Lame joke coming...

What do you get when you move a folder back and forth across your desktop?



HORIZON
SECURED

Active Directory



Warned you.... ;)

HORIZON
SECURED

Find Active Directory Security Risks

w/

David Horák
Founder of Horizon Secured
Security Engineer & Team Leader
www.horizon-secured.com

HORIZON
— SECURED —



Active Directory is dead? I don‘t mind...



HORIZON
— SECURED —

But first... Quiz!

- 3 questions during the talk
- 2 winners at the end
- Slido is used

HORIZON
SECURED



HORIZON
— SECURED —

Question 1/3

Does the NT hash cache, if you are member of Protected Users group?



HORIZON
SECURED

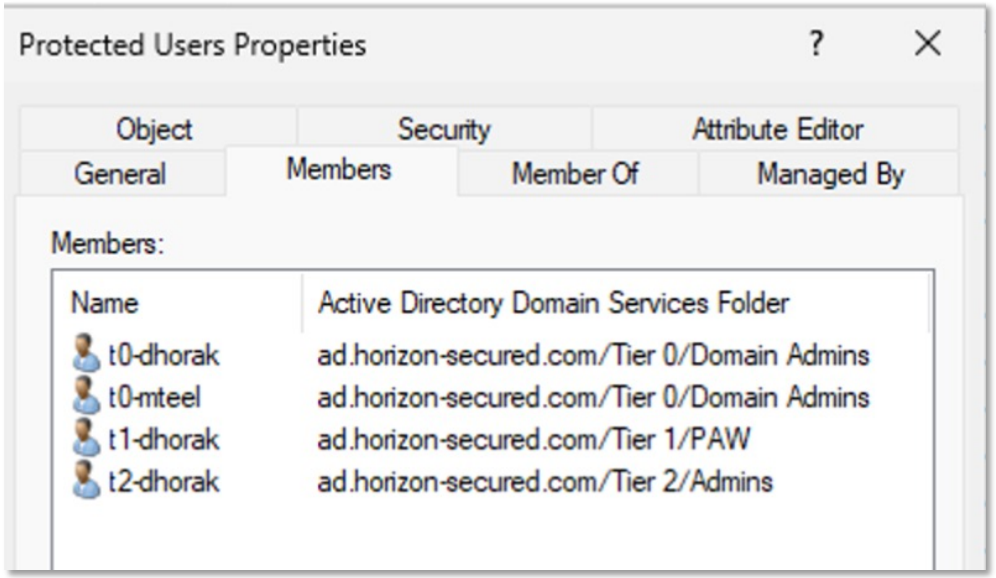
Protected Users group

HORIZON
— SECURED —

Protections

Device

- WDigest/CredSSP won't cache
- *NT hash not cached*
- Kerberos uses AES only



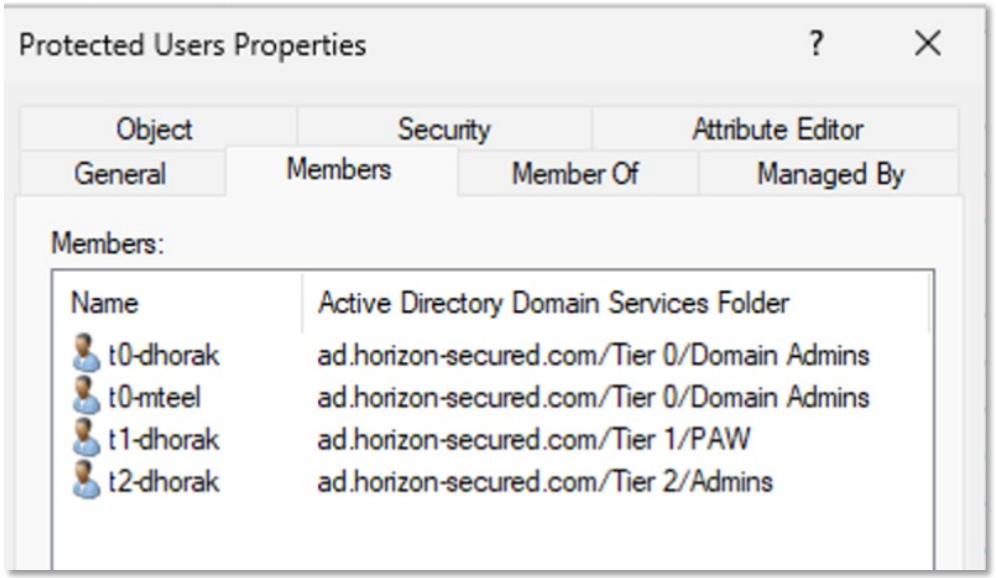
Protected Users group

HORIZON
— SECURED —

Protections

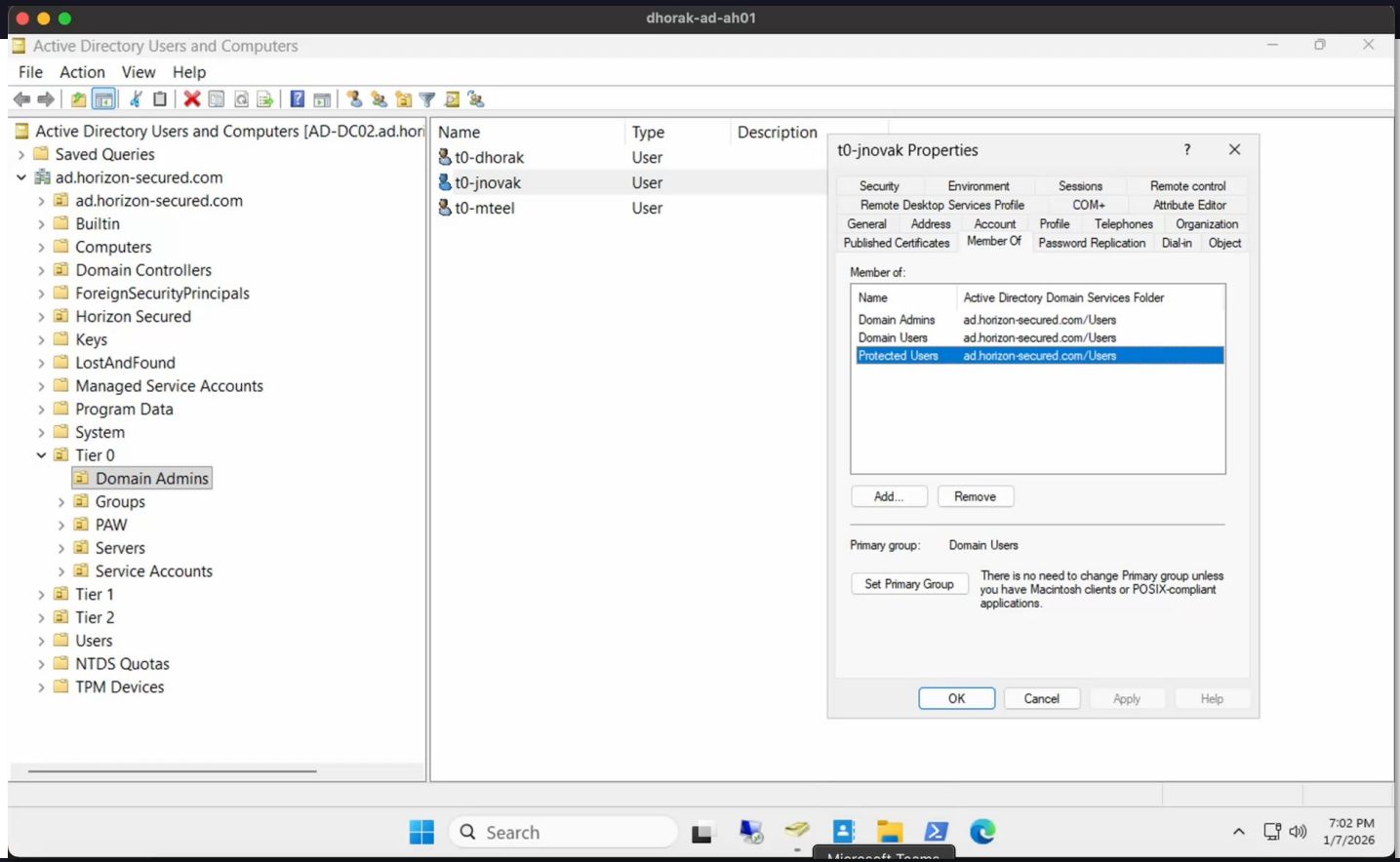
Domain Controller

- No NTLM authentication
- Kerberos DES/RC4 disabled
- No (un)constrained delegation
- TGT is 4-hour, non-renewable



Protected Users group

HORIZON
SECURED



Protected Users group

HORIZON
— SECURED —

FIX?

"Case was reported as a Moderate severity issue, which will be considered for a fix in a future release of the product."

Credits

- Peter Kloep (CQURE webinar)
- André Estêvão (testing & collaborating)

Device protections for signed in Protected Users

When the signed in user is a member of the Protected Users group, the group provides the following protections:

- Credential delegation (CredSSP) doesn't cache the user's plain text credentials even when the user enables the **Allow delegating default credentials** Group Policy setting.
- Windows Digest doesn't cache the user's plaintext credentials even when they've enabled Windows Digest.
- NTLM stops caching the user's plaintext credentials or NT one-way function (NTOWF).
- Kerberos stops creating Data Encryption Standard (DES) or RC4 keys. Kerberos also doesn't cache the user's plaintext credentials, or long-term keys after acquiring the initial Ticket Granting Ticket (TGT).
- The system doesn't create a cached verifier at user sign-in or unlock, so member systems no longer support offline sign-in.

Question 2/3

If an AD account is locked out, can you still brute-force it?



