semperis

Hackers don‘t break in, they log in

Warum der Schutz von Identitäten immer wichtiger wird!

Guido Grillenmeier

Semperis Principal Technologist, EMEA

12 Years Microsoft MVP

guidog@semperis.com

www.linkedin.com/in/guidogrillenmeier

LSZ FUTURE CONNECTIONS

IT-SECURITY & CYBER CRIME Summit West

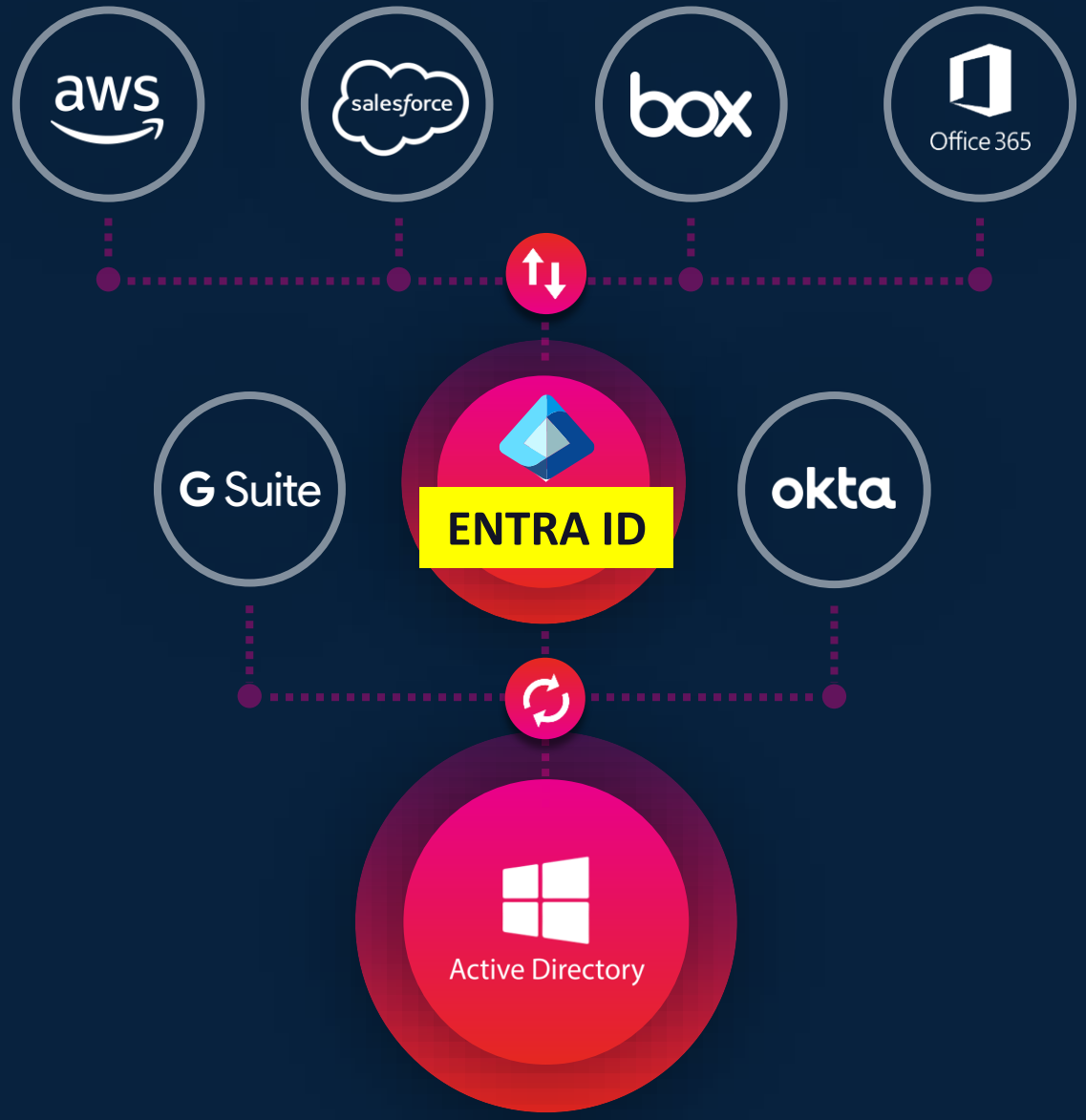
Dienstag
19. September
2023

semperis

KEYS TO THE KINGDOM

Wenn AD nicht sicher ist, ist es nichts mehr

- 90% aller Angriffe involvieren Identitäten-Missbrauch
- Systemische Schwachstellen machen AD zu einem begehrten Ziel
- Cloud Identitäten synchronisieren mit AD
- Zero Trust Modell bedarf hybride AD-Integrität



Für **90% von Unternehmen**, beginnt Identität mit AD

semperis

#1 NEW TARGET

90 % der untersuchten Angriffe beinhalten AD in irgendeiner Form, unabhängig davon, ob es sich um den ursprünglichen Angriffsvektor handelt oder um Persistenz oder Berechtigungen angestrebt wird

- Mandiant

MICROSOFT EXCHANGE

SOLARWINDS

COLONIAL PIPELINE

MAERSK

Phasen eines Ransomware-Angriffs

semperis

Initialer Zugang

- Phishing E-Mails
- Kompromittierte Web-Seiten
- Gezielter Angriff mit **gestohlenen Zugangs-Kennungen**

BYOVD

Nach dem Exploit

- Download von Malware für die **Recon-Phase**
- Verbindungen zu den C2* Systemen herstellen
- Fern-Verbindungen zur Kontrolle des weiteren Angriffs sind vorhanden

Suchen & Erkennen

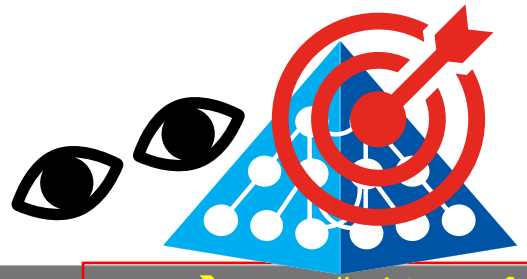
- Reconnaissance
- Prüfen der **AD Schwachstellen** mit dem Ziel zur **Kontroll-Übernahme der AD Domäne**
- Laterale Verbreitung auf anderen Systeme
- Sammeln von Anmelde-Kennungen und Elevation der Berechtigungen

Kernangriff

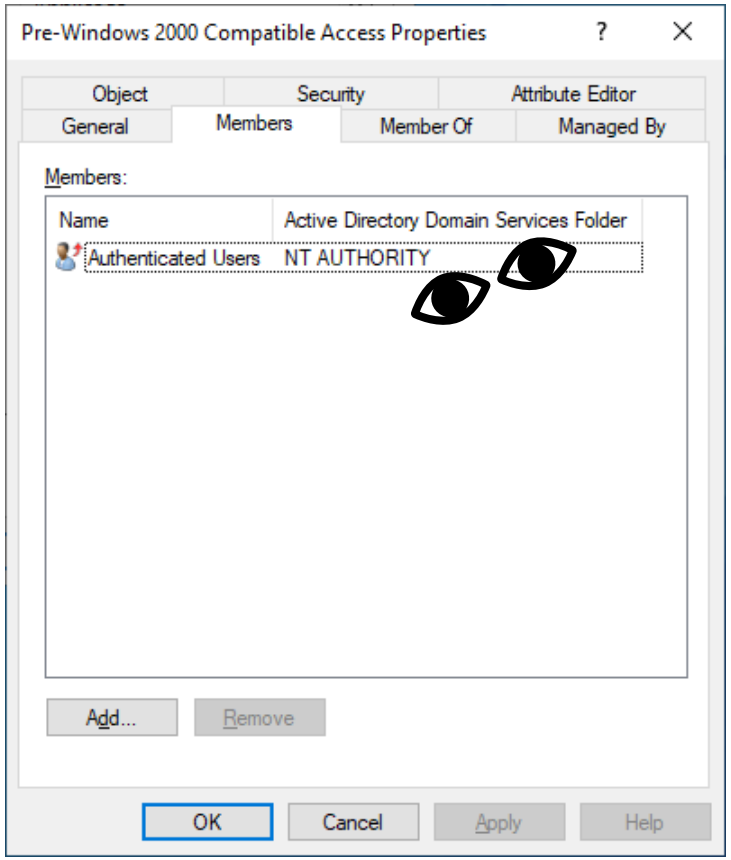
- Zugriff auf und Extraktion von Kerngeschäftsdaten
- Verschlüsselung von allen Systemen, inklusive der Backups und häufig einschließlich **AD-Domänencontrollern**

