semperis

LSZ

FUTURE CONNECTIONS

Active Directory: Back from Hell

or per Gartner: The Identity Immune System

Oliver Keizers

AVP EMEA Central, Semperis

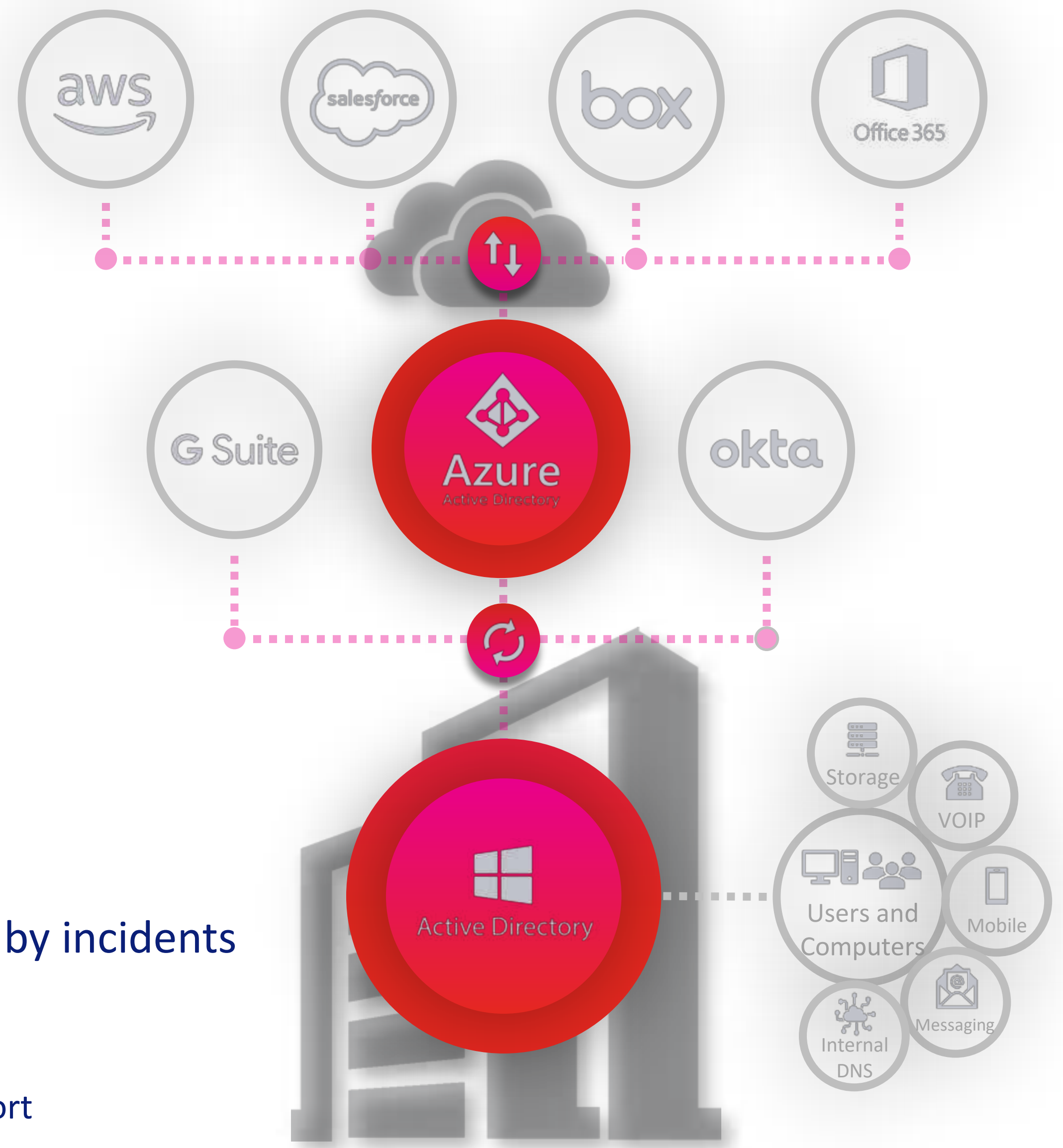
KEYS TO THE KINGDOM

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

- 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***

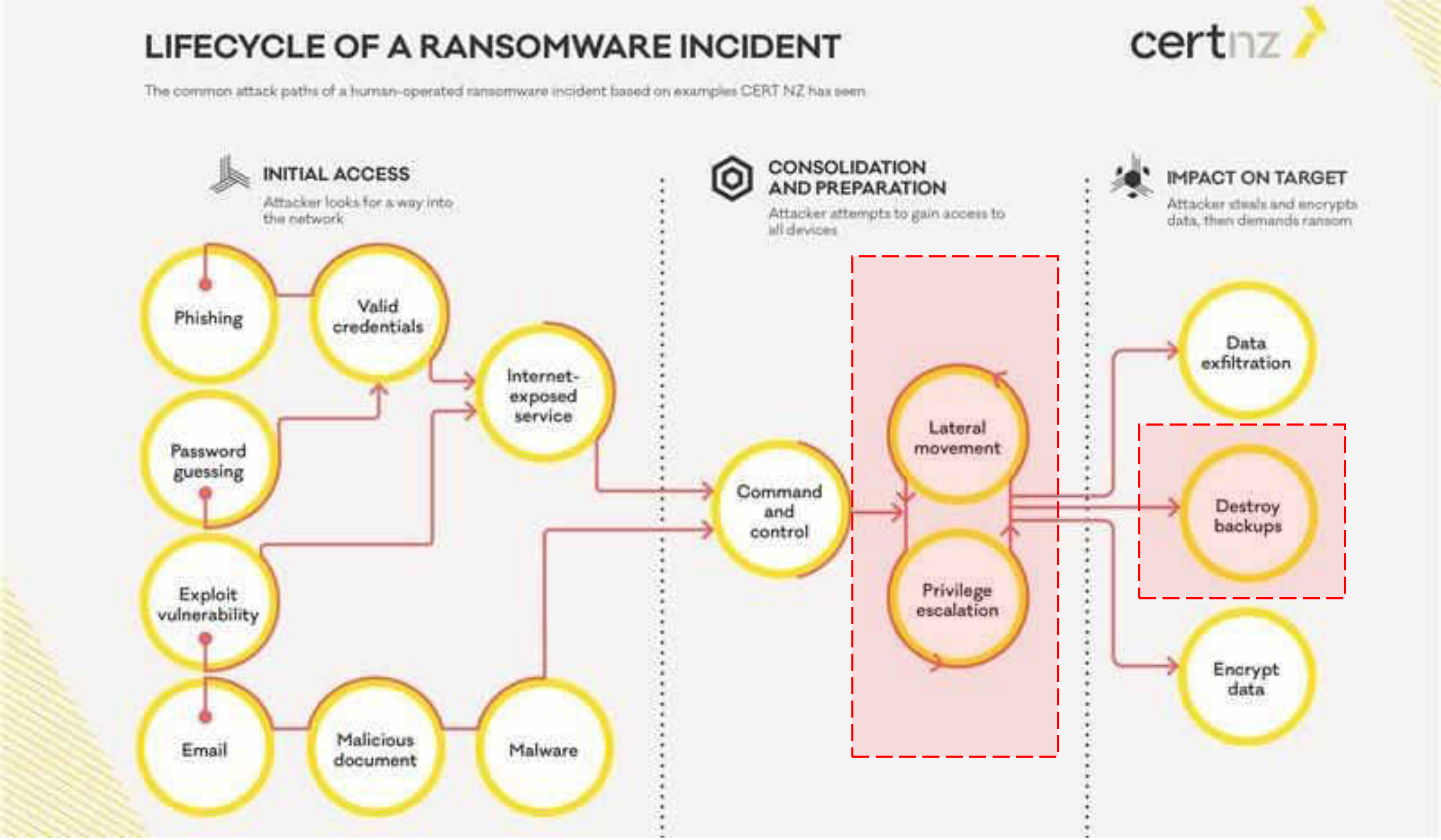
88% of customers impacted by incidents had "insecure AD configuration"

