semperis

Active Directory: Back from Hell

or per Gartner: The Identity Immune System

Oliver Keizers

AVP EMEA Central, Semperis

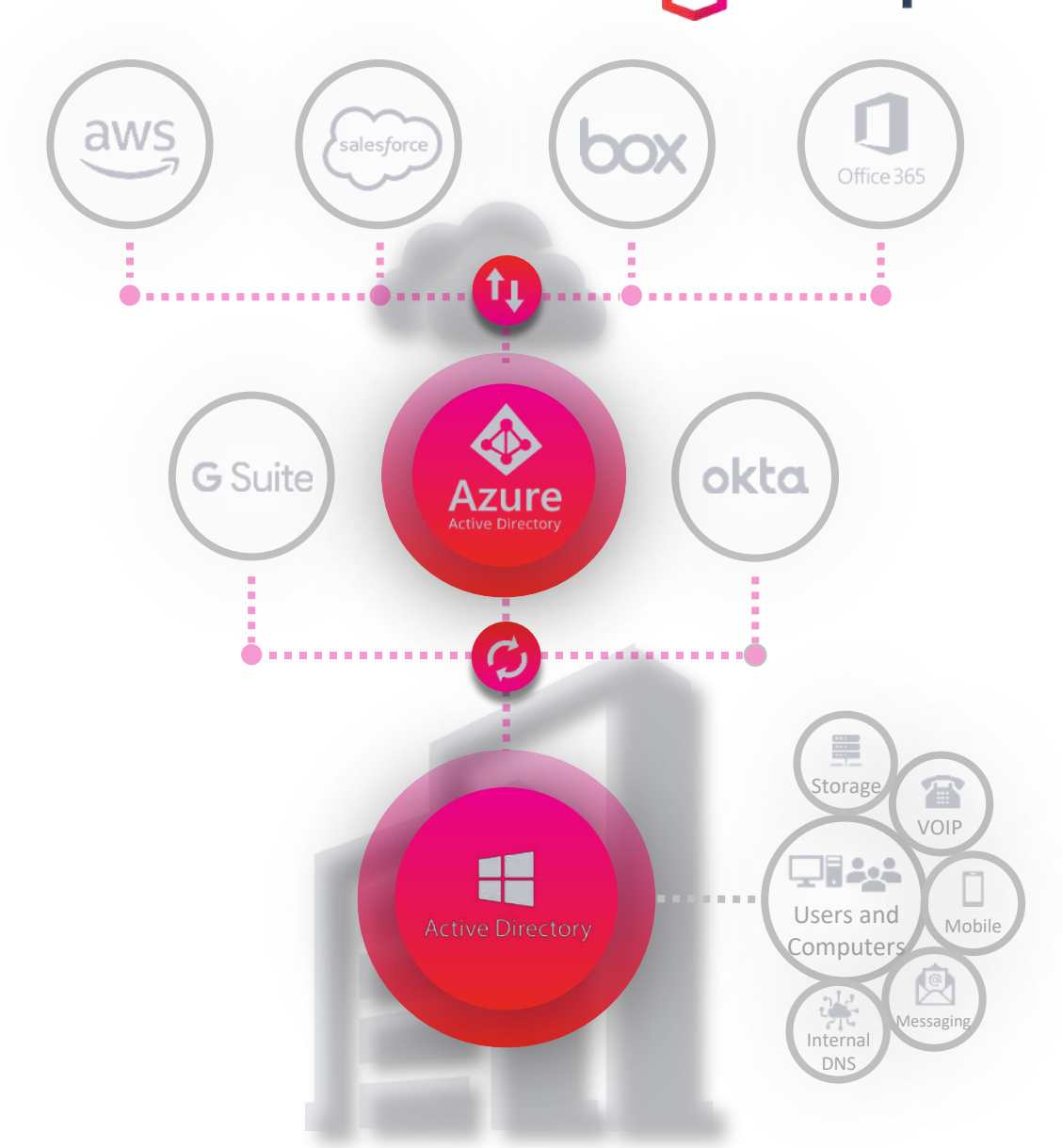
semperis

KEYS TO THE KINGDOM

Identity is the new perimeter! If AD isn't secure, nothing is

It's easy to forget how dependent an organization has become on Active Directory.

- Cloud identity ***extends*** from AD
- Systemic weakness make AD a ***soft target***
- 80% of all breaches involve ***credential abuse***
- Zero trust model assumes ***AD integrity***



Phases of a Ransomware-Attack

semperis

Initial Access

- Phishing emails
- Malicious websites
- Targeted attacks with **stolen credentials**

Post Exploit

- Download of malware for **Recon-Phase**
- Connection to C2* systems
- Remote connection established

Reconnaissance

- Evaluation of **AD vulnerabilities** to gain domain-dominance
- Lateral movement to other systems
- Credential harvesting and privilege escalation

Core attack

- Access to and Extraction of core-business data
- Encryption of devices, often **including AD DCs**

