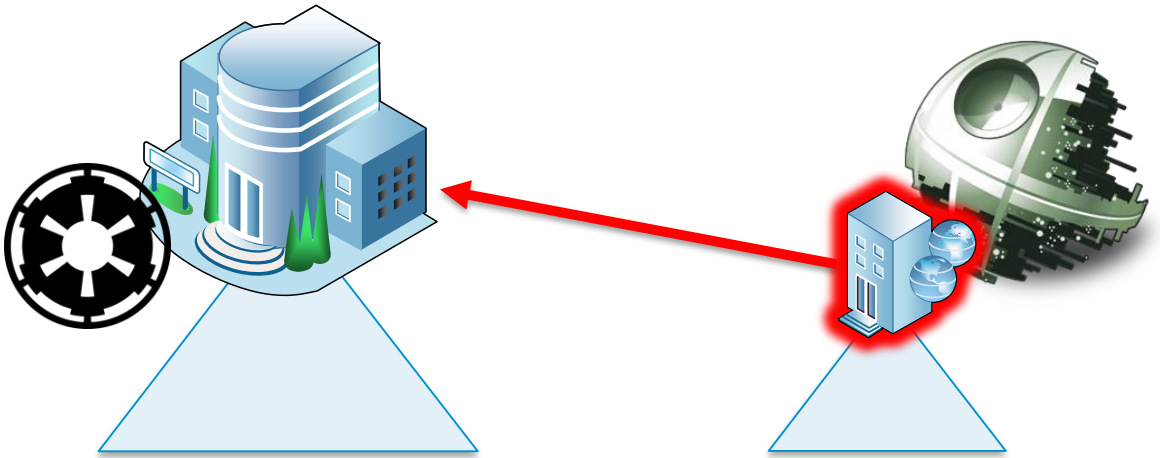
Findings

- Automatic two-way trust between root and child
- Migration feature *SidHistory* is enabled by default
- The AD-Forest is the security boundary, not the domain

Counter Measures

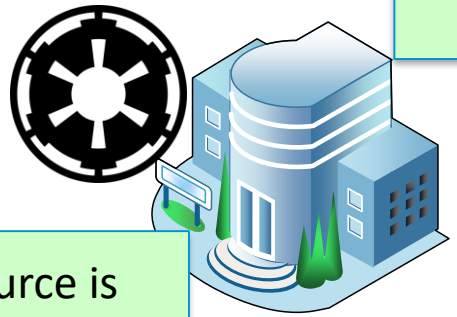
- Sid History Filtering
- Untrusted domains in a separate forest (?)

Threat model: Separate Forests
Is the trusting Forest in Danger?

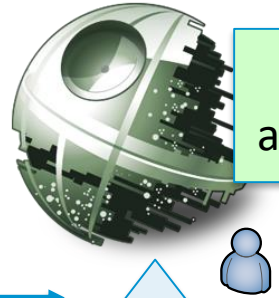


Separate Forests

Domain quarantine (SID filtering) is **enabled** by default.
No foreign ExtraSIDs