—Microsoft Digital Defense Report



Phases of a Ransomware-Attack

semperis



LIFECYCLE OF A RANSOMWARE INCIDENT

certnz

The common attack paths of a human-operated ransomware incident based on examples CERT NZ has seen

INITIAL ACCESS

Attacker looks for a way into the network

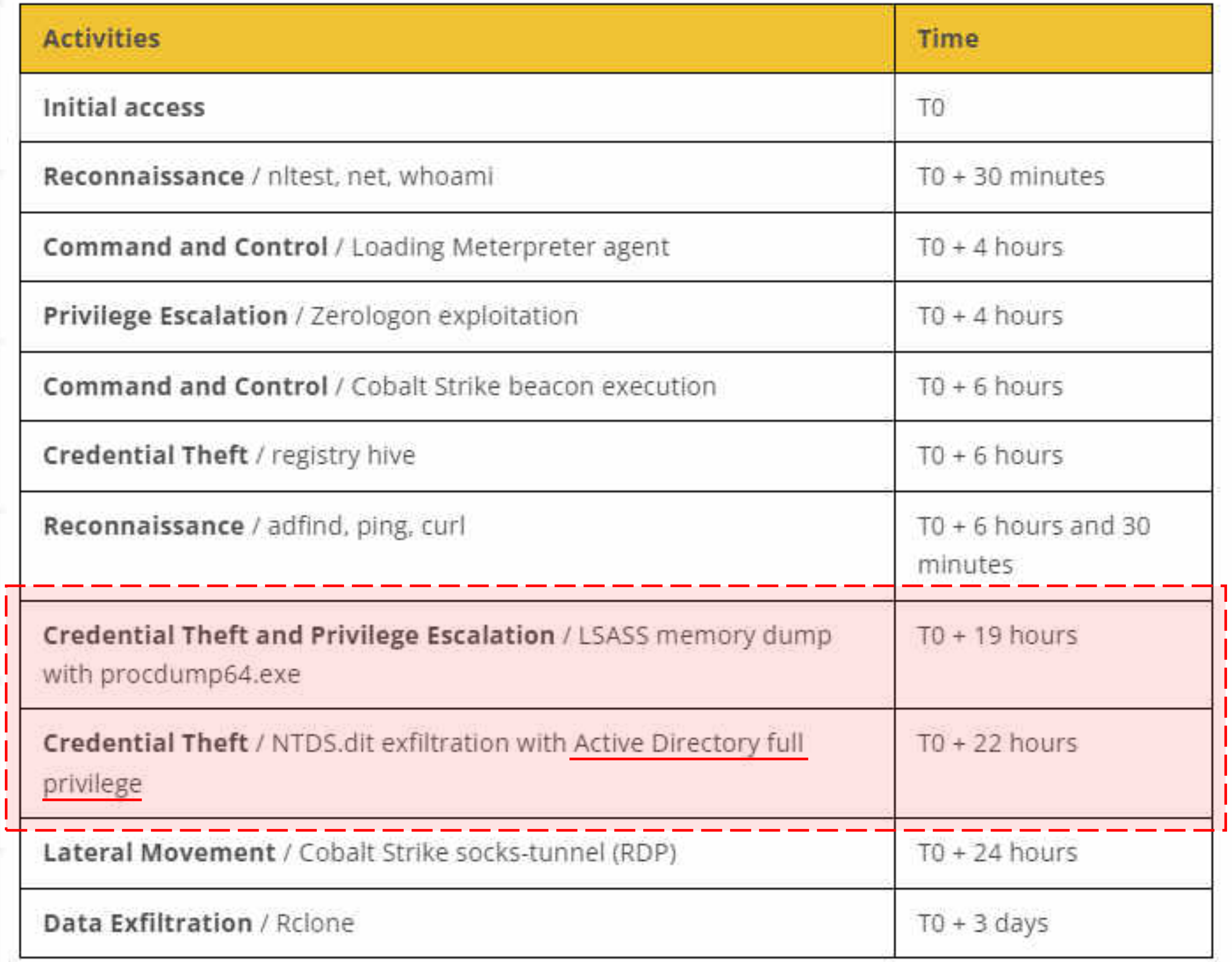
CONSOLIDATION AND PREPARATION

Attacker attempts to gain access to all devices

IMPACT ON TARGET

Attacker steals and encrypts data, then demands ransom

https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/



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

The Five Eyes' urgent guidance on AD security threats

Cybersecurity agencies from the **Five Eyes** alliance, including **CISA** and the **NSA**, are urging organizations to strengthen security around Microsoft Active Directory (AD), a prime target for cyber attackers. A **recent report** highlights more than a dozen tactics used by threat actors to exploit AD and offers protective measures. Due to its widespread use and complexity, AD is especially vulnerable to attacks.

Presentation outline:

- Five Eyes report overview and key take-aways
- Free resources to implement the Five Eyes' AD security guidance
- Semperis' coverage for AD attacks observed in the Five Eyes report
- Semperis' approach to improving AD resiliency
- Q&A

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC

Detecting and Mitigating Active Directory Compromises

First published: September 2024

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

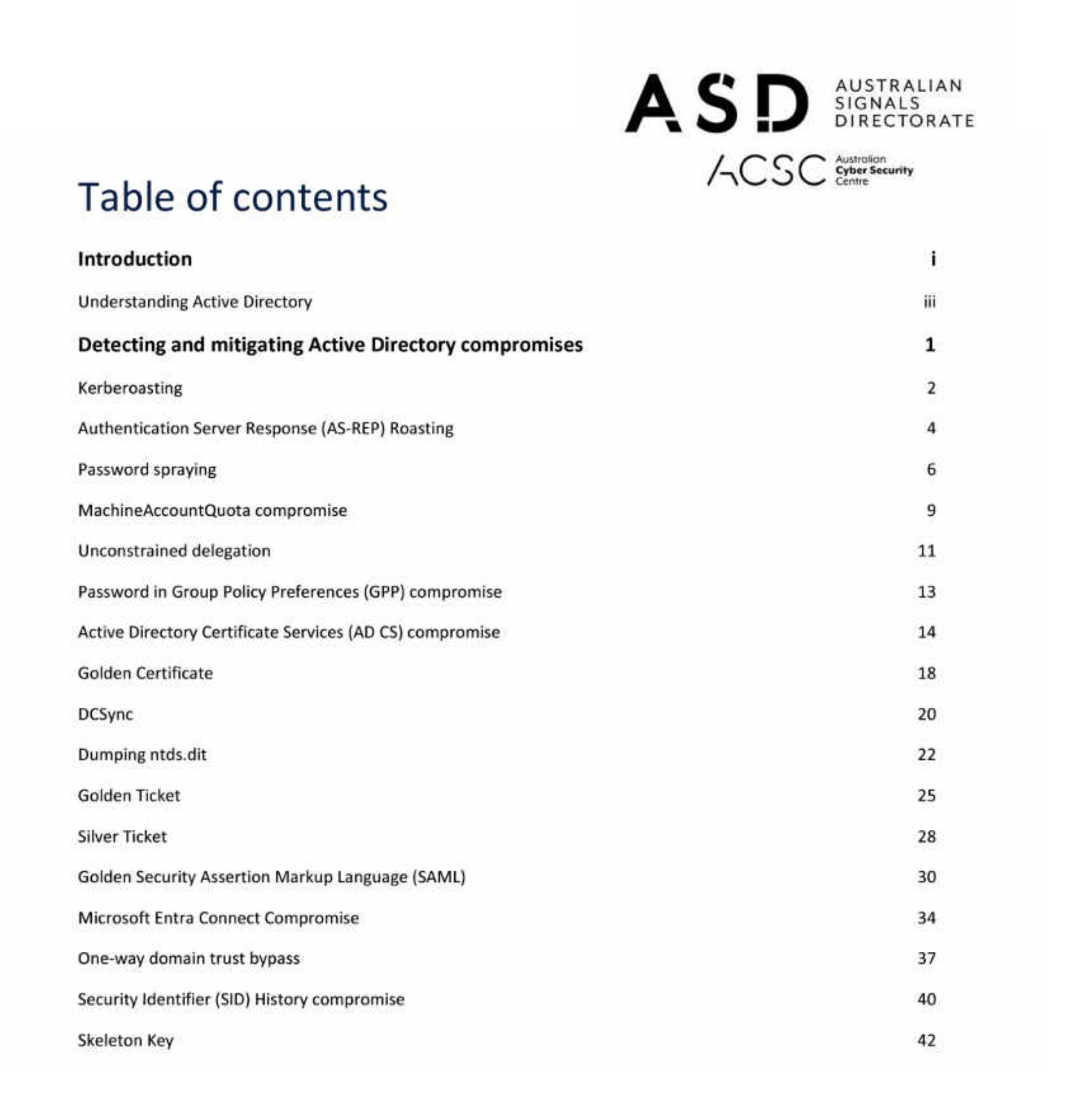
National Cyber Security Centre
a part of GCHQ