* C2 = Command-and-Control

semperis

Activities	Time
Initial access	T0
Reconnaissance / nltest, net, whoami	T0 + 30 minutes
Command and Control / Loading Meterpreter agent	T0 + 4 hours
Privilege Escalation / Zerologon exploitation	T0 + 4 hours
Command and Control / Cobalt Strike beacon execution	T0 + 6 hours
Credential Theft / registry hive	T0 + 6 hours
Reconnaissance / adfind, ping, curl	T0 + 6 hours and 30 minutes
Credential Theft and Privilege Escalation / LSASS memory dump with procdump64.exe	T0 + 19 hours
Credential Theft / NTDS.dit exfiltration with Active Directory full privilege	T0 + 22 hours
Lateral Movement / Cobalt Strike socks-tunnel (RDP)	T0 + 24 hours
Data Exfiltration / Rclone	T0 + 3 days

Bumblebee gained Domain Dominance is just 19 hours after initial access

Source: Cybereason THREAT ANALYSIS REPORT, August 2022 - *Bumblebee Loader – The High Road to Enterprise Domain Control*
https://www.cybereason.com/blog/threat-analysis-report-bumblebee-loader-the-high-road-to-enterprise-domain-control

semperis

#1 Top Trend

Identity Threat Detection and Response (ITDR) is a Gartner “top trend” for cybersecurity in 2023

“While organizations understand the criticality of AD, the security of AD is often overlooked. If AD is breached, an attacker gets virtually unrestrained access to the organization’s entire network and resources. **This makes AD a prominent high-value target for threat actors**.”

Gartner

Emerging Technologies and Trends Impact Radar: Security

semperis

Gartner recommends AD-specific security and recovery.

"Tools from vendors such as … **Semperis** … offer a more complete backup and recovery platform for Active Directory than those found in the Active Directory backup modules included in most enterprise backup software."

"Organizations without a useful backup system will be left with few options but to ***pay the ransom****."* — Nik Simpson, Gartner

Source: How to Protect Backup Systems from Ransomware (Gartner)

Steps to Manually Perform a Forest Recovery

1. Pull the network cables from all DCs or otherwise disable
2. Connect DCs to be restored to a private network (oh yes - establish a global private VLAN)

For each domain,

3. Nonauthoritative restore of first writeable DC
4. Auth restore of SYSVOL on that DC
5. Look for malware, etc. Forensic analysis: is it safe to continue?
6. Reset all admin account passwords
7. Seize FSMOs
8. Metadata cleanup of all writeable DCs except for targeted seed forest DCs
9. Configure DNS on the forest root DC
10. Remove the global catalog from each DC.

<Wait for GC to be removed…>

11. Delete DNS NS records of DCs that no longer exist
12. Delete DNS SRV records of DCs that no longer exist
13. Raise the RID pool by 100K
14. Invalidate the current RID pool
15. Reset the computer account of the root DC twice
16. Reset krbtgt account twice

<you have a seed forest at this point>

17. Configure Windows Time
18. Verify replication health
19. Add GC to a DC for each OS version in each domain

<Wait for GCs to be created…>

20. Take a backup of all DCs in the seed forest
21. Create an IFM package for each OS version, in each domain, your DCs are running
22. Build out seed forest with additional DCs to support Tier 0 / Tier 1 operations:

For each DC to be repromoted into the seed forest,

23. Clean up the (former) DC using /FORCEREMOVAL or rebuild OS
24. Send IFM package to server

<Wait>

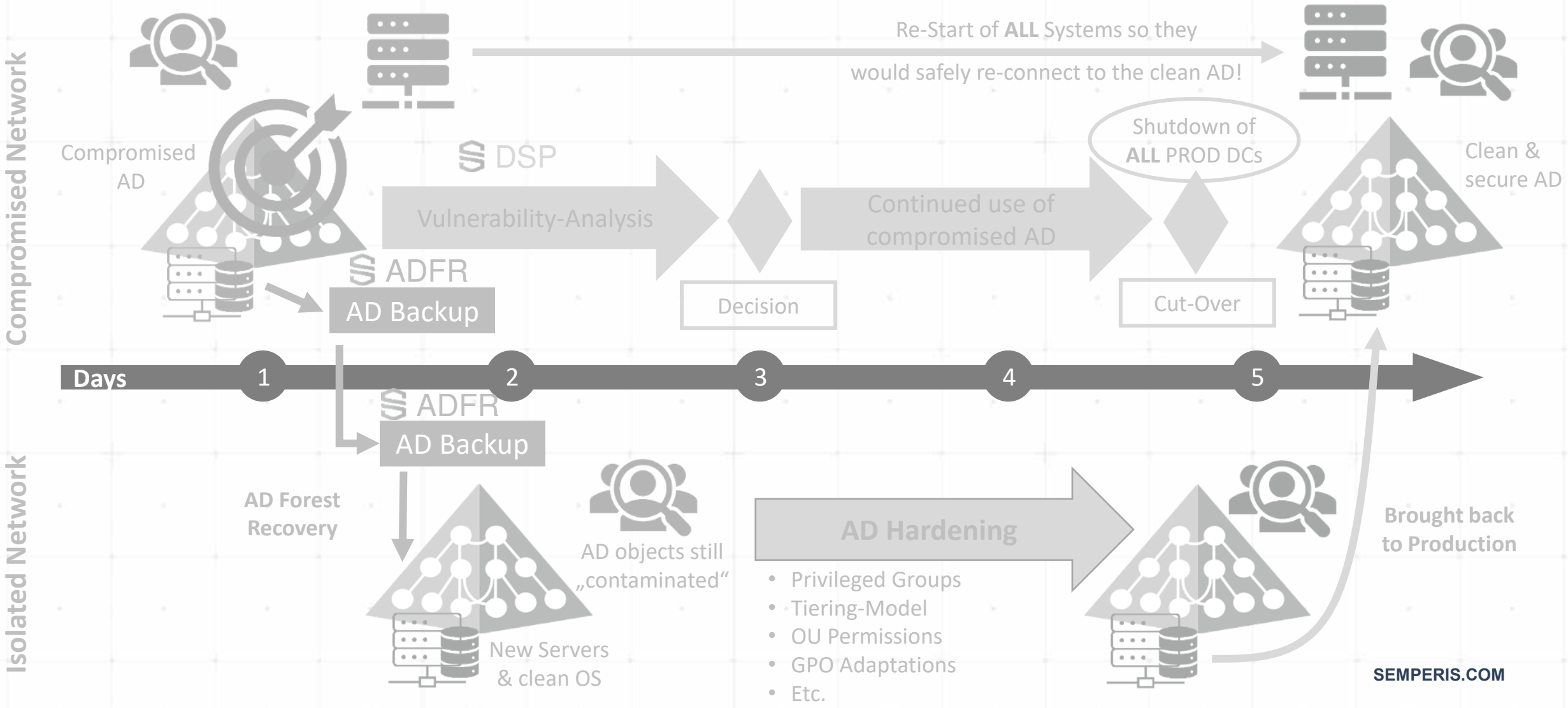
25. Take the DC off the public network and put it on the seed forest network.
26. Run a DCPROMO IFM