HORIZON
SECURED

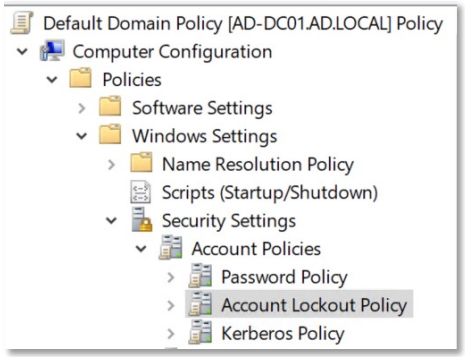
Account Lockout policy

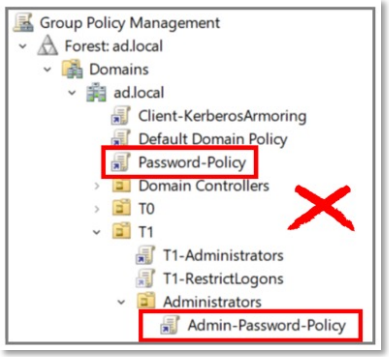
HORIZON
— SECURED —

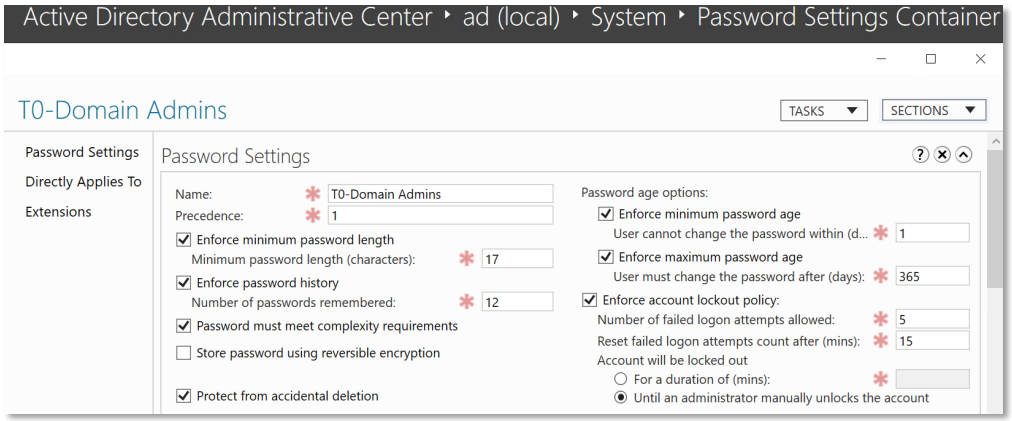
„Each domain can have only one account policy. The account policy must be defined in the default domain policy or in a new policy that is linked to the root of the domain“

Multiple Account Policies ?