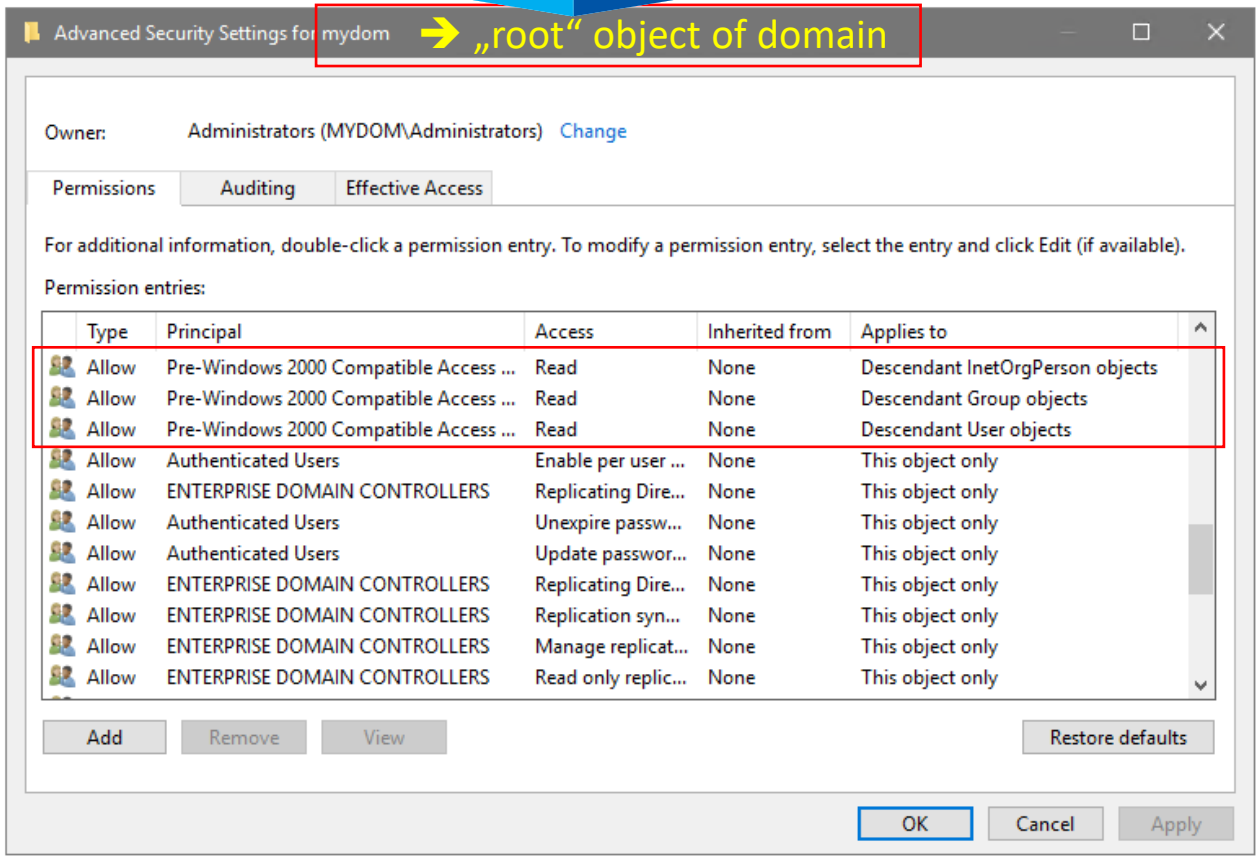
IN THROUGH OUT

Standard LESE-Rechte in AD



semperis

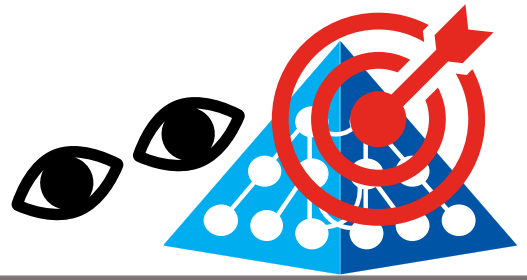




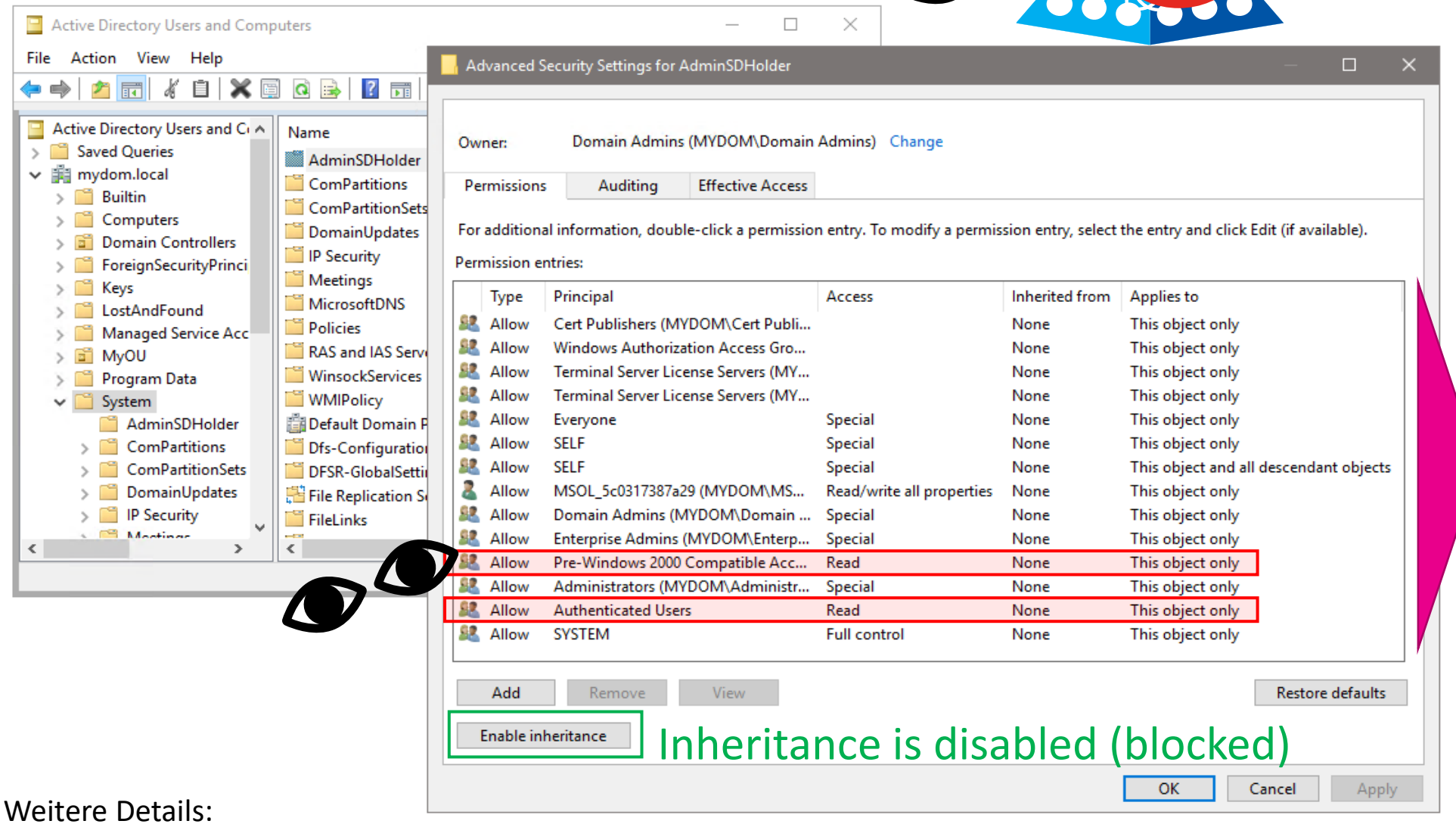
Siehe SEMPERIS BLOG

https://www.semperis.com/blog/security-risks-pre-windows-2000-compatibility-windows-2022

Standard LESE-Rechte in AD



semperis



AdminSDHolder

These permissions are “stamped” periodically on all your privileged groups and users (!)

Weitere Details:
https://www.semperis.com/wp-content/uploads/resources-pdfs/resources-improving-ad-security-posture-adminsdholder.pdf