<Days pass…>
<Large enough forest to support basic operations>

27. Verify health of the full forest
28. Move restored forest to the corporate network

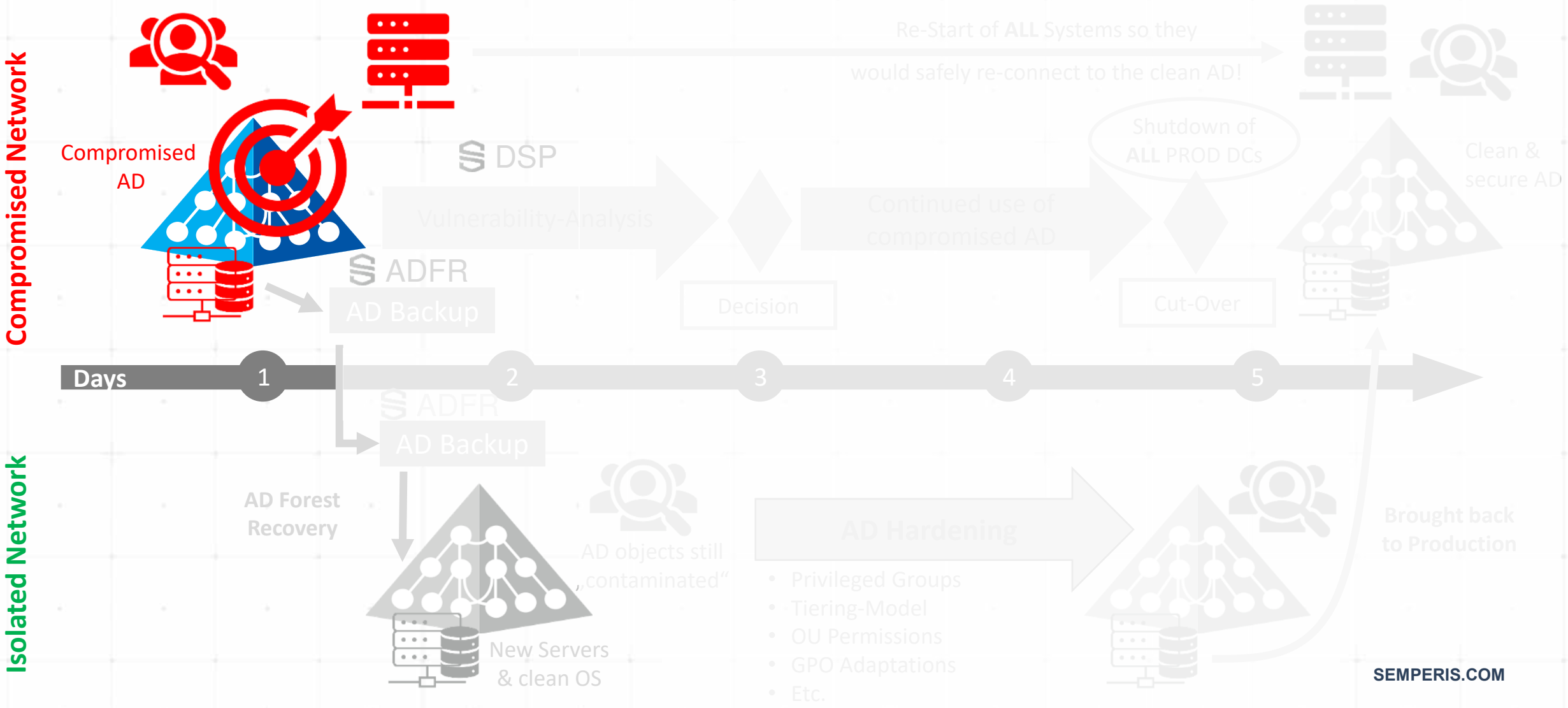
Microsoft Whitepaper: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/ad-forest-recovery-guide