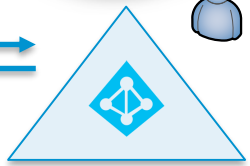
Ressource is secured by ACL



User is authenticated here

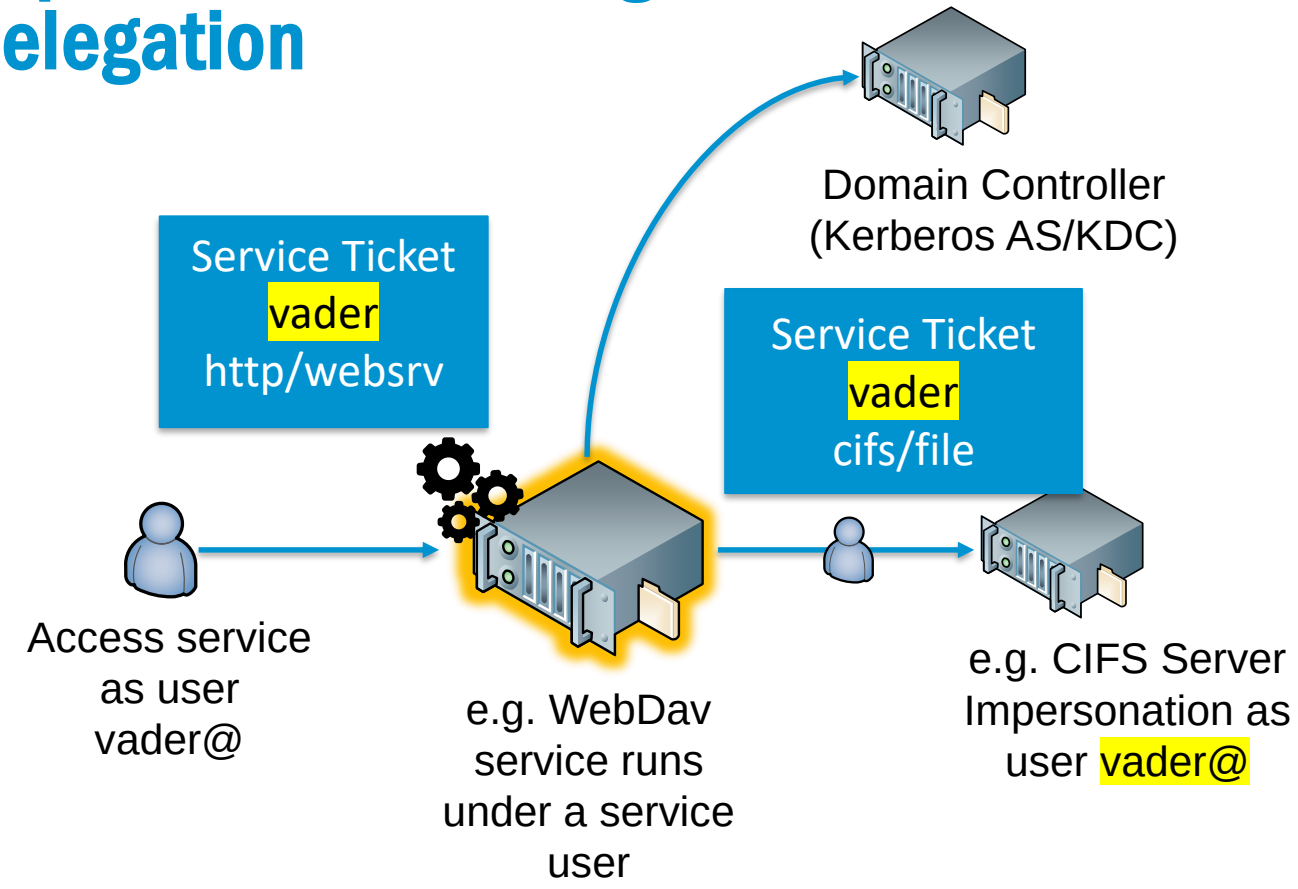
Other ressources may be accessible

Forest Trust
(two-way)