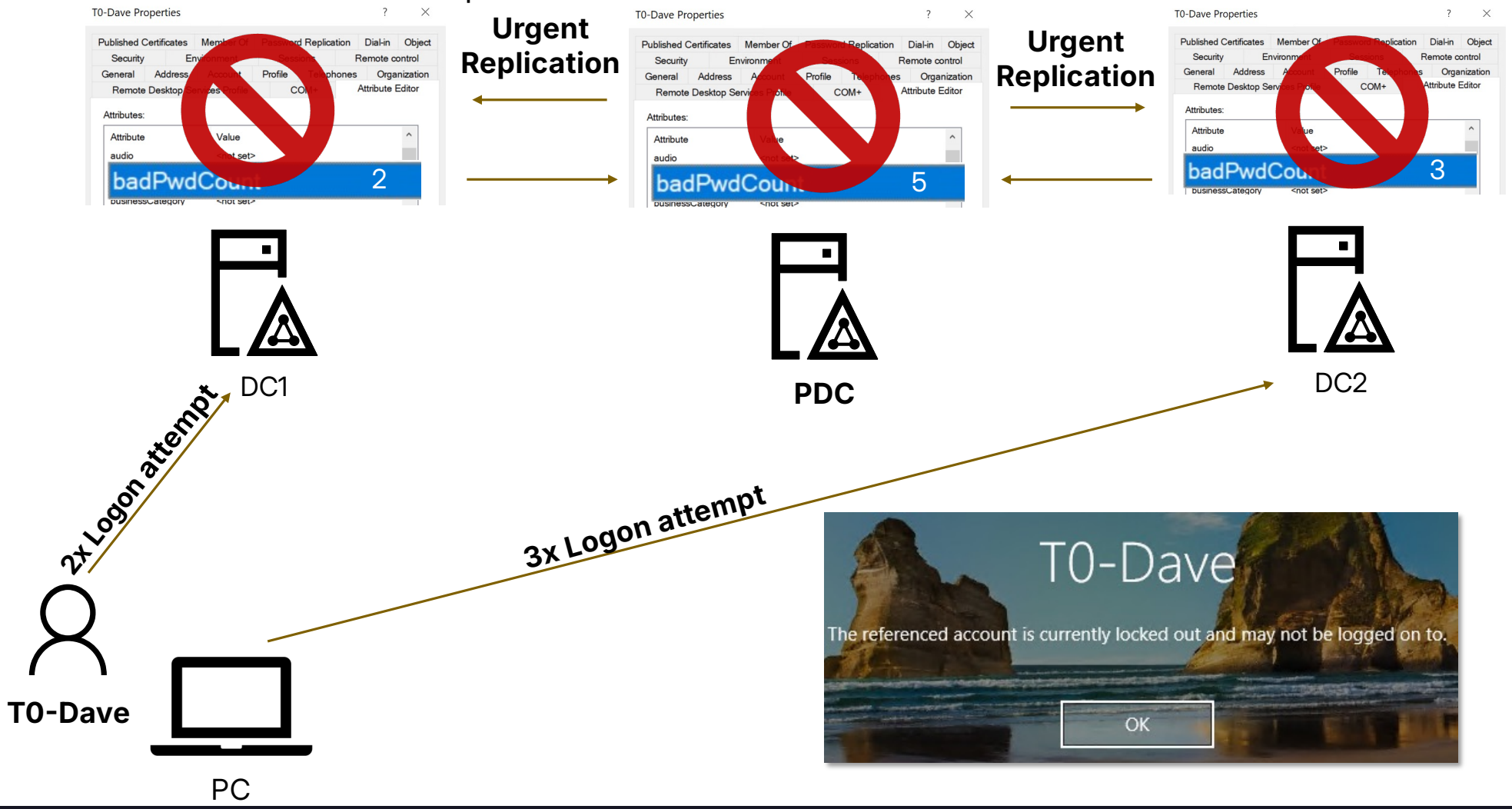
- Fine Grained Password Policies







Lockout Treshold: 5 bad attempts



Account Lockout policy

HORIZON
SECURED

MS Documentation:

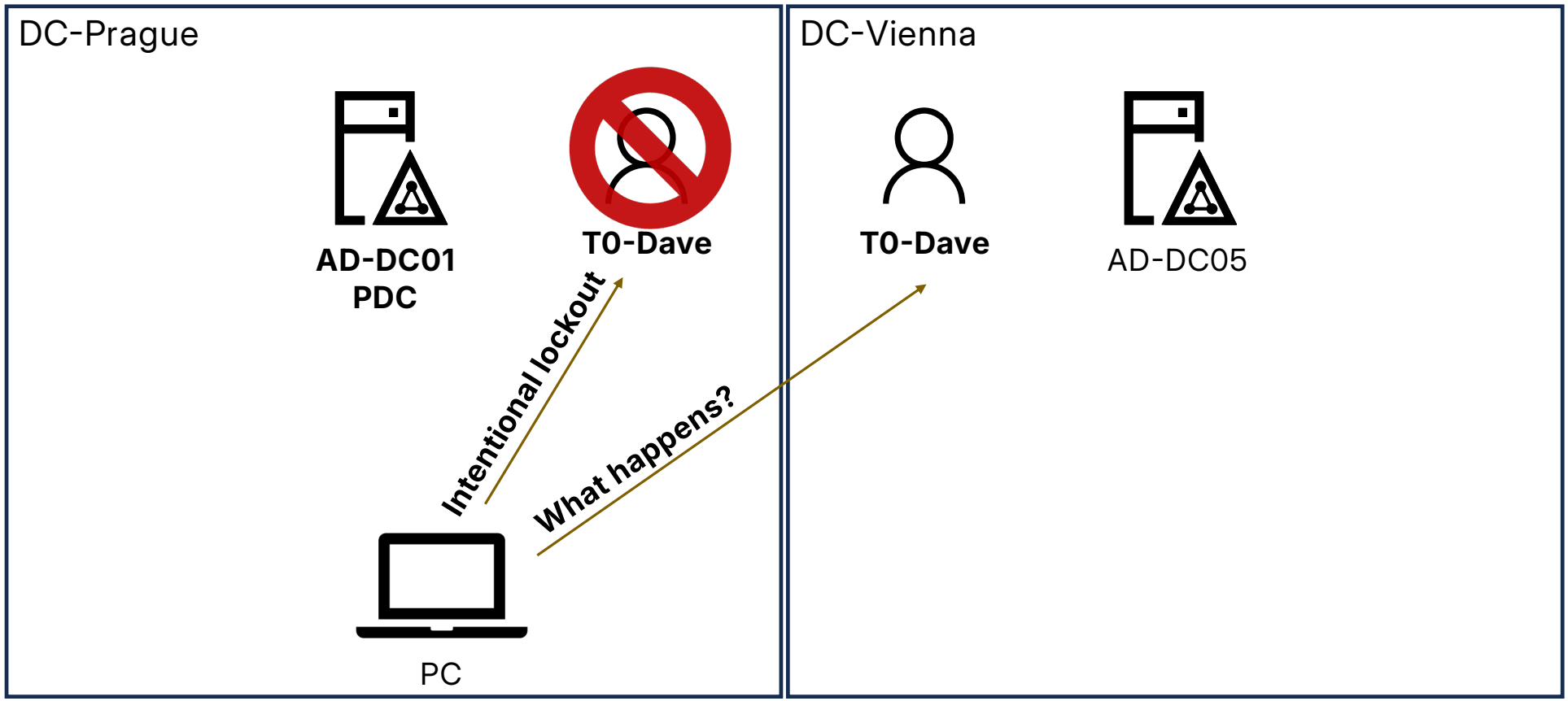
„Urgent Active Directory replication is always triggered by certain events on all domain controllers within the ***same site****“*

What if...