Real life AD-incident example – the AD details

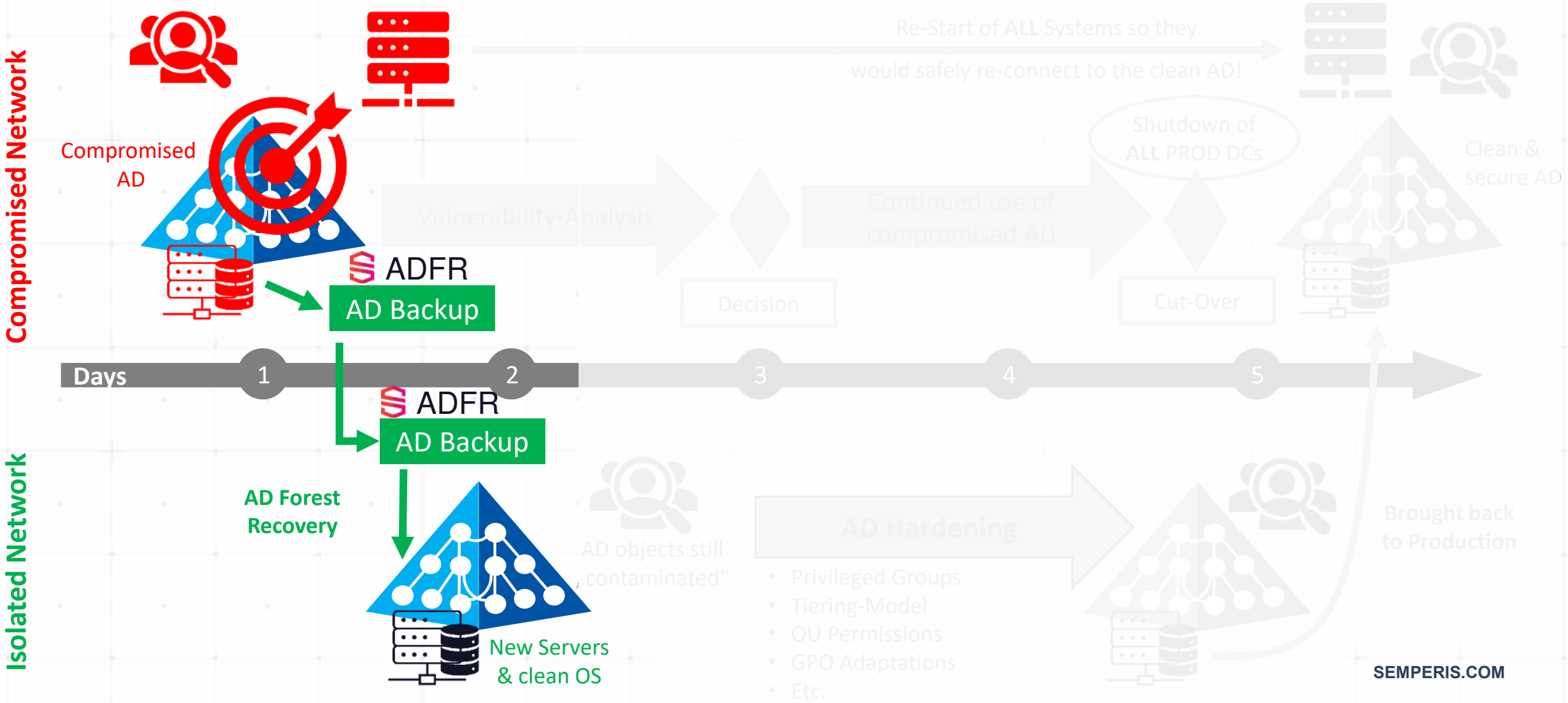


SEMPERIS.COM

You've been BREACHED !!!