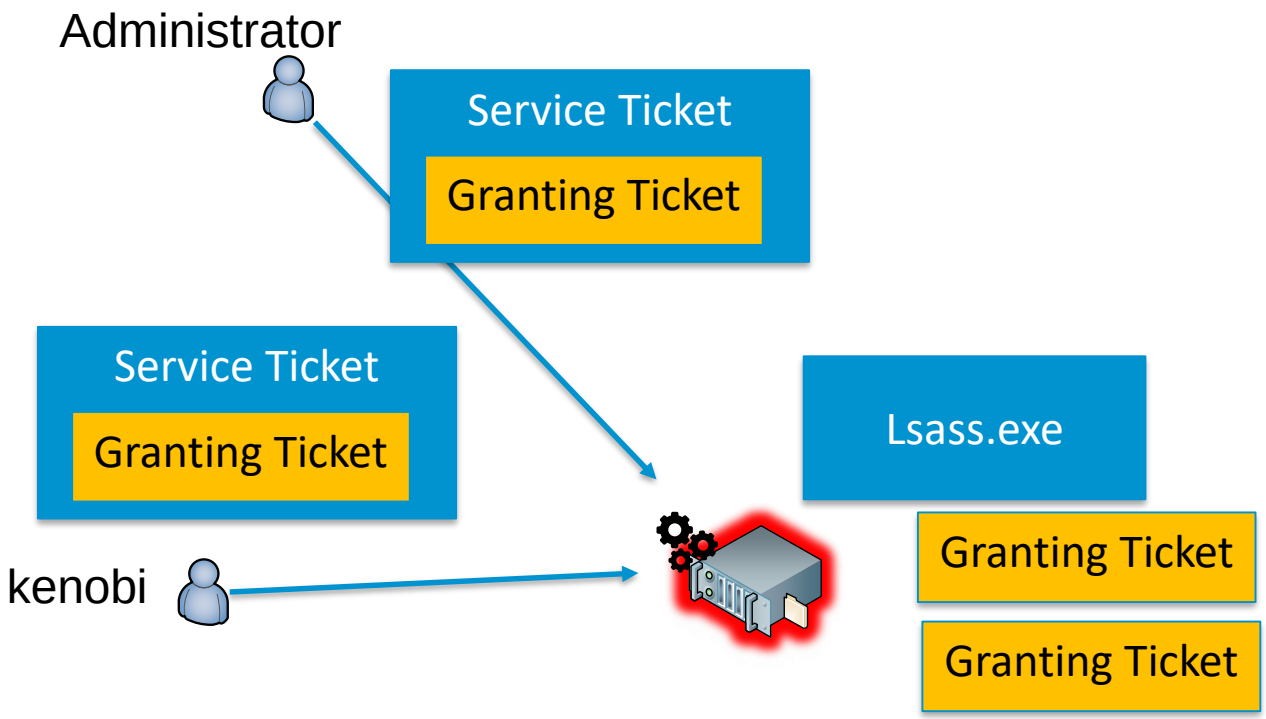


deathstar.mil

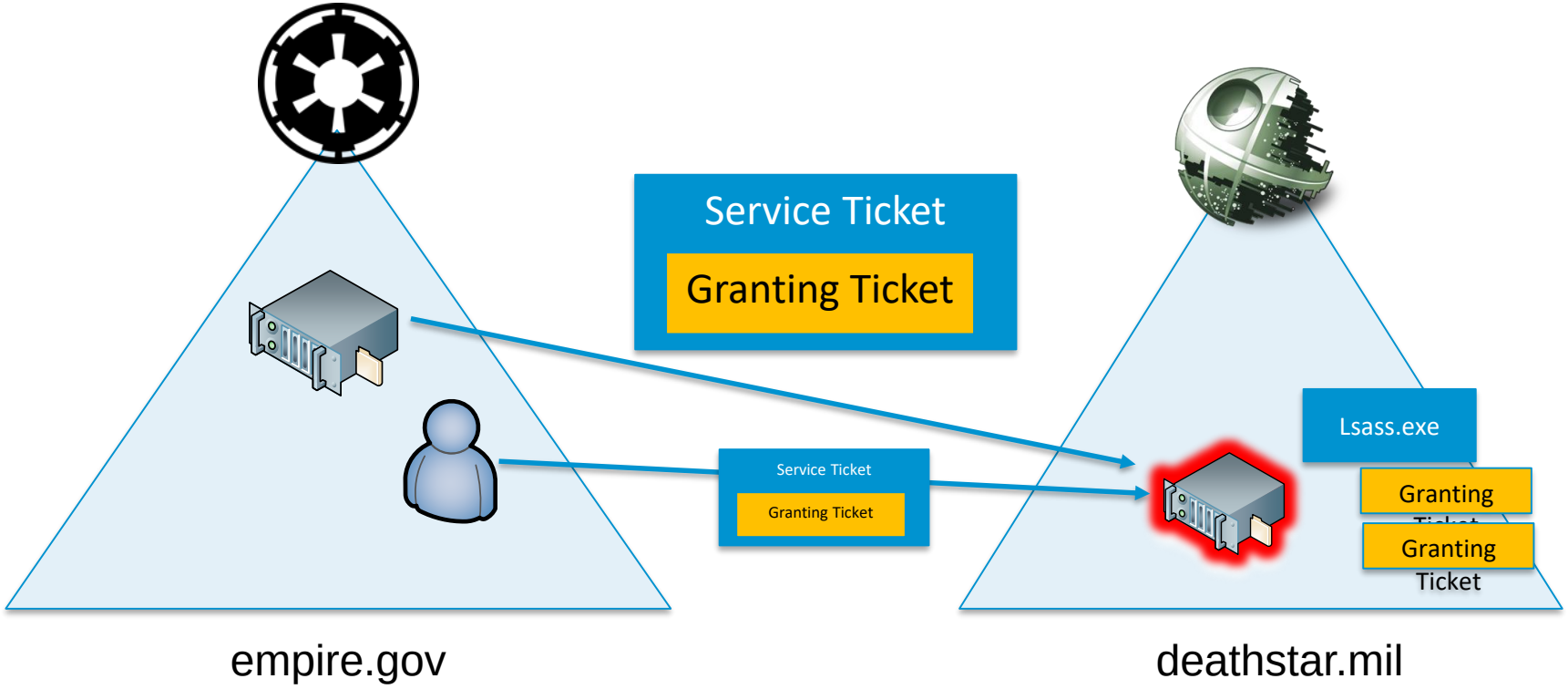