National Cyber Security Centre
PART OF THE GCSB

semperis

Common AD attacks observed by the Five Eyes

The report aims to spread awareness about common techniques attackers use to target AD and infiltrate organizations. The warnings underscores the **urgent need** for organizations worldwide to shore up their AD defenses.



ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre

Table of contents

semperis

Key takeaways from the Five Eyes' AD security report:

Securing AD isn't optional—it's essential: As the central hub for authentication and authorization, a breach of AD compromises your entire network.

AD is a prime target: With 90% of organizations using AD, attackers know it's there, often misconfigured, and if they gain control, it's game over.

Persistence is hard to detect: Attackers can remain hidden for months or even years, bypassing defenses.

Complexity gets exploited: Hidden relationships in AD give attackers opportunities to escalate privileges and achieve domain dominance.

Cloud risks extend from AD: A compromised AD often leads to compromised cloud services like Entra ID.

Zero Trust relies on AD: Zero trust becomes irrelevant if the identity system "source of truth" is compromised. When attackers own your AD, they get access to any app or data that depends on AD.

Recovery is costly and disruptive: AD recovery can take weeks if you're not prepared or performing manually.

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

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.”

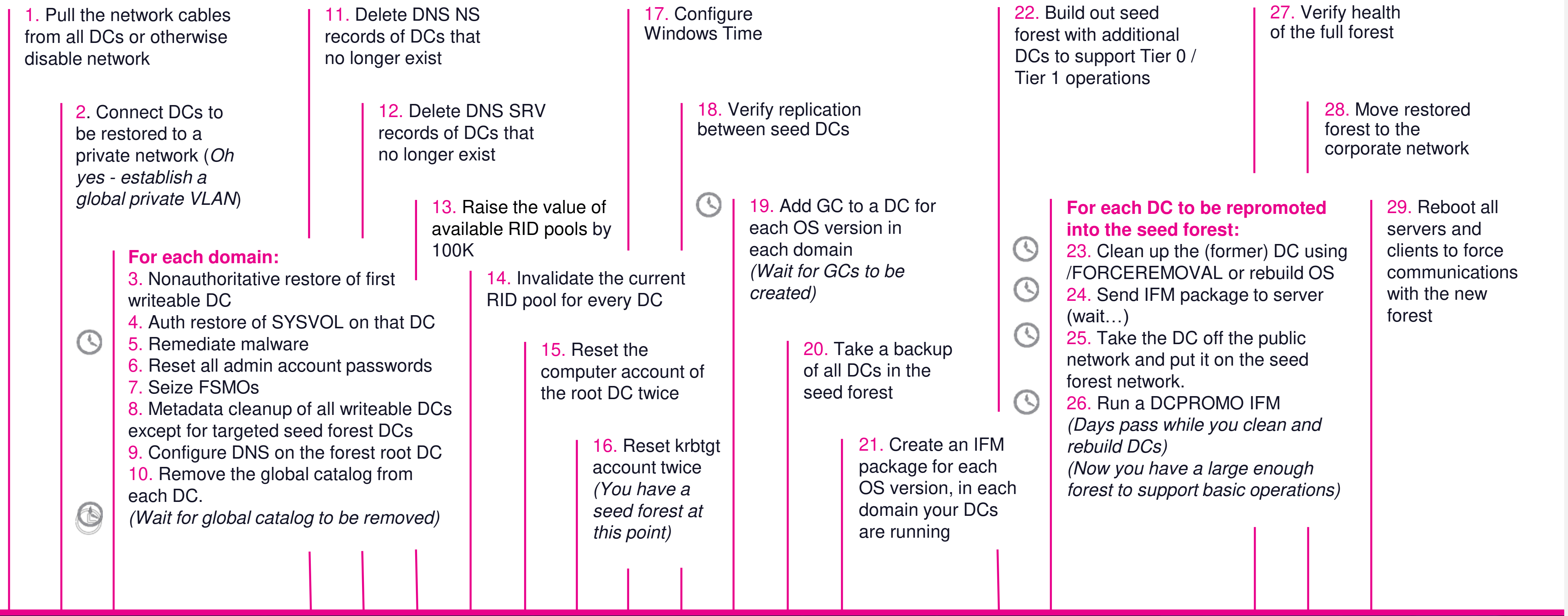
> *“Organizations without a **useful** backup system will be left with few options but to* **pay the ransom.**” — Nik Simpson, Gartner

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

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

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

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.

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.