PHASE I – Spin up a SAFETY NET for AD



PHASE II – AD Vulnerability Analysis

semperis

Compromised Network

Compromised AD

DSP

Vulnerability-Analysis

Decision

ADFR

AD Backup

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

Days 1 2 3 4 5

Isolated Network

ADFR

AD Backup

AD Forest Recovery

New Servers & clean OS

AD objects still „contaminated“

AD Hardening

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

Brought back to Production

PHASE II – AD Vulnerability Analysis

semperis

Compromised Network

Compromised AD

DSP

Vulnerability-Analysis

Decision

PURPLE KNIGHT

www.purple-knight.com

ADFR

AD Backup

Days 1 2 3 4 5

Isolated Network

ADFR

AD Backup

forest druid

powered by semperis

PHASE II – AD Vulnerability Analysis

semperis

Compromised Network

Compromised AD

DSP

Vulnerability-Analysis

Decision

ADFR

AD Backup

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

Days 1 2 3 4 5

Isolated Network

ADFR

AD Backup

AD Forest Recovery

New Servers & clean OS

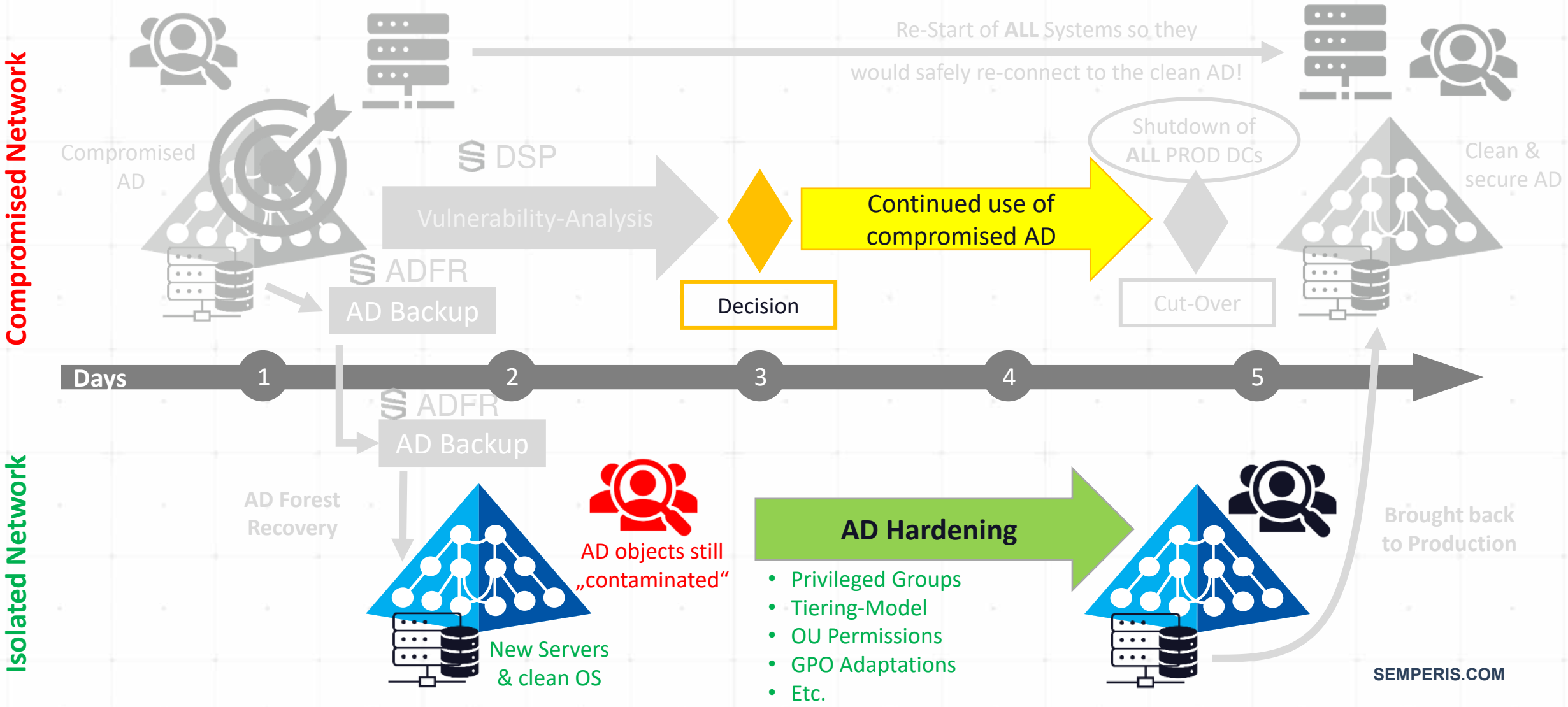
AD objects still „contaminated“

AD Hardening

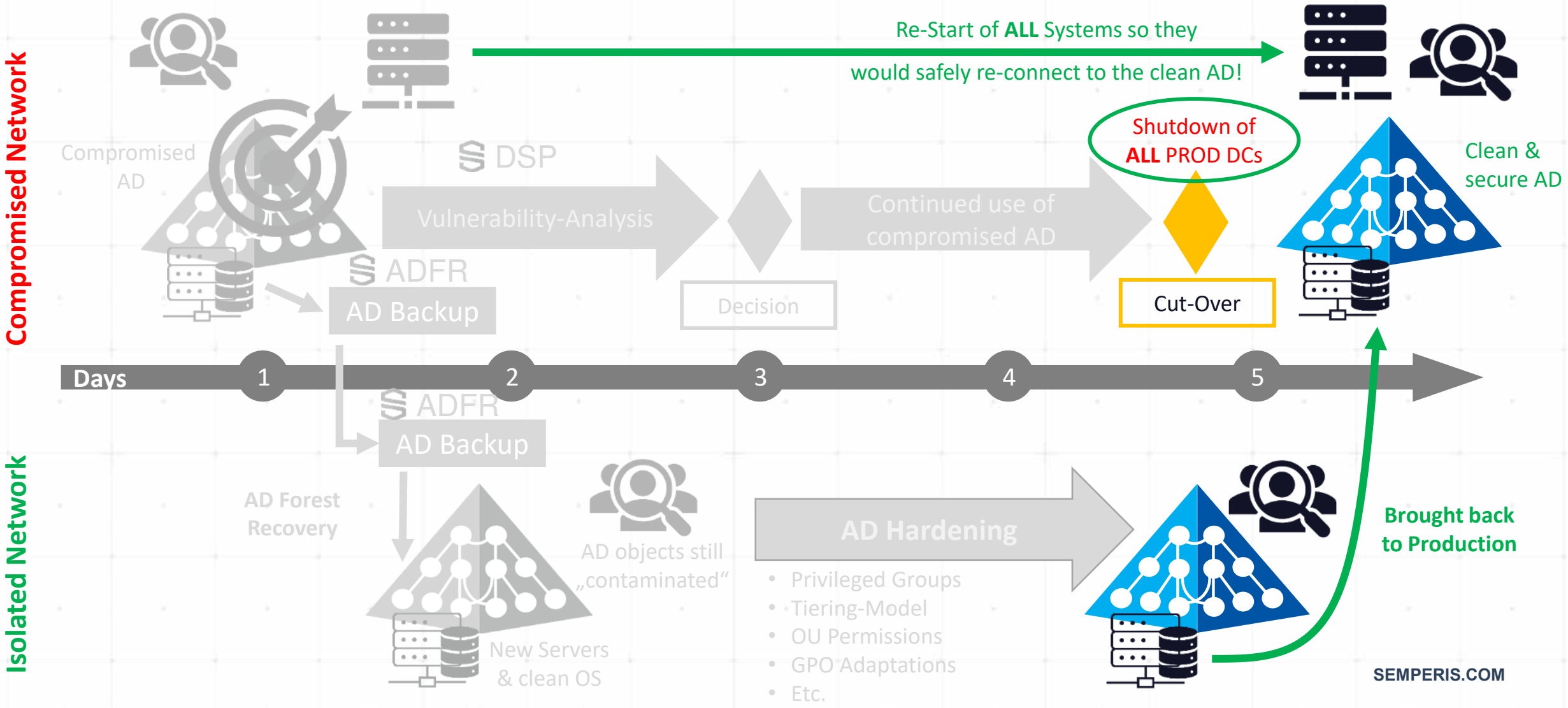
- Privileged Groups
- Tiering-Model
- OU Permissions
- GPO Adaptations
- Etc.

Brought back to Production

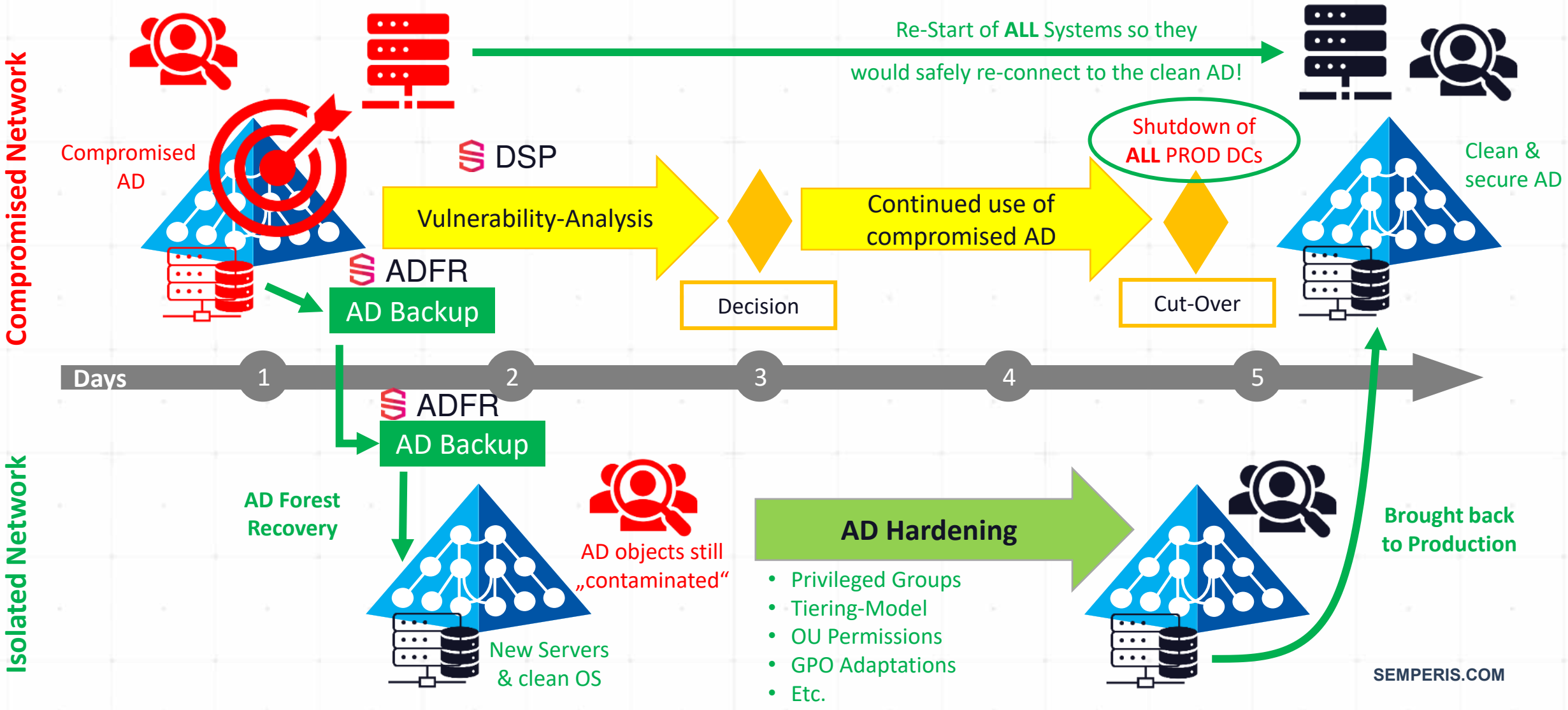
PHASE III – Divide and Conquer!