Impersonation through Delegation



Implications of Unconstrained Delegation



Separate Forests



https://imgur.com/gallery/RTIaYCs

Microsoft Printer Bug

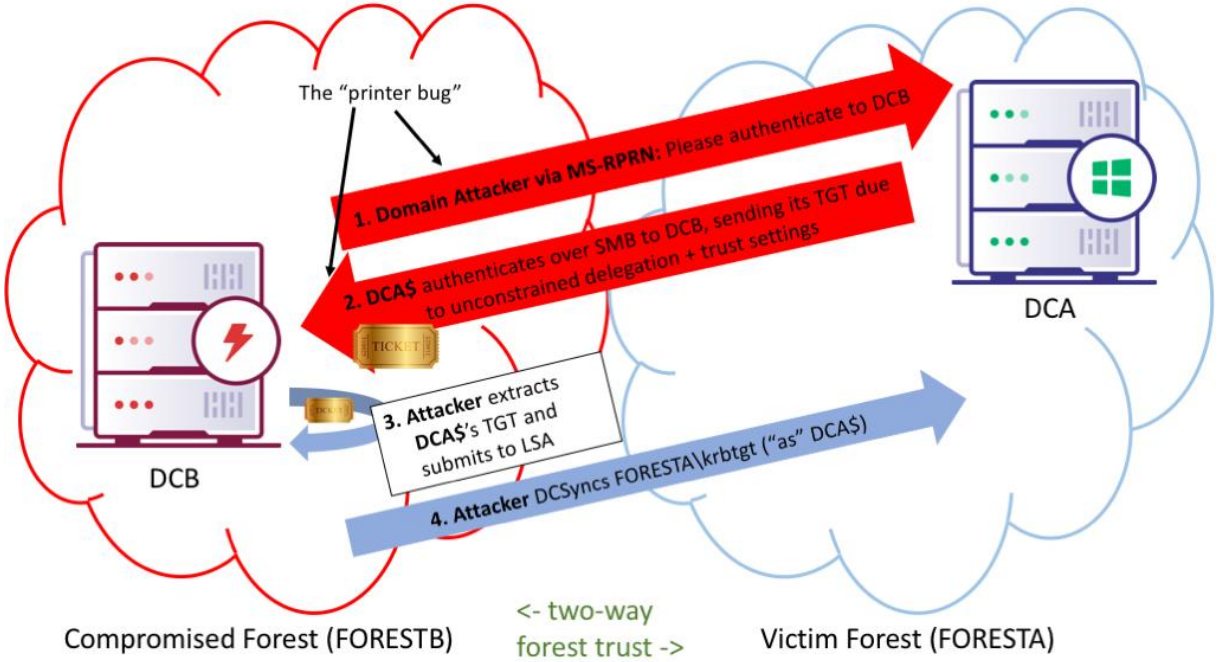