Der Ernstfall - Beispiel aus dem realen Leben

DAS OPFER

- Mittlerer Osten
- Telco & Banking
- Kritische Infra
- Mehr als 1.000 Server

ENGAGEMENT

- Laufender Angriff, aber Opfer lebt noch
- QGROUP* bittet SEMPERIS um Unterstützung

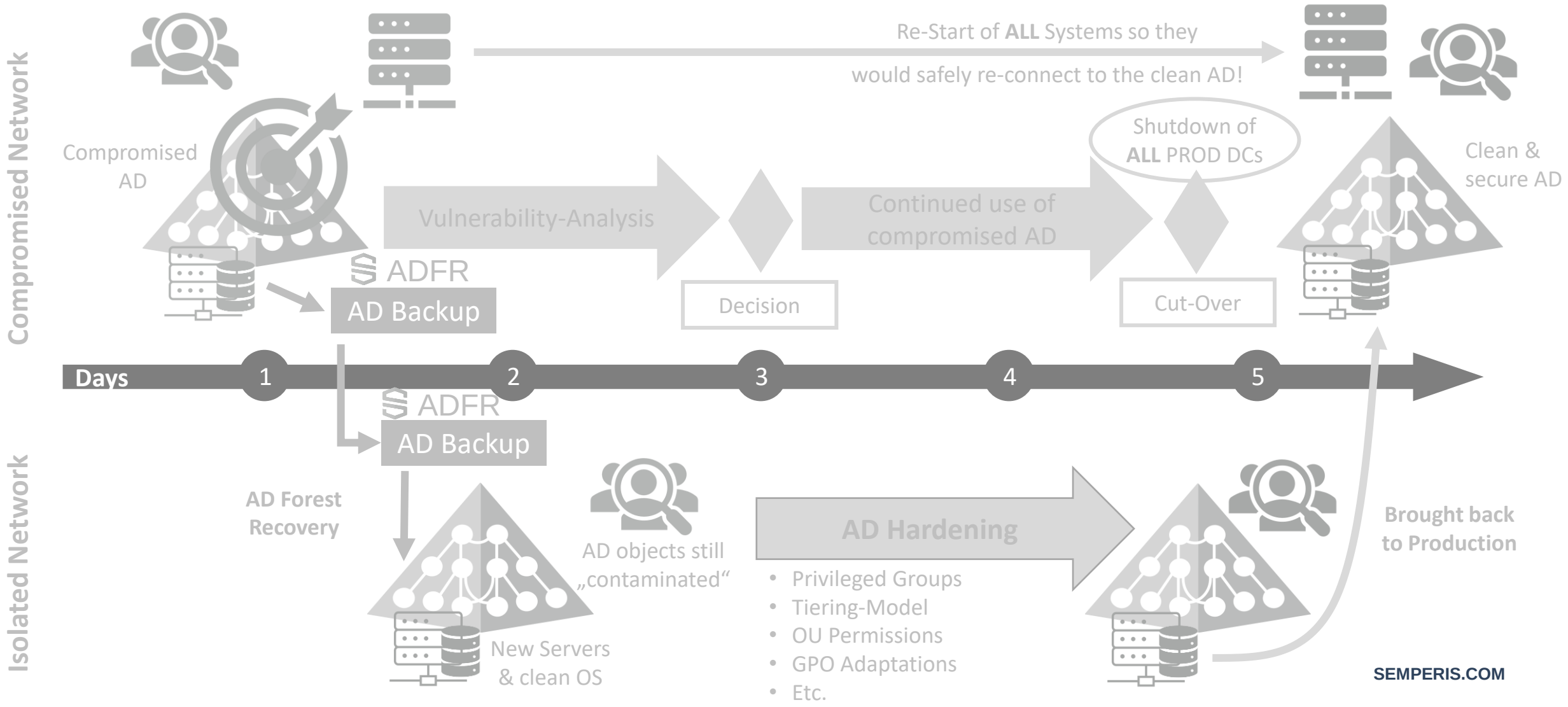
DIE ANGREIFER

- Nicht einer, sondern mehrere!
- Bekannte Gruppen aus unterschiedlichen Ländern

Es benötigte eine sehr koordinierte Zusammenarbeit zwischen den Experten von QGROUP und SEMPERIS, um diese Angriffe zu bekämpfen!