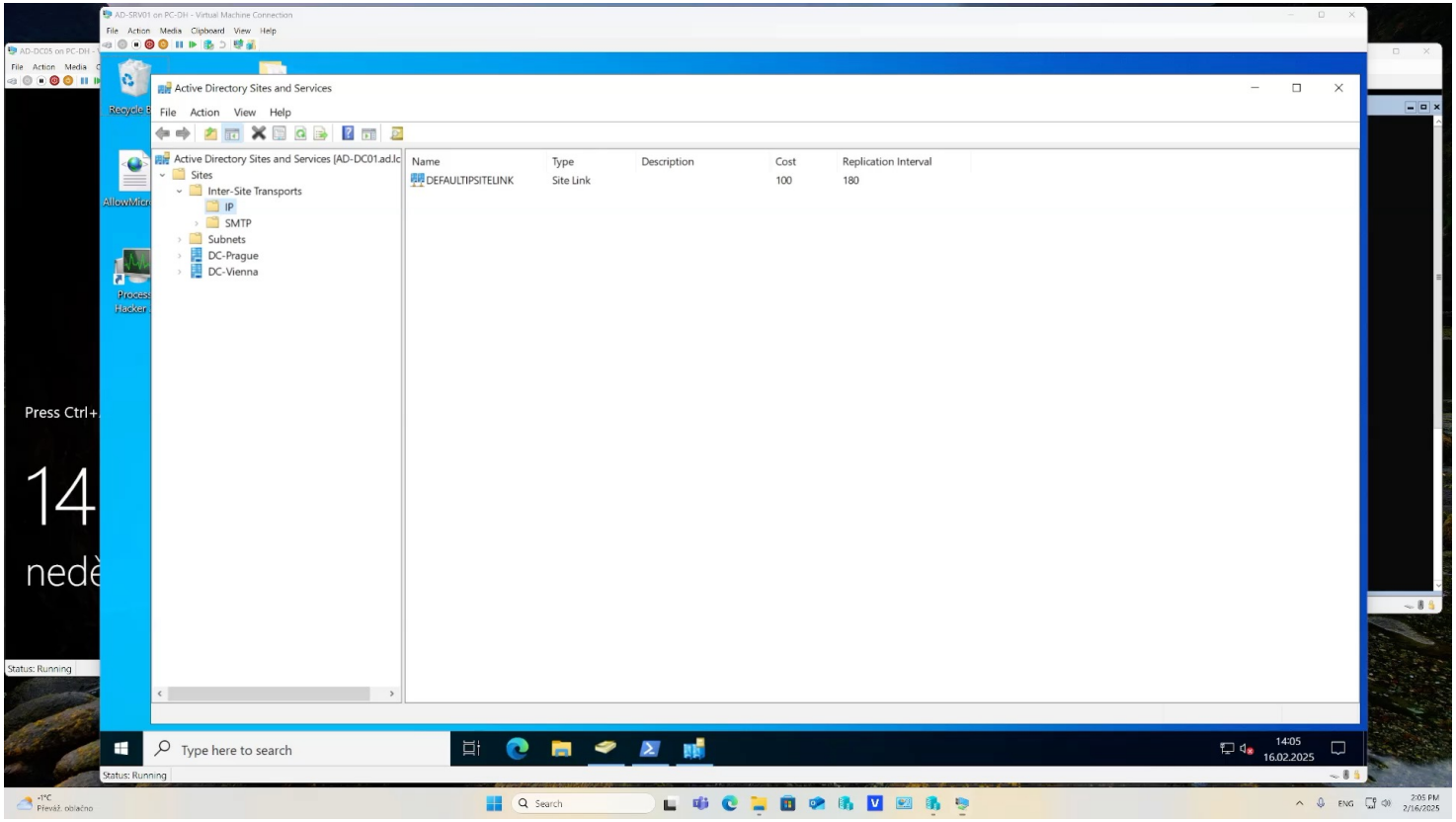
I intentionally lock out the account in the site with PDC and then try to brute-force it in another site ?