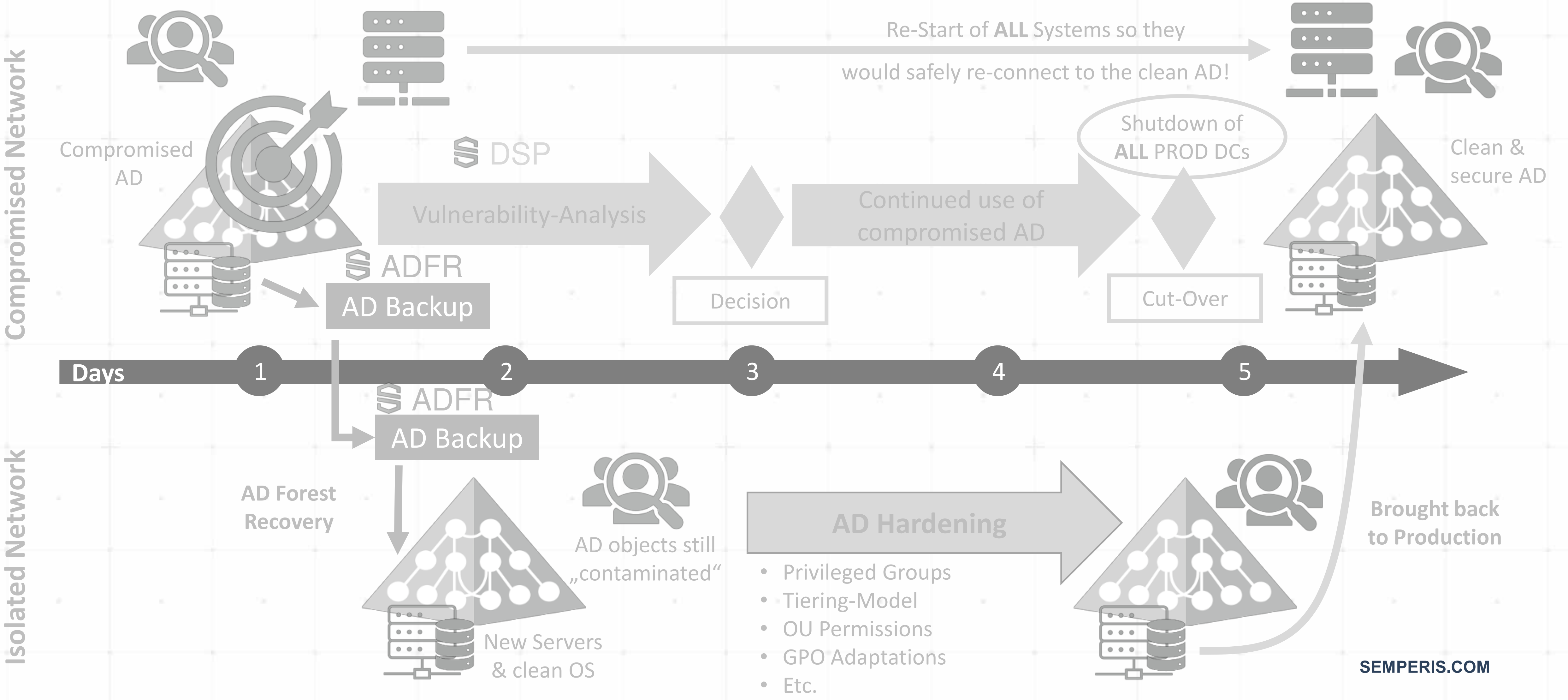
On-Premise Active Directory and Azure Active Directory