* QGROUP *ist ein EDR- + IR-Experte aus Deutschland*

Der Ernstfall - Beispiel aus dem realen Leben

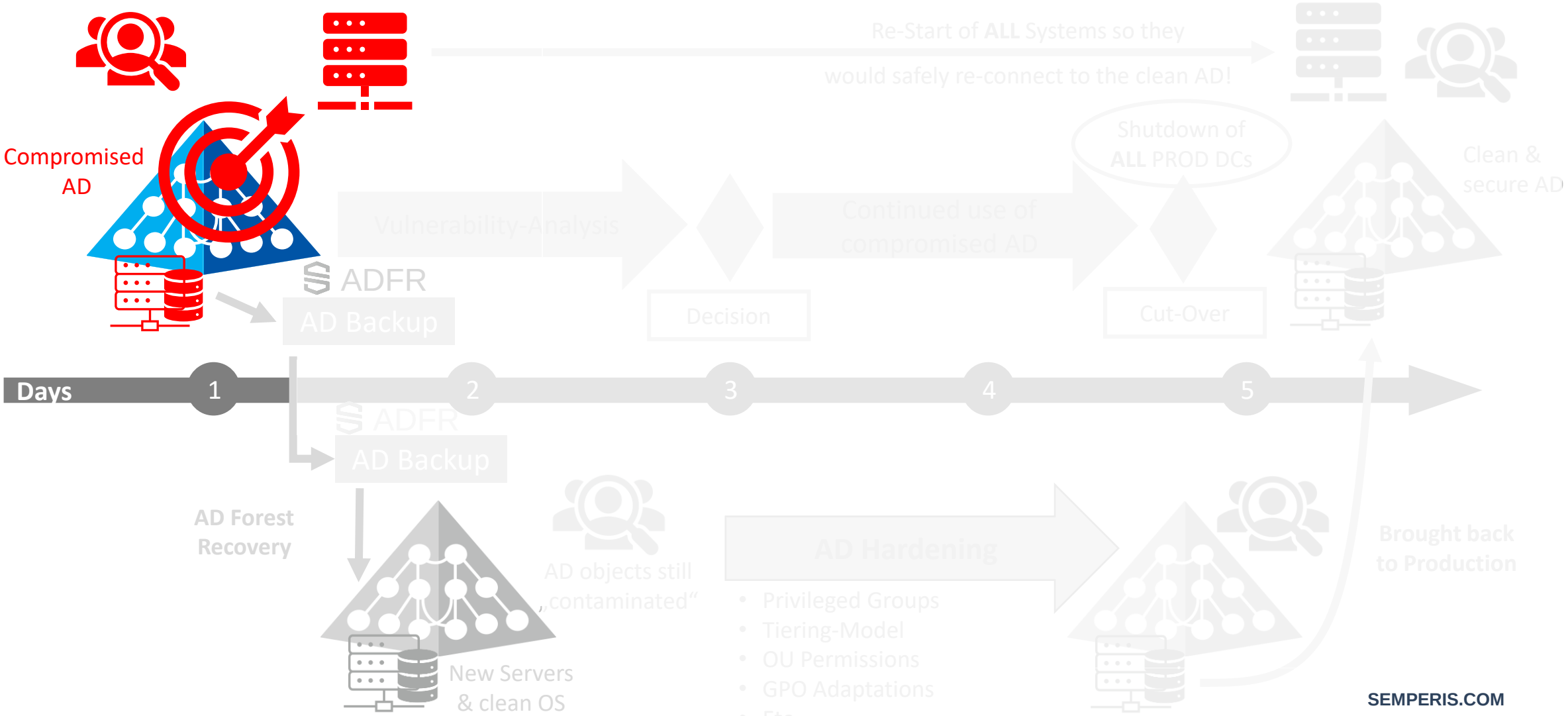


Die Angreifer sind schon DRINNEN !!!

semperis

Compromised Network

Isolated Network

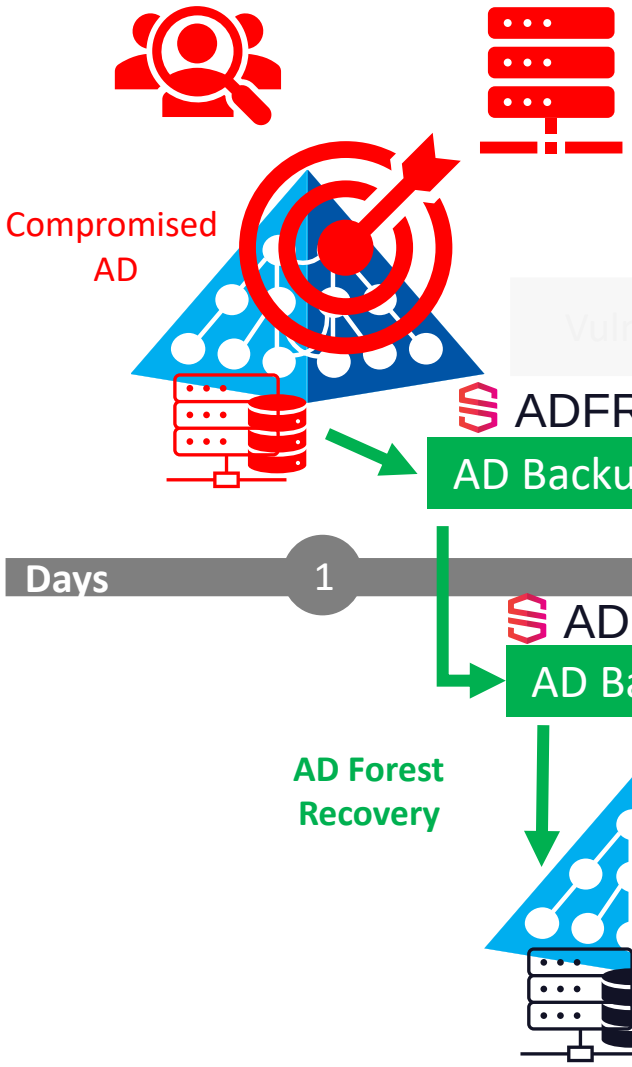


PHASE I – SICHERHEITS-NETZ für AD

semperis

Compromised Network

Isolated Network



Re-Start of **ALL** Systems so they would safely re-connect to the clean AD!

Shutdown of **ALL** PROD DCs

Clean & secure AD

Vulnerability-Analysis

Continued use of compromised AD

Decision

Cut-Over

3

4

5

AD objects still „contaminated“

AD Hardening

- Privileged Groups
- Tiering-Model
- OU Permissions
- GPO Adaptations
- Etc.