Intersite Replication: 180 minutes (Default)
Lockout Treshold: 5 bad attempts
Lockout Duration: 15 minutes



Account Lockout policy



Account Lockout policy

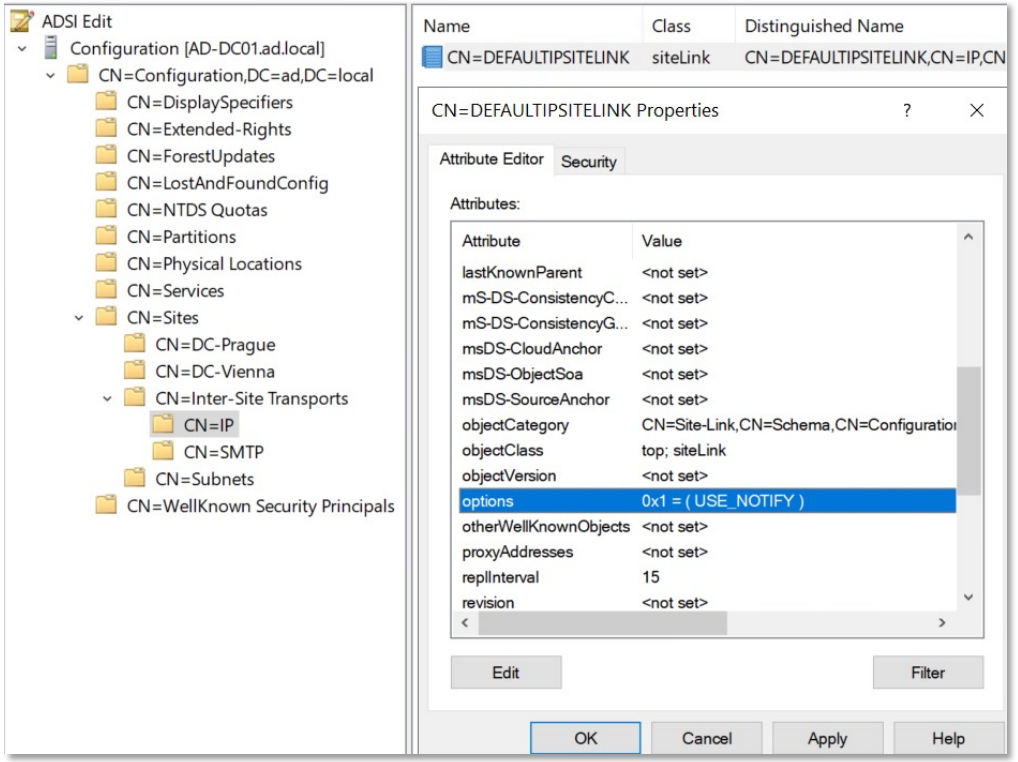
HORIZON
— SECURED —

Solution

Change intersite replication

- Change Notification System

ADSIEdit.msc > Configuration partition > Sites > Inter-Site Transports > IP > DEFAULTSITELINK > Attribute Editor > ***Options = 1***



Question 3/3

Does Credential Guard protect credentials entered in RDP?