PHASE IV – Bring hardened AD back to PROD



Real life AD-incident example – they SURVIVED!

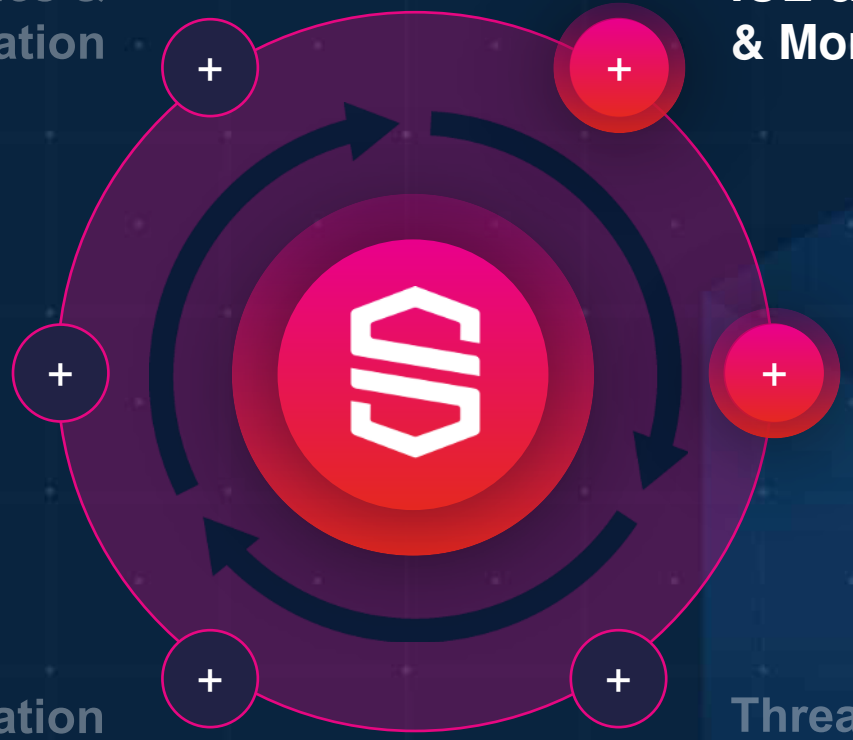


semperis

So, what does it take to secure your AD?

semperis

Before an attack | During an attack | After an attack



Forensics & Investigation

IOE & IOC Discovery & Monitoring

Cyber-First Disaster Recovery

Vulnerability Assessments

Auto-Remediation & IR

Threat Detection & Visibility

Round-the-clock IR global support team

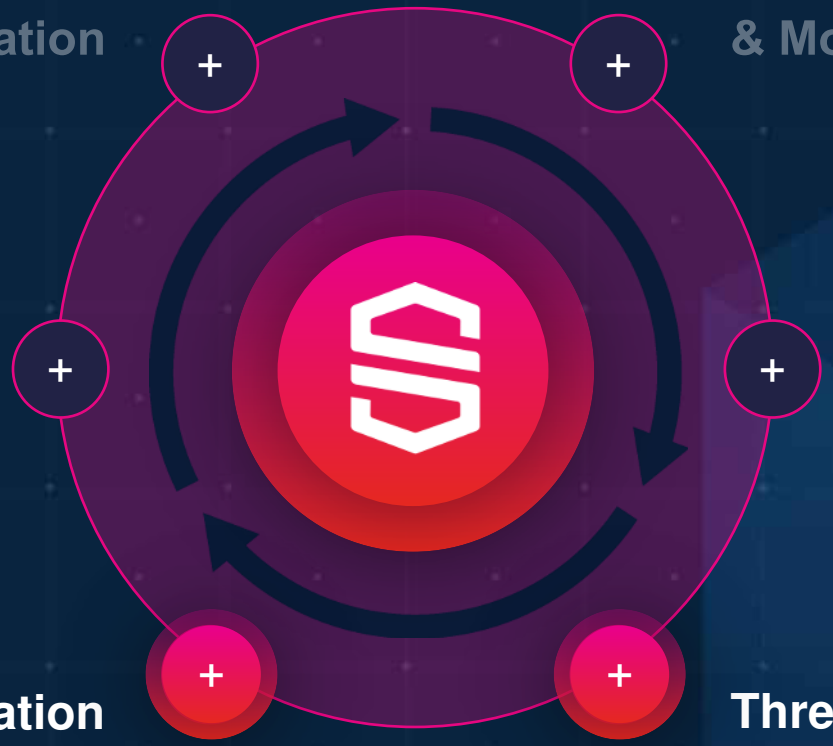
semperis

Before an attack | During an attack | After an attack

Forensics & Investigation

IOE & IOC Discovery & Monitoring

Cyber-First Disaster Recovery



Vulnerability Assessments

Auto-Remediation & IR

Threat Detection & Visibility

Round-the-clock IR global support team

semperis

Before an attack → During an attack → After an attack

Forensics & Investigation

IOE & IOC Discovery & Monitoring

Cyber-First Disaster Recovery

Vulnerability Assessments

Auto-Remediation & IR

Threat Detection & Visibility

Round-the-clock IR global support team

semperis

SOLUTIONS OVERVIEW

Semperis Free Tools
Purple Knight™
Forest Druid™

(PK) **Purple Knight to evaluate the config & security** of your Active Directory.