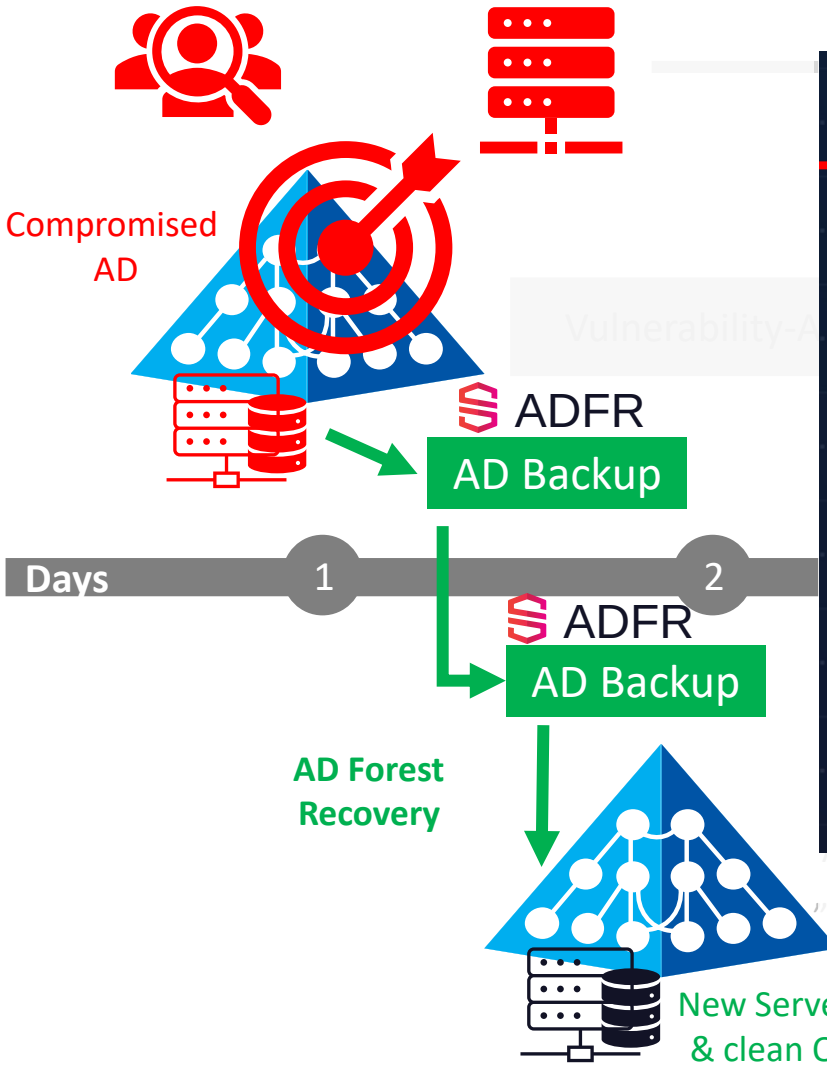
Brought back to Production

PHASE I – SICHERHEITS-NETZ für AD

semperis

Compromised Network

Isolated Network



BACKUP COMPARISON

ADFR vs. other Domain Controller backups

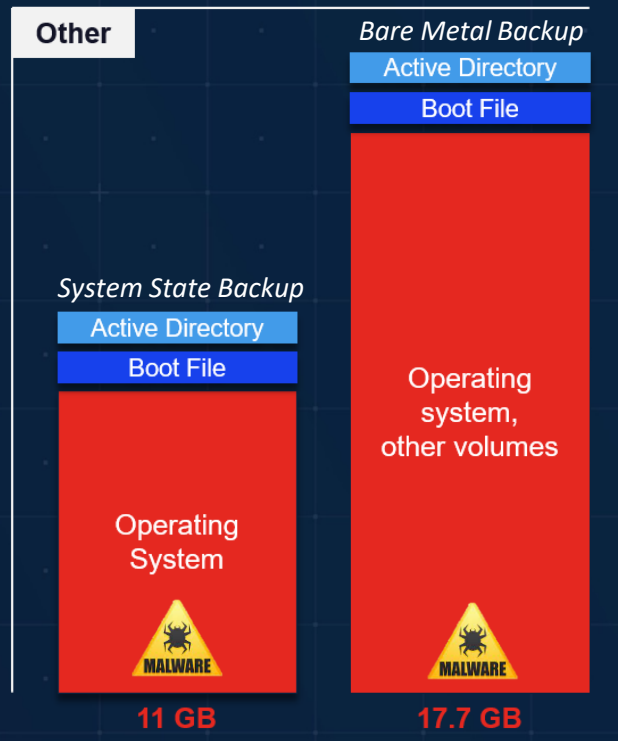
ADFR

116 MB (500 MB uncompressed)

- Active Directory
- Boot File

ADFR backups

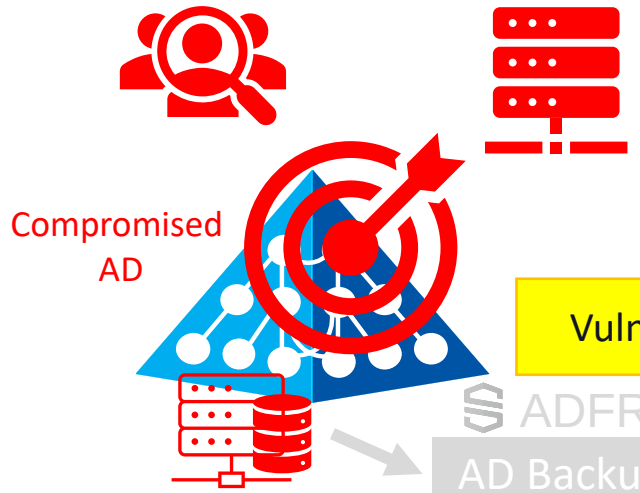
- ✓ Contain no OS → no OS-resident malware in recovery
- ✓ Remove dependence on source hardware → recover anywhere
- ✓ Are significantly smaller
- ✓ Provide faster backup and recovery
- ✓ Require less storage



PHASE II – AD Schwachstellen Analyse

semperis

Compromised Network



Vulnerability-Analysis

Decision

ADFR

AD Backup

Days 1 2 3 4 5

ADFR

AD Backup

Isolated Network

Re-Start of **ALL** Systems so they would safely re-connect to the clean AD!

Shutdown of **ALL** PROD DCs

Continued use of compromised AD

Cut-Over

Clean & secure AD

AD Forest Recovery

AD objects still „contaminated“

New Servers & clean OS

AD Hardening

- Privileged Groups
- Tiering-Model
- OU Permissions
- GPO Adaptations
- Etc.

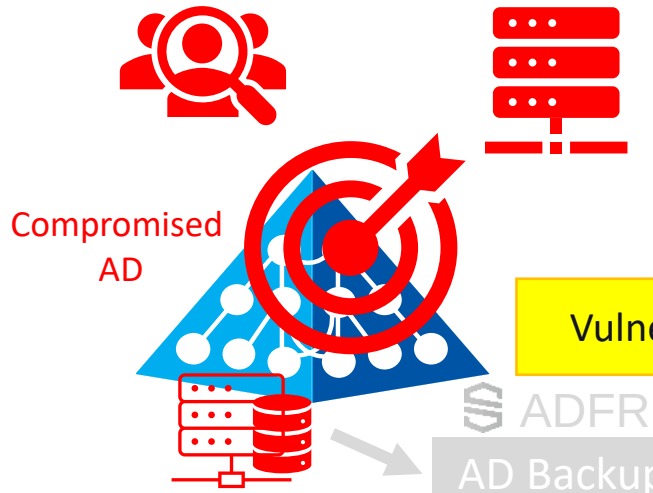
Brought back to Production

PHASE II – AD Schwachstellen Analyse

semperis

Compromised Network

Isolated Network



Vulnerability-Analysis

Decision

PURPLE KNIGHT

ADFR
AD Backup

ADFR
AD Backup

Days 1 2 3

FREE → www.purple-knight.com
www.purple-knight.com/forest-druid

BLOODHOUND

forest druid
powered by semperis

Gefährliche AD-Rechte & MEHRERE Angreifer

SECURITY INDICATOR

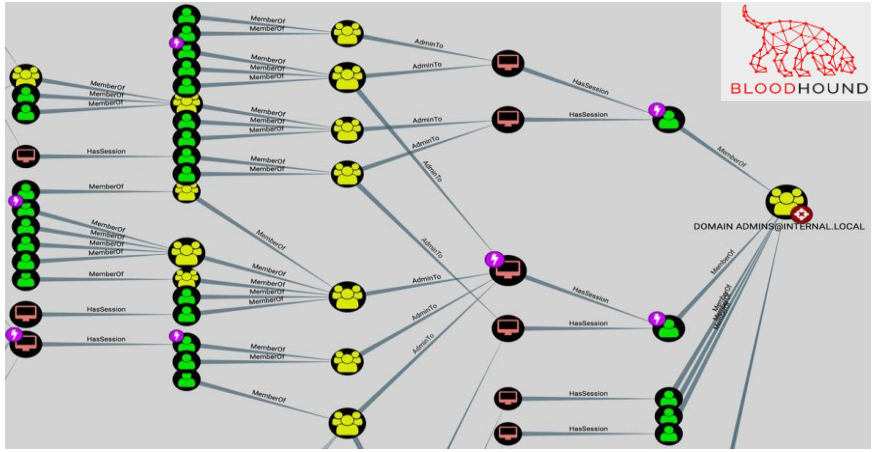
Dangerous control paths expose certificate templates

SEVERITY	WEIGHT
Warning	7

Security Frameworks

MITRE ATT&CK

- Credential Access



Domain Computers were allowed to change certificate templates – which allows intruders to create their own authentication certificates for any user!