HORIZON
SECURED

RDP as a Big Brother

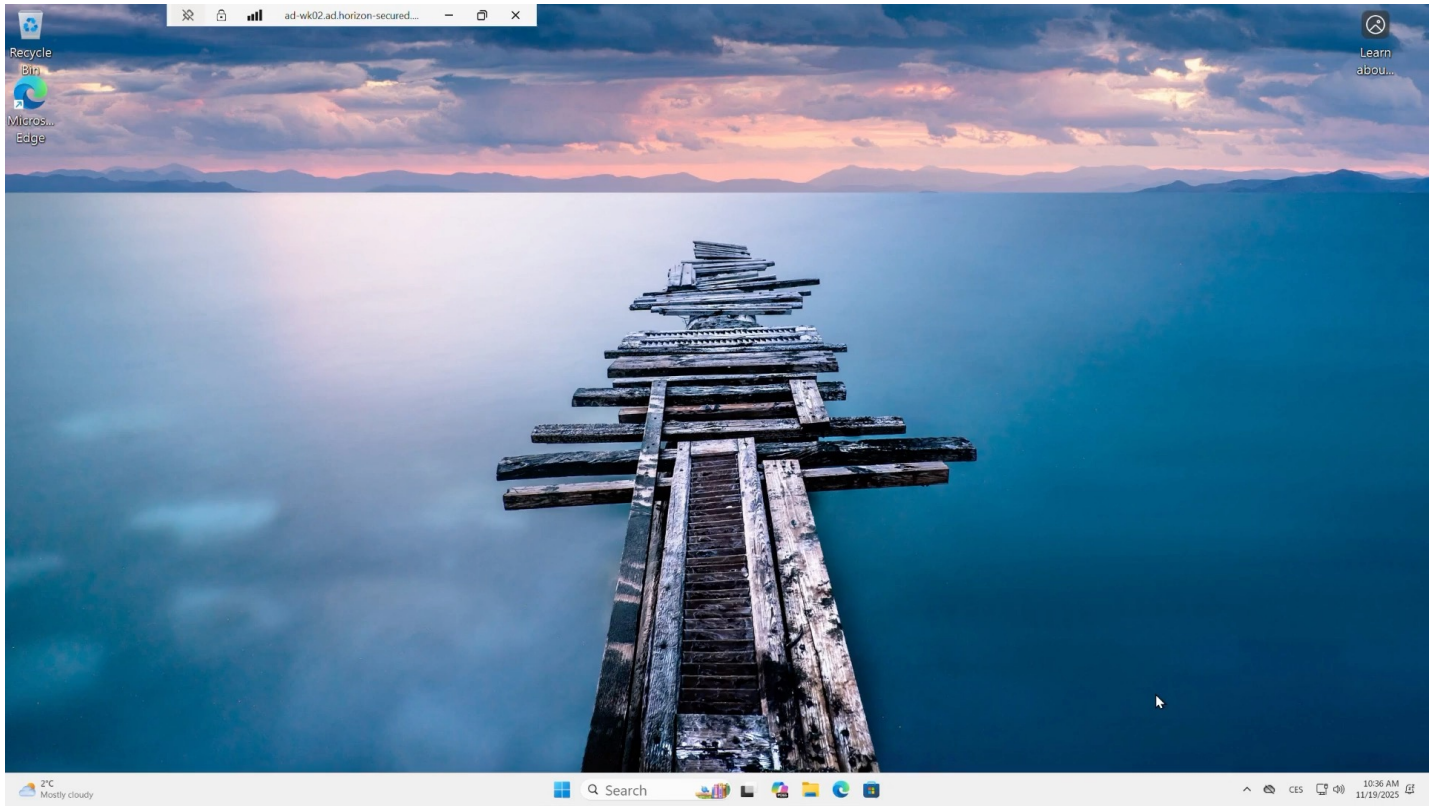




But it does not stop there...

RDP as a Big Brother

HORIZON
— SECURED —



RDP as a Big Brother

HORIZON
— SECURED —

Protection?