(FD) **Forest Druid to discover attack paths** for defensive teams to prevent privileged domain access.

Semperis Directory Services Protector™

(DSP) **Real-time tracking and AD auditing** providing granular search, comparison and restoration of objects and attributes with superb data integrity through source correlation.

On-Premise Active Directory and Azure Active Directory

Semperis Active Directory Forest Recovery™

(ADFR) **Fully automated disaster recovery orchestration** through a simple restoration wizard, introducing the first hardware-agnostic Active Directory recovery.

semperis

What does it take to manually perform an Active Directory forest recovery?

Days to weeks…

1. Pull the network cables from all DCs or otherwise disable network

2. Connect DCs to be restored to a private network (*Oh yes - establish a global private VLAN*)

For each domain:

3. Nonauthoritative restore of first writeable DC
4. Auth restore of SYSVOL on that DC
5. Remediate malware
6. Reset all admin account passwords
7. Seize FSMOs
8. Metadata cleanup of all writeable DCs except for targeted seed forest DCs
9. Configure DNS on the forest root DC
10. Remove the global catalog from each DC.
(Wait for global catalog to be removed)

11. Delete DNS NS records of DCs that no longer exist

12. Delete DNS SRV records of DCs that no longer exist

13. Raise the value of available RID pools by 100K

14. Invalidate the current RID pool for every DC

15. Reset the computer account of the root DC twice

16. Reset krbtgt account twice
(You have a seed forest at this point)

17. Configure Windows Time

18. Verify replication between seed DCs

19. Add GC to a DC for each OS version in each domain
(Wait for GCs to be created)

20. Take a backup of all DCs in the seed forest

21. Create an IFM package for each OS version, in each domain your DCs are running

22. Build out seed forest with additional DCs to support Tier 0 / Tier 1 operations

For each DC to be repromoted into the seed forest:

23. Clean up the (former) DC using /FORCEREMOVAL or rebuild OS
24. Send IFM package to server (wait…)
25. Take the DC off the public network and put it on the seed forest network.
26. Run a DCPROMO IFM
(Days pass while you clean and rebuild DCs)
(Now you have a large enough forest to support basic operations)

27. Verify health of the full forest

28. Move restored forest to the corporate network

29. Reboot all servers and clients to force communications with the new forest

Semperis' five-click automated AD recovery:

1. Login to console
2. Click **Forest Recovery**
3. Choose backup set to recover from
4. Click **Analyze**
5. Click **Recover**

Compare to:

Semperis' AD Forest Recovery

Minutes to hours…

Semperis orchestrates a fully automated forest recovery process—avoiding human errors, reducing downtime by 90%, and eliminating the risk of malware reinfection.

Important considerations

Manual recovery is error-prone and often requires additional cycles to correct missteps, extending the timeline even further.

General purpose backup only automates step 3, leaving the rest of the recovery process a mostly manual effort.

Required staff for manual AD forest recovery:
Core AD team, operators at every datacenter, plus other external support (Estimated 10-15 IT support staffers in average enterprise)

Required staff for Semperis' ADFR:
Only 1-2 AD admins

The world's biggest brands trust Semperis

93 Net promoter score | 99% Customer retention

Gartner peerinsights 5.0 ★★★★★

#1 Big-box retailer

#1 Consulting service

#1 Hospital network

#1 Airline carrier

#1 Independent bank

#1 Coffeehouse chain

#1 Law firm

#1 Seafood producer

#1 Irrigation manufacturer

#1 Property insurer

#2 Auto insurer

#3 PC vendor

5/5 Largest healthcare companies

2/10 Largest pharma companies

2/10 Largest US cities

2/25 Largest US counties

Top 5 semiconductor manufacturer

54,967,674

identities protected by Semperis (and counting)

Top 10 IT sourcing vendor

*Ranking based on company size and revenue

semperis

Thank you

Questions?

Oliver Keizers

AVP EMEA Central, Semperis

KKR

INSIGHT PARTNERS

Microsoft Partner

Enterprise Cloud Alliance

Microsoft Accelerator Alumni

Microsoft Co-Sell

Inc.5000 N° 3 2021 IND SECURITY

500 Technology Fast 500 2021 NORTH AMERICA Deloitte.

Inc. 5000 Vet100 SBA IVMF

Inc. Best Workplaces

CYBER SECURITY EXCELLENCE AWARDS WINNER 2022

2021 GLOBEE AWARDS GRAND WINNER CYBER SECURITY GLOBAL EXCELLENCE AWARDS

CISO CHOICE AWARDS

2021 FORTRESS CYBER SECURITY AWARD

2021 CYBERCRIME MAGAZINE HOT 150 CYBERSECURITY COMPANIES

GLOBAL INFOSEC AWARDS WINNERS CYBER DEFENSE MAGAZINE 2021

SC 2020 awards Winner