A special **helpdesk account** was granted the rights to **reset the password** of everyone in the domain.

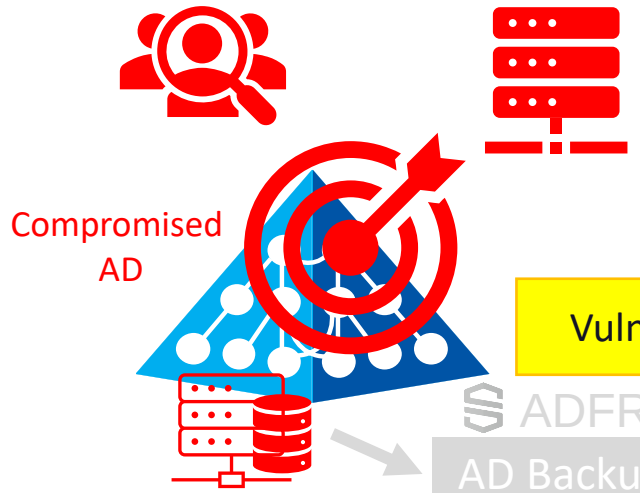
And **EVERYONE** was permissioned to reset the password of the helpdesk account!

Analysis of EDR Team showed that **MULTIPLE attackers were active** in the environment at the SAME time (**four** different “fingerprints” were found) – intruders were happily re-using the existing Domain-Admin accounts whenever one of the AD admins changed their password!

PHASE II – AD Schwachstellen Analyse

semperis

Compromised Network



Vulnerability-Analysis

Decision

ADFR

AD Backup

Days 1 2 3 4 5

ADFR

AD Backup

Isolated Network

Re-Start of **ALL** Systems so they would safely re-connect to the clean AD!

Shutdown of **ALL** PROD DCs

Continued use of compromised AD

Cut-Over

Clean & secure AD

AD Forest Recovery

AD objects still „contaminated“

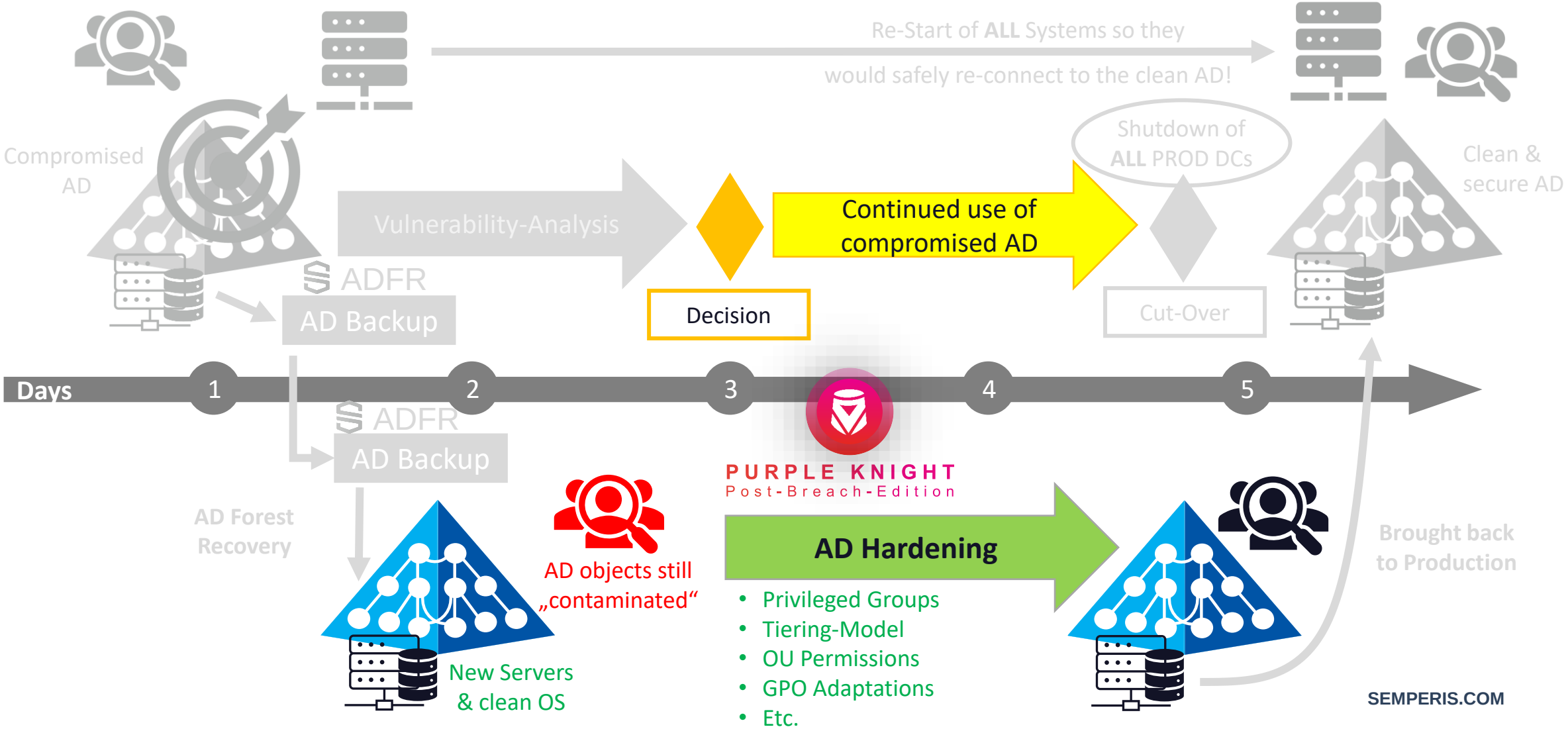
New Servers & clean OS

AD Hardening

- Privileged Groups
- Tiering-Model
- OU Permissions
- GPO Adaptations
- Etc.

Brought back to Production

PHASE III – Divide and Conquer!