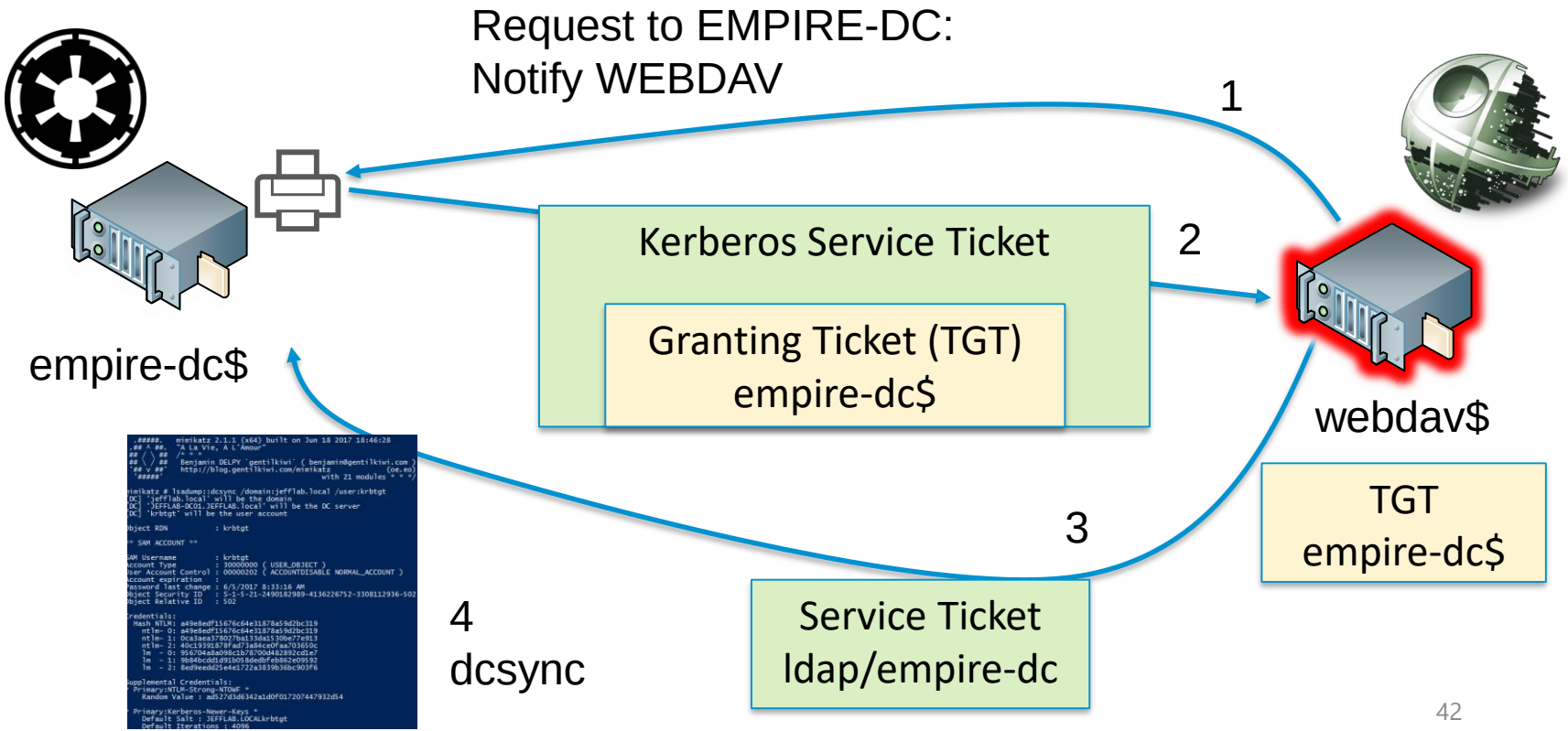
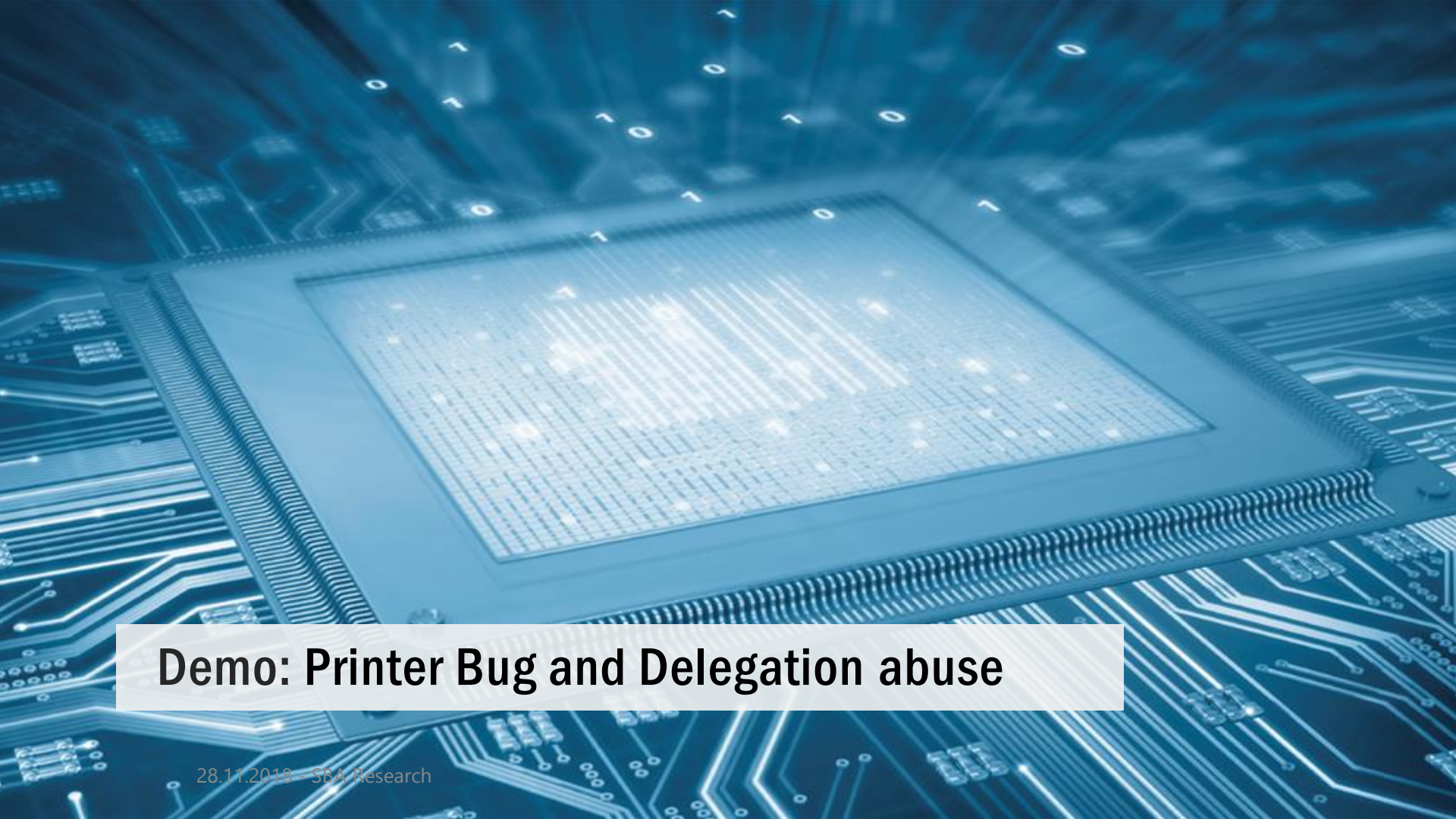