- There is **no setting** to simply „disable this“
- But there is **hope…**



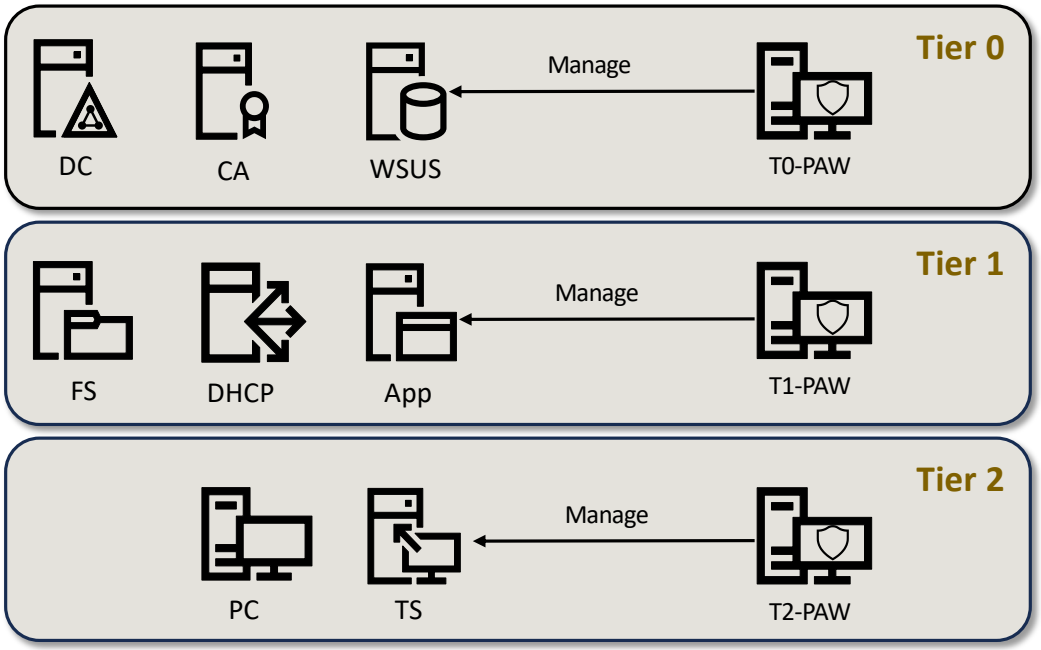
There are still things to discover

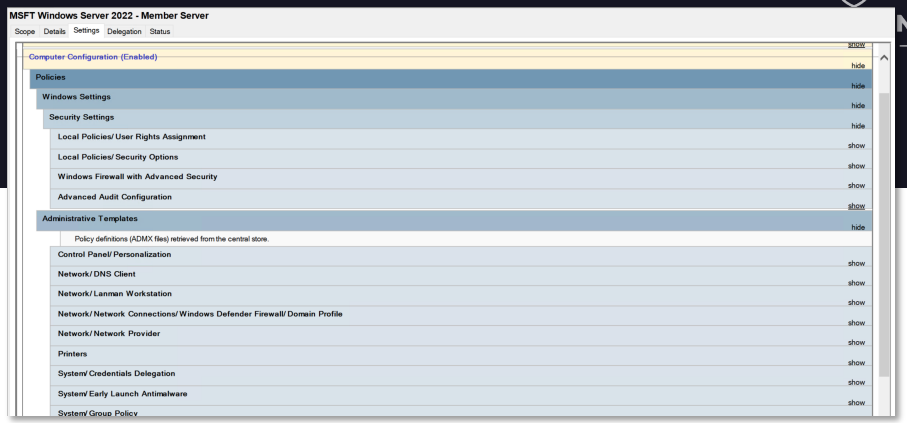
HORIZON
SECURED

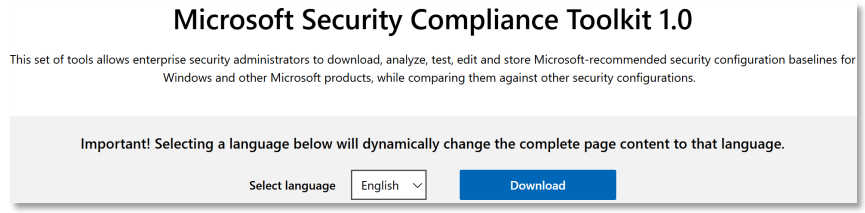
- To protect against these unknown threats you must **follow best practices**

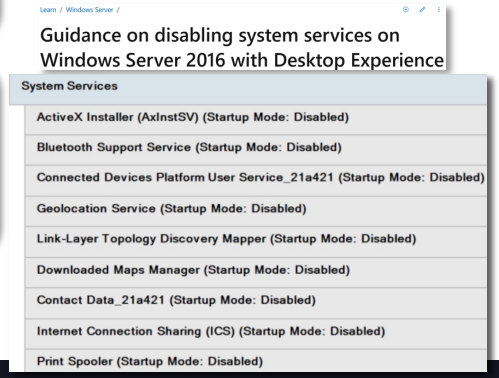


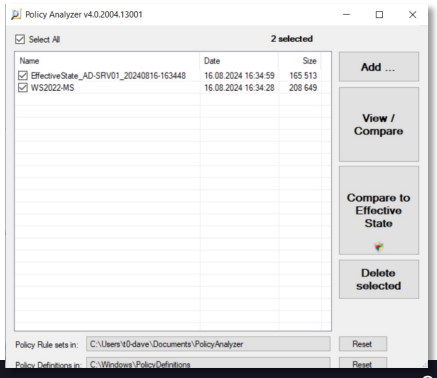
Best Practices











Key Takeaways

HORIZON
SECURED

- Do not trust anything, always verify
- There are unknown threats, you **cannot protect yourself** from
  - **Or can you?**
- Follow **best practices** – they have been around for ages

Quiz

Quiz winner is...

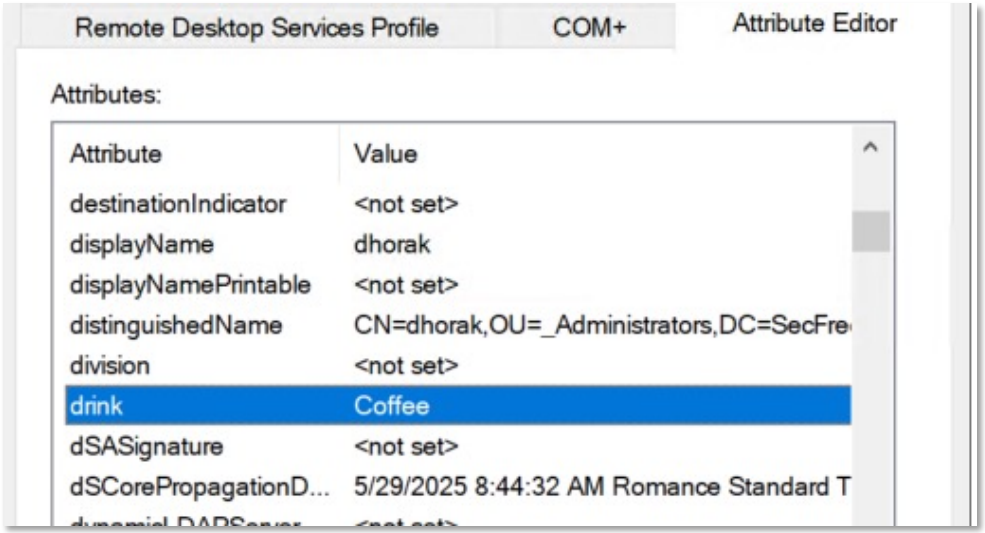
(we will contact you after the webcast)

- Do you want to talk?
  - Write me a DM and let's have a virtual ***drink*** together

@horizon_secured

Horizon Secured

*„The drink **(Favourite Drink)** attribute type specifies the favorite drink of an object (or person).“*



Thank you for joining !

David Horák
Founder of Horizon Secured
Security Engineer & Team Leader

HORIZON
— SECURED —

www.horizon-secured.com
david.horak@horizon-secured.com
Prague, Czech Republic