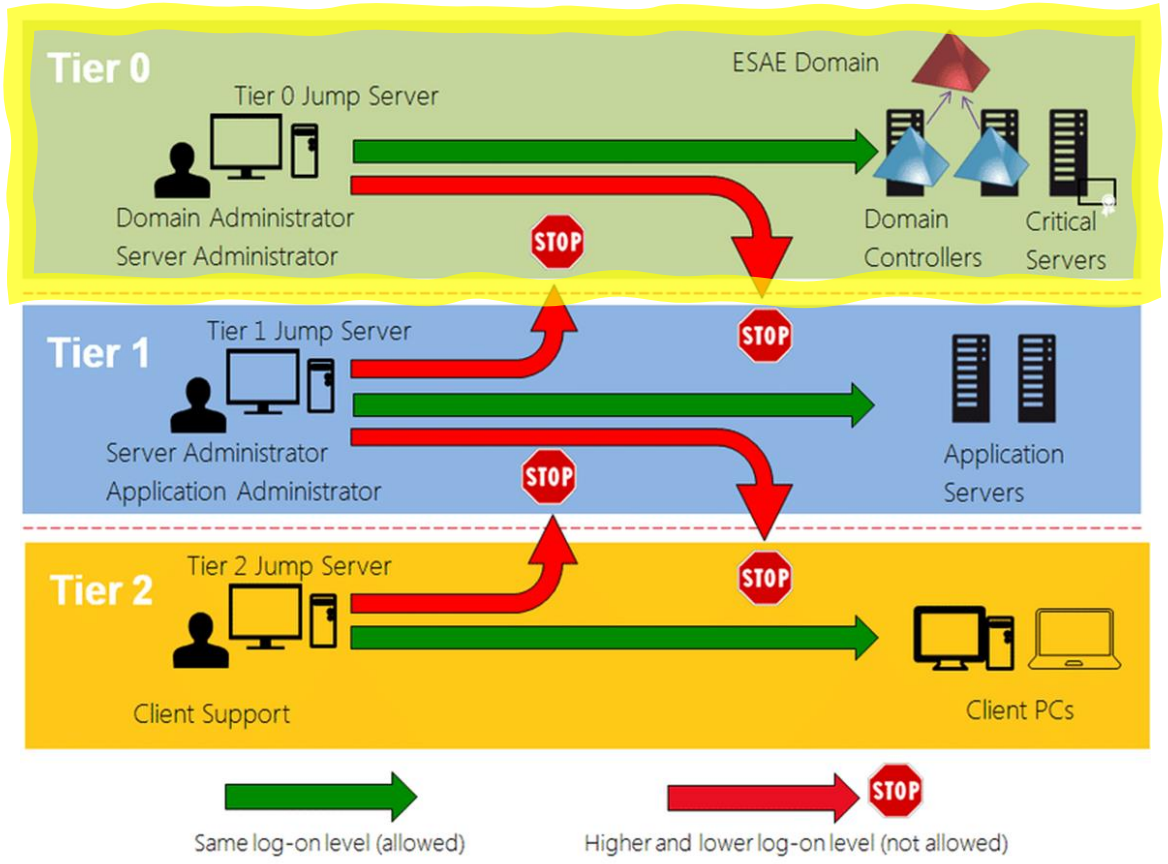


AD Härtungs-Autobahn …

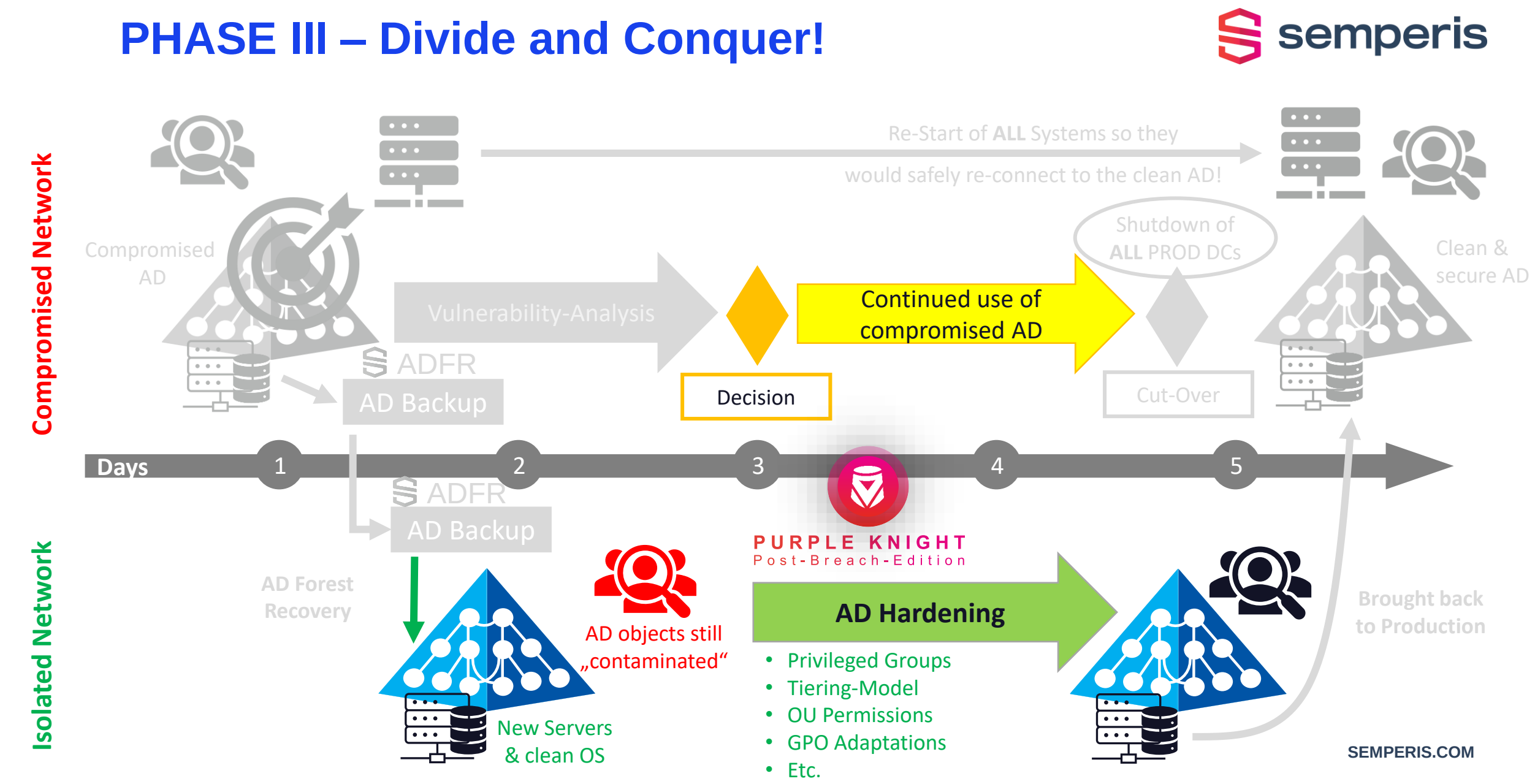
1.5 Tage verfügbar um AD zu härten

- Tiering-Model (w/o MFA)
- NEW accounts in Privileged Groups
- Protected Users group
- No Privileged Accounts with SPNs
- OU Permissions
- GPO Adaptations
- …