Semperis Active Directory Forest Recovery™

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

Real life AD-incident example – the AD details

semperis



Compromised Network

Isolated Network

Compromised AD

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

DSP

Vulnerability-Analysis

Decision

Continued use of compromised AD

Shutdown of **ALL** PROD DCs

Cut-Over

Clean & secure AD

ADFR

AD Backup

Days 1 2 3 4 5

ADFR

AD Backup

AD Forest Recovery

New Servers & clean OS

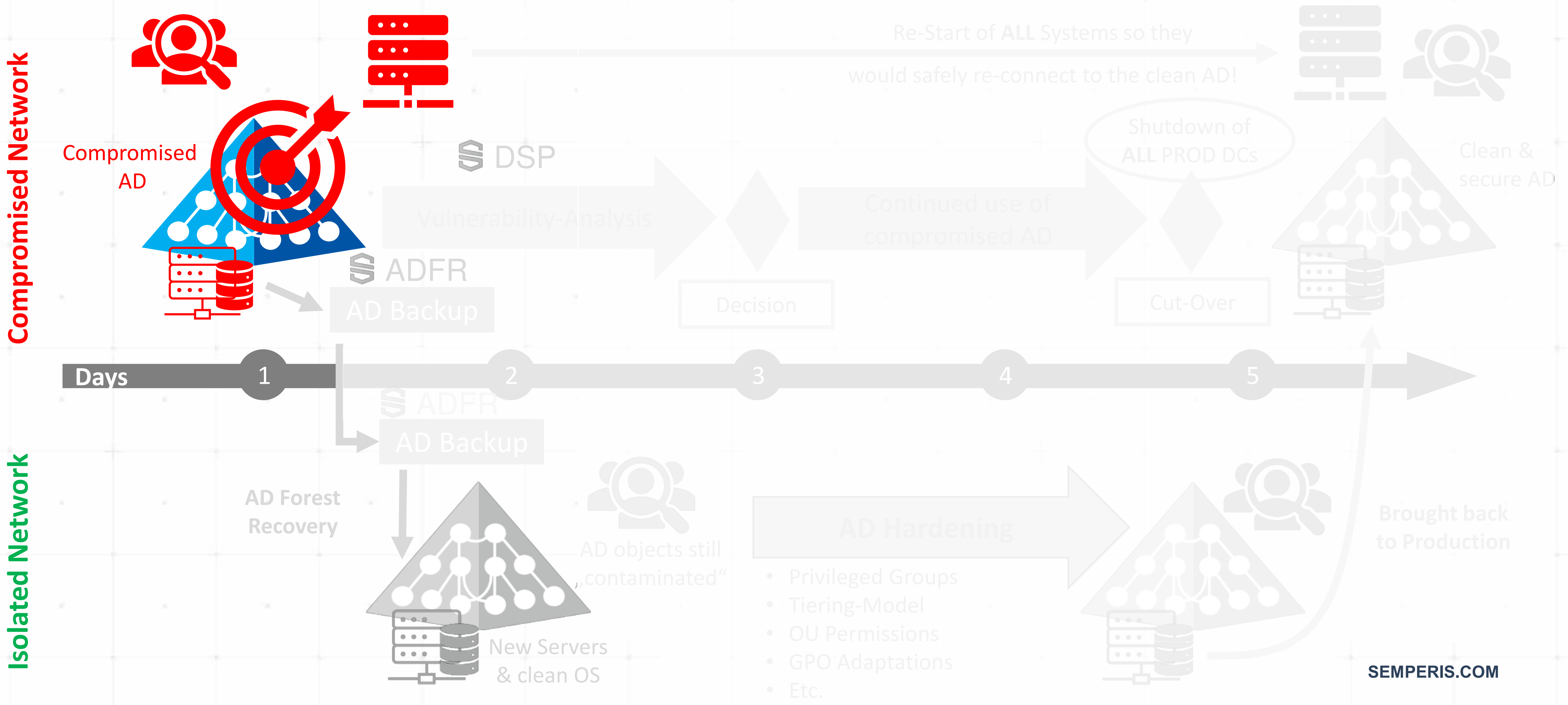
AD objects still „contaminated“

AD Hardening

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

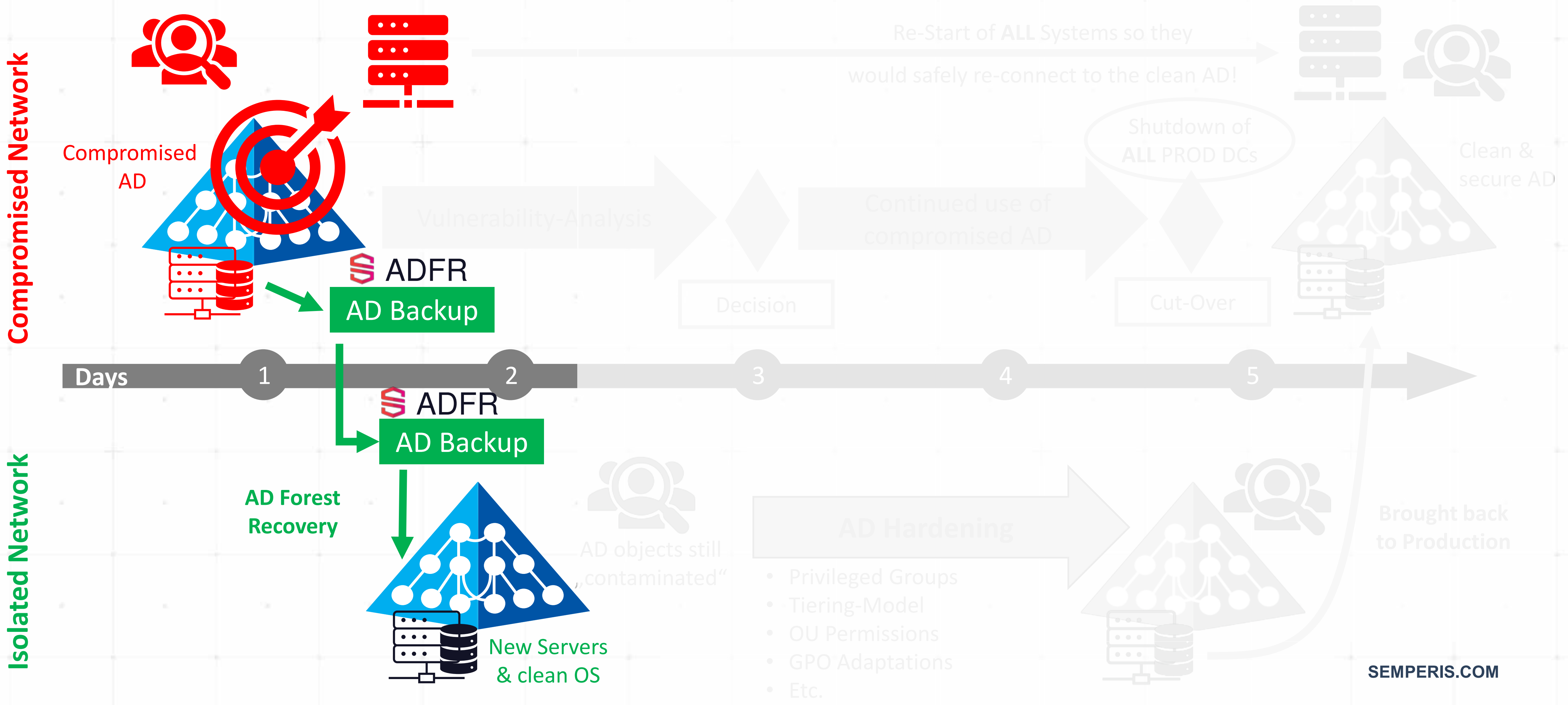
Brought back to Production

You’ve been BREACHED !!!

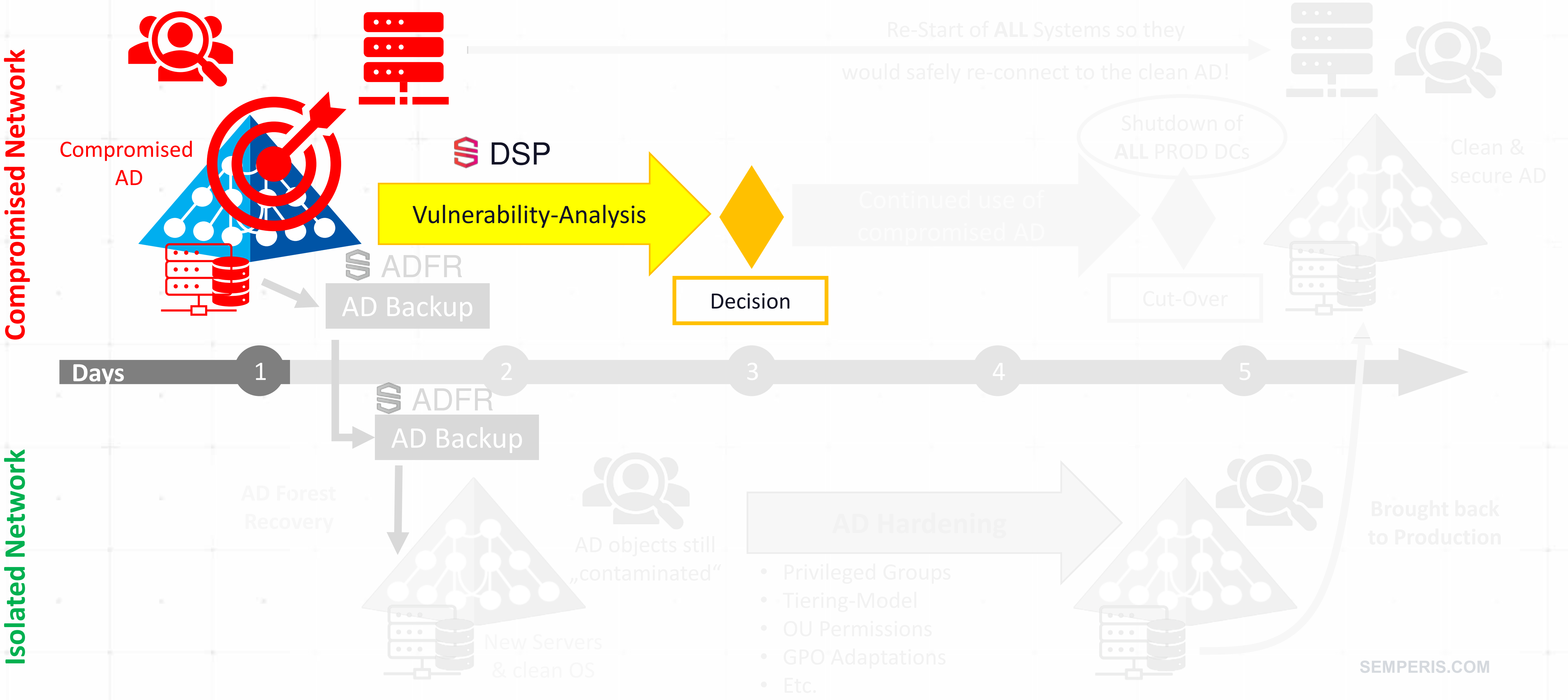


- Privileged Groups
- Tiering-Model
- OU Permissions
- GPO Adaptations
- Etc.