Image from: https://www.harmj0y.net/blog/redteaming/not-a-security-boundary-breaking-forest-trusts/
https://posts.specterops.io/hunting-in-active-directory-unconstrained-delegation-forests-trusts-71f2b33688e1

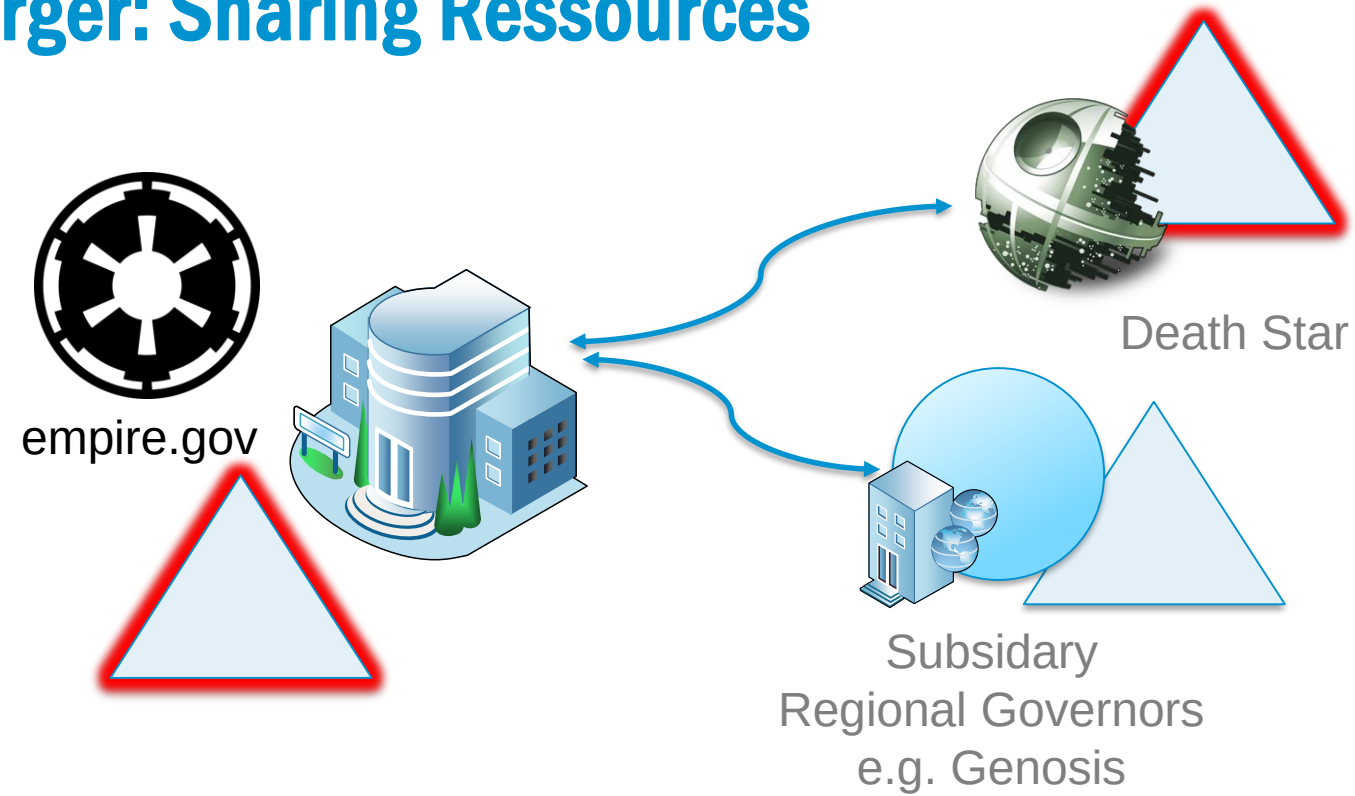
Attack Path of Unconstrained Delegation + Printer Bug





Demo: Printer Bug and Delegation abuse

Merger: Sharing Ressources



Counter Measures

- Patch (July 2019, KB unknown)
- netdom trust […] /enabletgtdelegation:no
  - Each Domain Controller in each Forest ;-)
- Put Admins in Protected Users Security Group
- Account flag „Account is sensitive and cannot be delegated“ of Administrators (not Computers)
- ~~Disable Spooler on Domain Controllers~~

Windows Hacking Training (3 Day course)

@ SBA Research

https://www.sba-research.org/professional-services/advanced-training/windows-hacking/

Pentest you should

Questions

20th Century Fox ; Lucasfilm, Ltd. ; producer, Howard Kazanjian ; story by George Lucas ; screenplay by Lawrence Kasdan and George Lucas ; director, Richard Marquand. Star Wars. Episode VI, Return of the Jedi. Beverly Hills, Calif. :20th Century Fox Home Entertainment, 2013.

COMET

Competence Centers for
Excellent Technologies

Reinhard Kugler

Andreas Bernauer

SBA Research gGmbH

Floragasse 7/5, 1040 Vienna

rkugler@sba-research.org

Bundesministerium Verkehr, Innovation und Technologie

Bundesministerium Digitalisierung und Wirtschaftsstandort

FFG Forschung wirkt.

wirtschaftsagentur wien Ein Fonds der Stadt Wien

FWF Der Wissenschaftsfonds.

netidee OPEN INNOVATIONS