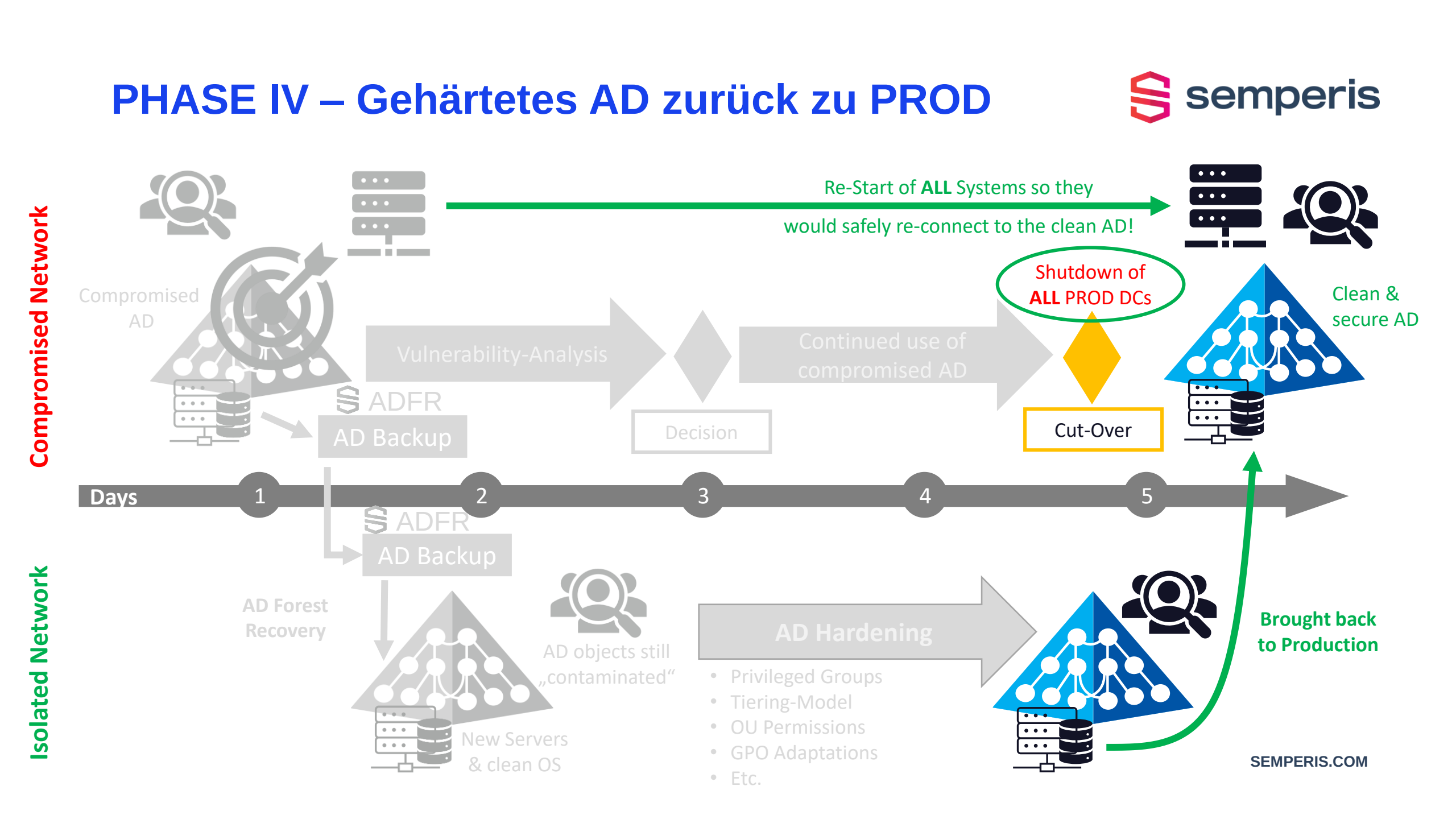
Source: Microsoft



PHASE III – Divide and Conquer!



PHASE IV – Gehärtetes AD zurück zu PROD

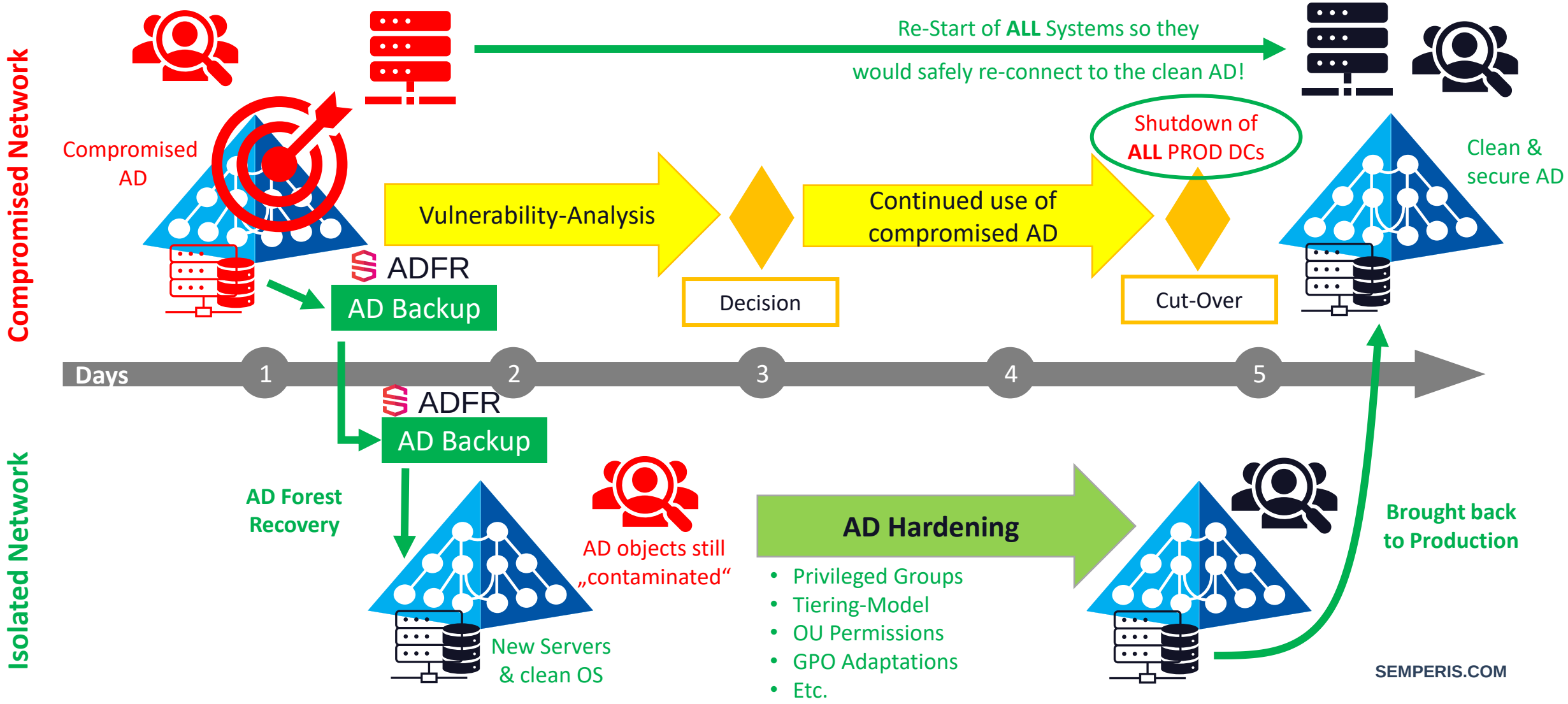


Quelle: https://www.youtube.com/watch?v=cIpBpGQ0XTI

… oder suche nach “changing tires while driving” ☺

Der Ernstfall – das Opfer hat ÜBERLEBT!

semperis



Kernergebnis

1. Sehr SCHNELLE Wiederherstellung eines funktio… und SICHEREN Active Directory Forest
2. Keine gehackten privilegierte Ke… für die Angreifer mehr im Zugriff
3. Alle existierenden … AAD *„Pass-Through Authenticati…* 365 haben nach der Wiederherstellung proble… ktioniert

Semperis hat geholfen, dass sie überleben!

semperis

PRODUKTANGEBOT

Semperis Purple Knight™

(PK) **Bewertung der Sicherheit eines Kunden AD** mithilfe eines Active Directory-Sicherheitsscanners, der von der Elite der Microsoft-Identitätsexperten entwickelt und gepflegt wird.

Semperis Directory Services Protector™

(DSP) **Echtzeit-Tracking und AD-Auditing** mit granularer Suche, Abgleich und Wiederherstellung von Objekten und Attributen mit höchster Datenintegrität durch Quellkorrelation.

On-Premise Active Directory und Azure Active Directory

Semperis Active Directory Forest Recovery™

(ADFR) **Vollständig automatisierte AD Forest Disaster-Recovery** mittels eines einfachen Restore-Wizards, erstmalig mit Hardware-agnostischer & Malware-freier AD-Wiederherstellung.

Thank you

Fragen? Kommt zum Round-Table 5 …

Guido Grillenmeier

Semperis Principal Technologist, EMEA

guidog@semperis.com

www.linkedin.com/in/guidogrillenmeier