PHASE I – Spin up a SAFETY NET for AD



PHASE II – AD Vulnerability Analysis



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

ADFR

AD Backup

Isolated Network

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

Purple Knight

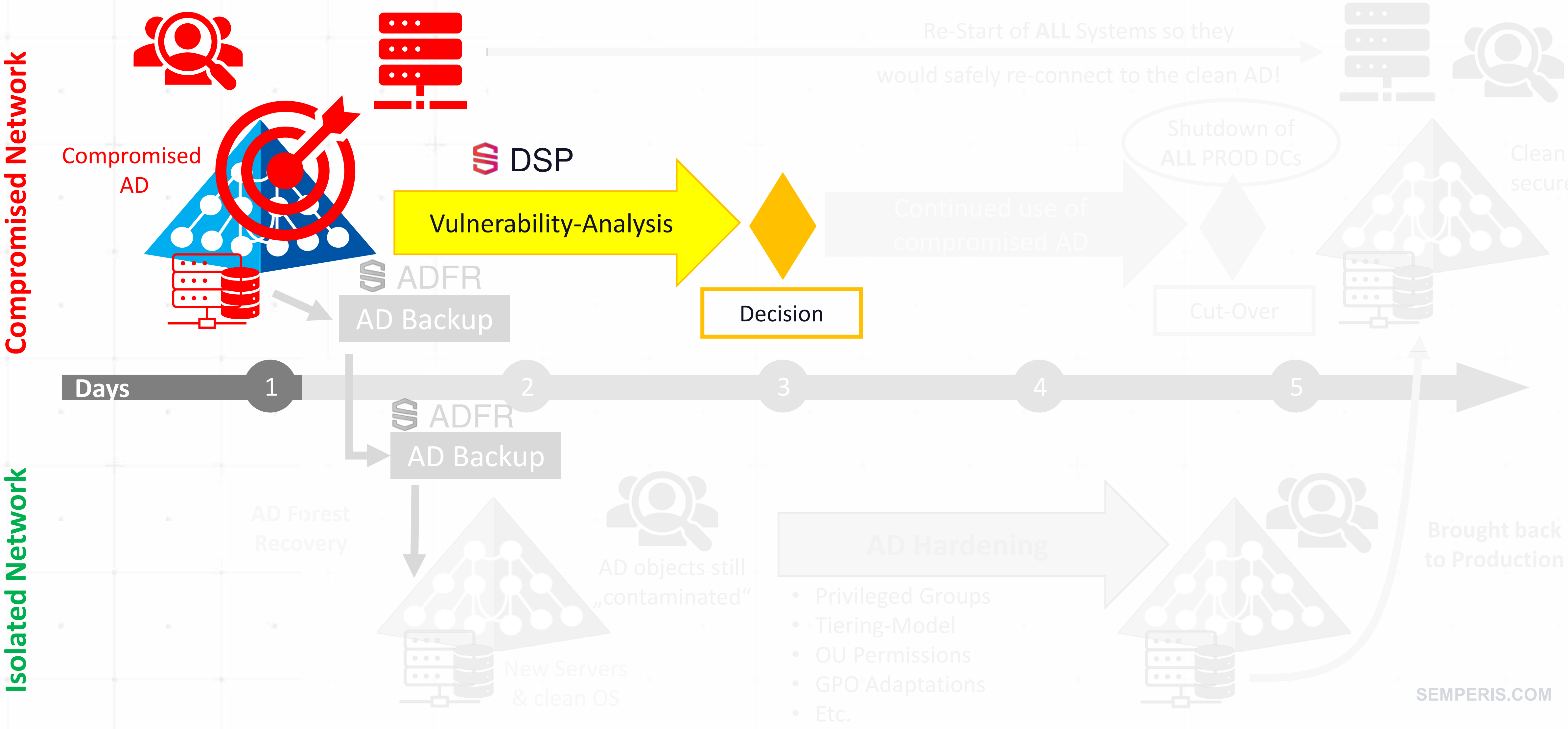
PURPLE KNIGHT

www.purple-knight.com

FOREST DRUID

https://www.semperis.com/forest-druid/

PHASE II – AD Vulnerability Analysis



Compromised Network

Compromised AD

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

DSP

Vulnerability-Analysis

Decision

Shutdown of ALL PROD DCs

Clean & secure AD

Continued use of compromised AD

Cut-Over

ADFR

AD Backup

Days 1 2 3 4 5

ADFR

AD Backup

Isolated Network

AD Forest Recovery

AD objects still „contaminated“

AD Hardening

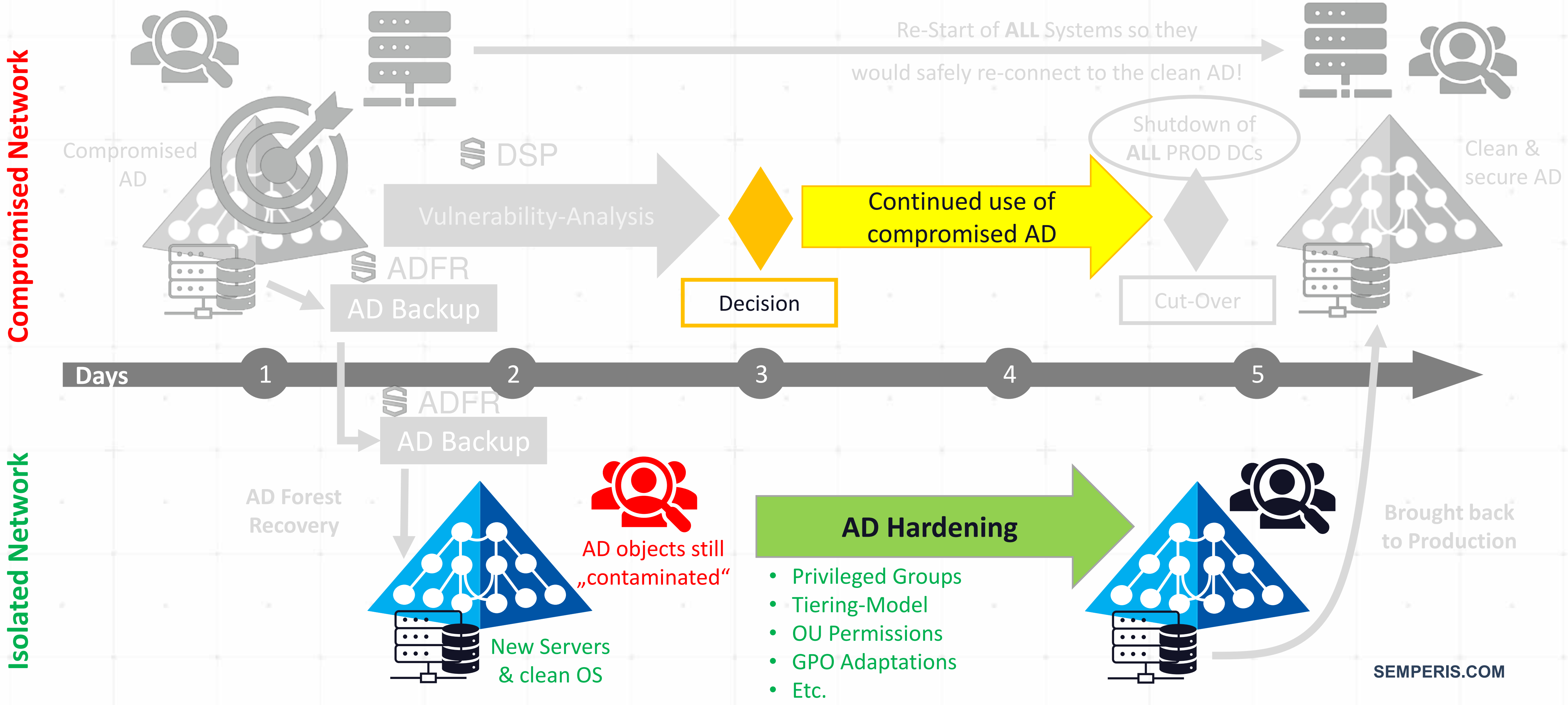
- Privileged Groups
- Tiering-Model
- OU Permissions
- GPO Adaptations
- Etc.

Brought back to Production

New Servers & clean OS

PHASE III – Divide and Conquer!

semperis



Compromised Network

Compromised AD

DSP

Vulnerability-Analysis

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

ADFR

AD Backup

Decision

Continued use of compromised AD

Shutdown of **ALL** PROD DCs

Cut-Over

Clean & secure AD

Days 1 2 3 4 5

ADFR

AD Backup

Isolated Network

AD Forest Recovery

AD objects still „contaminated“

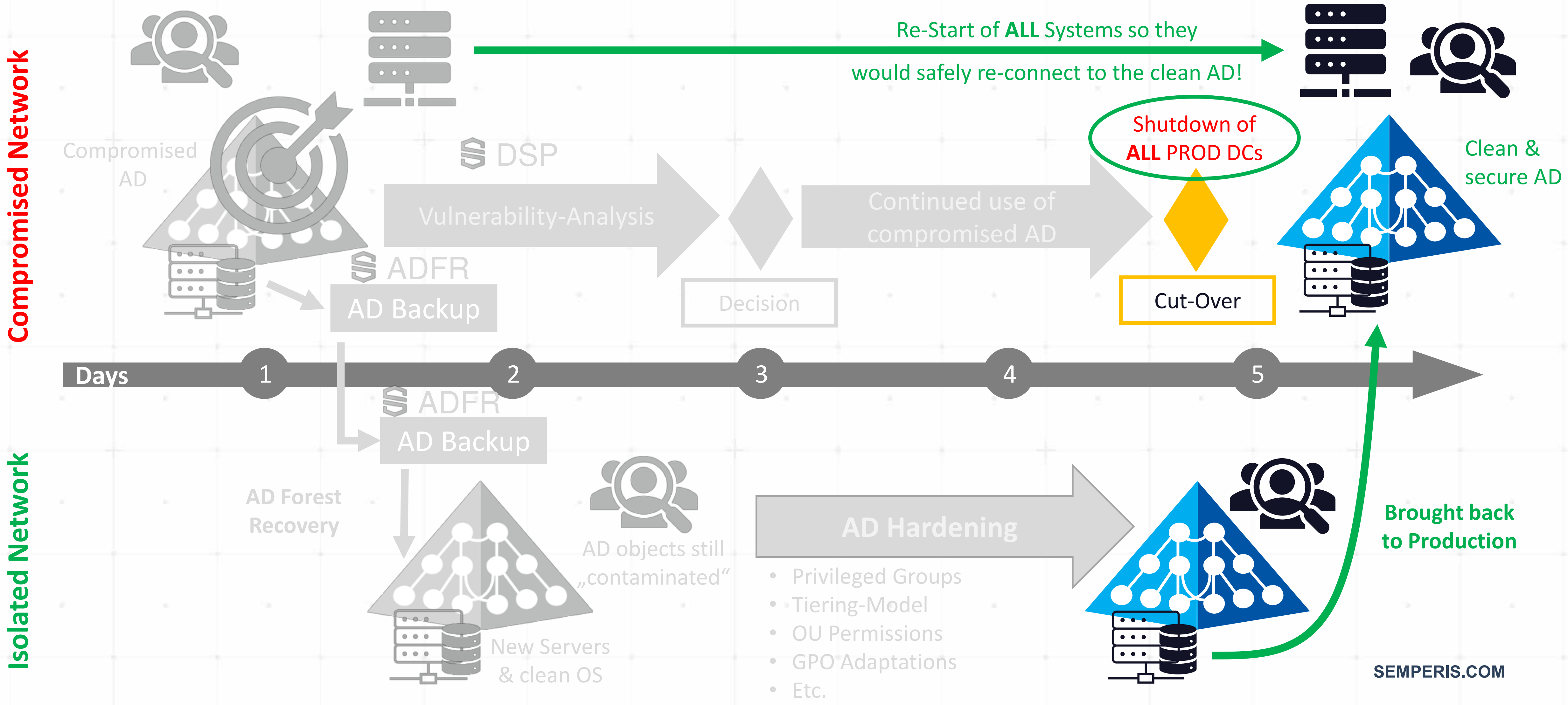
New Servers & clean OS

AD Hardening

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

Brought back to Production

PHASE IV – Bring hardened AD back to PROD



Compromised Network

Isolated Network

Compromised AD

DSP

Vulnerability-Analysis

Continued use of compromised AD

Decision

ADFR

AD Backup

Days 1 2 3 4 5

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.

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

Shutdown of **ALL** PROD DCs

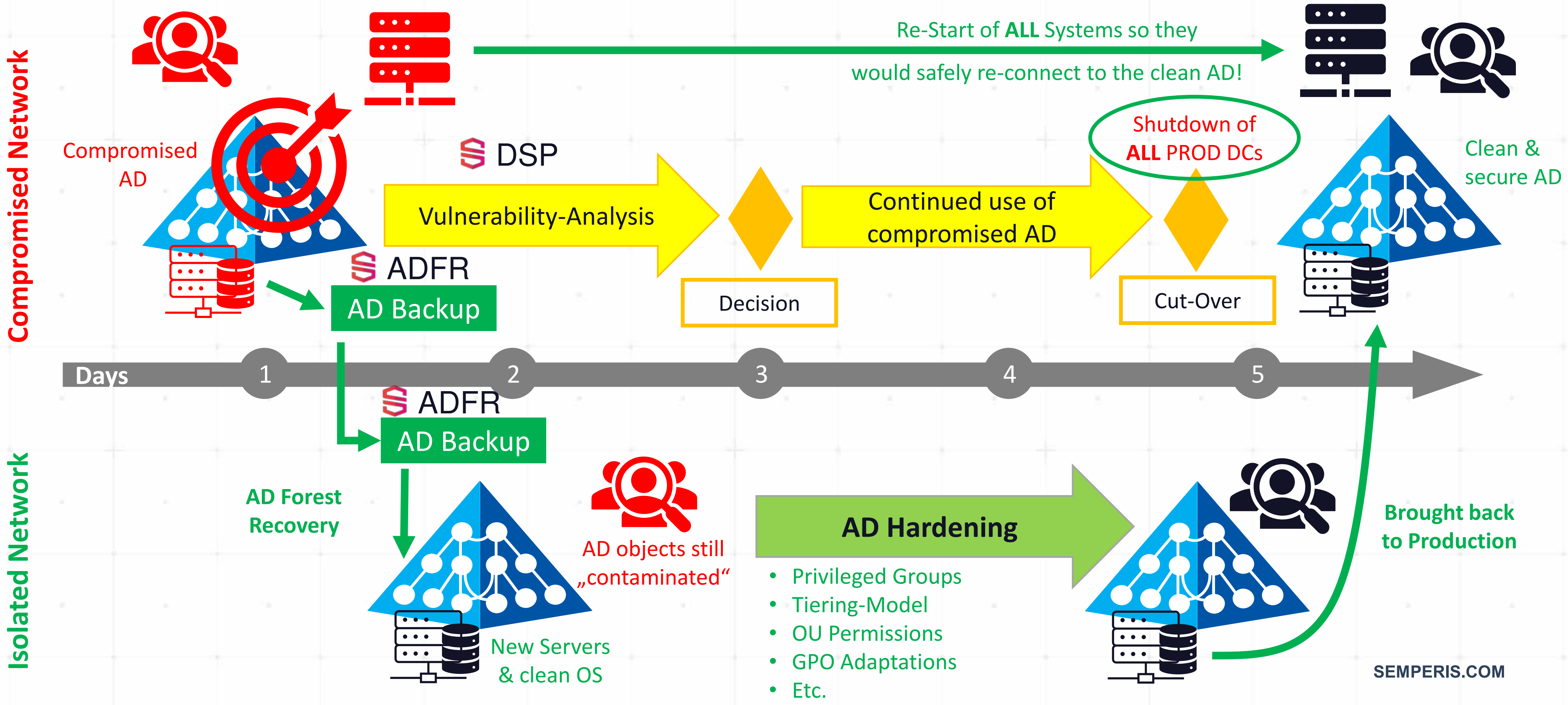
Cut-Over

Clean & secure AD

Brought back to Production

Real life AD-incident example – they SURVIVED!

semperis



Compromised Network

Compromised AD

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

DSP

Vulnerability-Analysis

Decision

Continued use of compromised AD

Shutdown of **ALL** PROD DCs

Cut-Over

Clean & secure AD

ADFR

AD Backup

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.

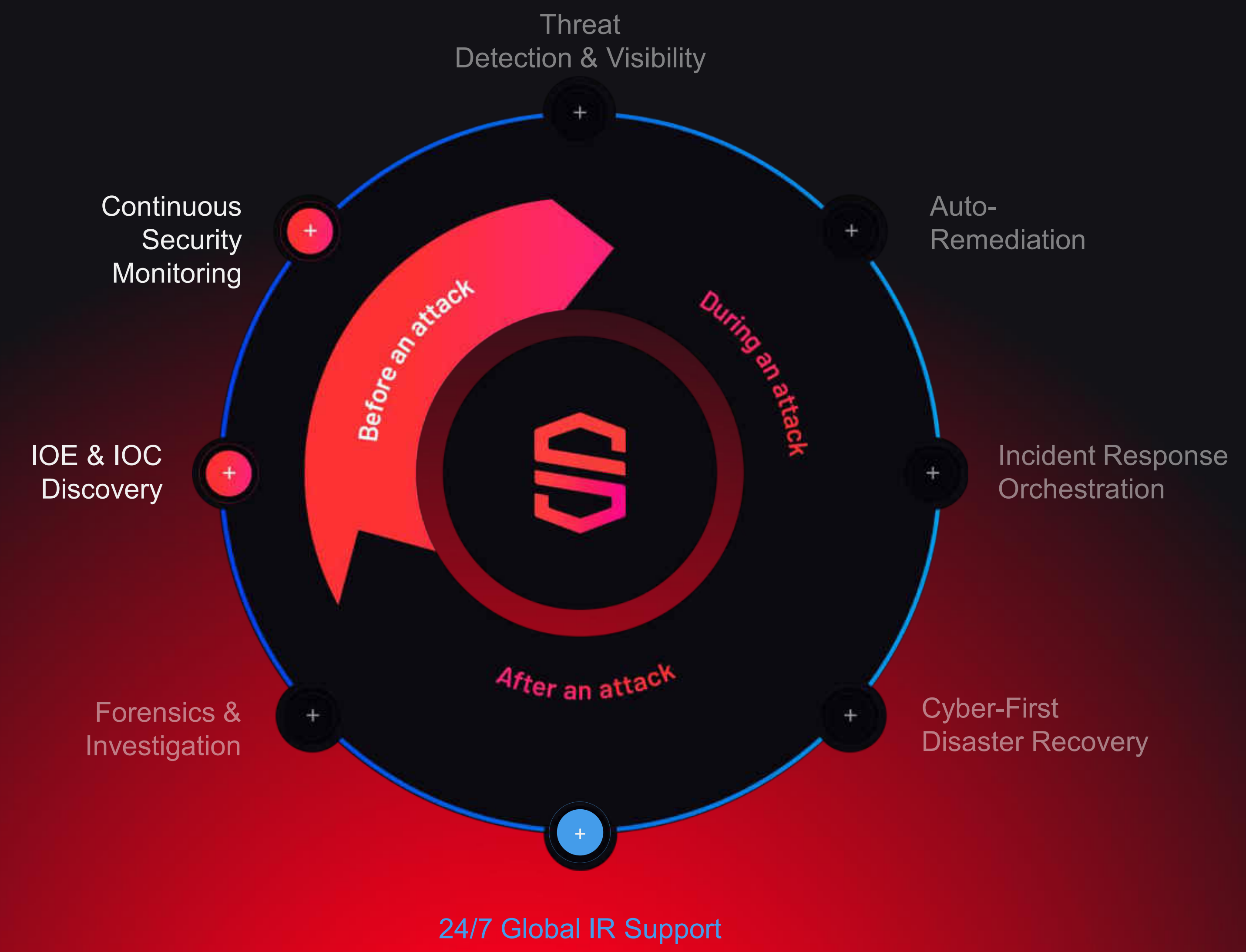
Brought back to Production

SEMPERIS.COM

So, what does it take to secure your AD?

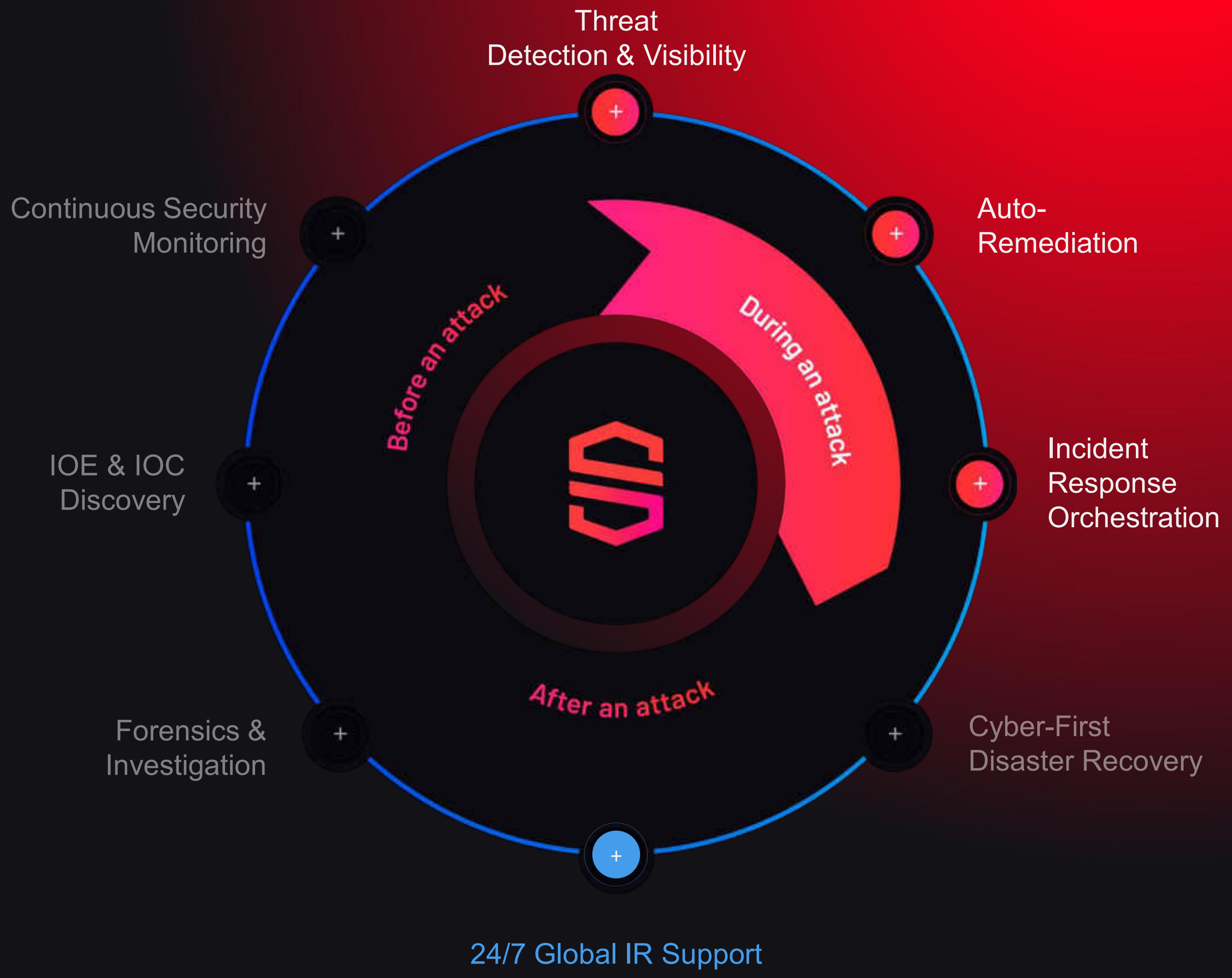
semperis

PRE attack


Threat Detection & Visibility
Auto-Remediation
Incident Response Orchestration
Cyber-First Disaster Recovery
24/7 Global IR Support
Forensics & Investigation
IOE & IOC Discovery
Continuous Security Monitoring
Before an attack
During an attack
After an attack

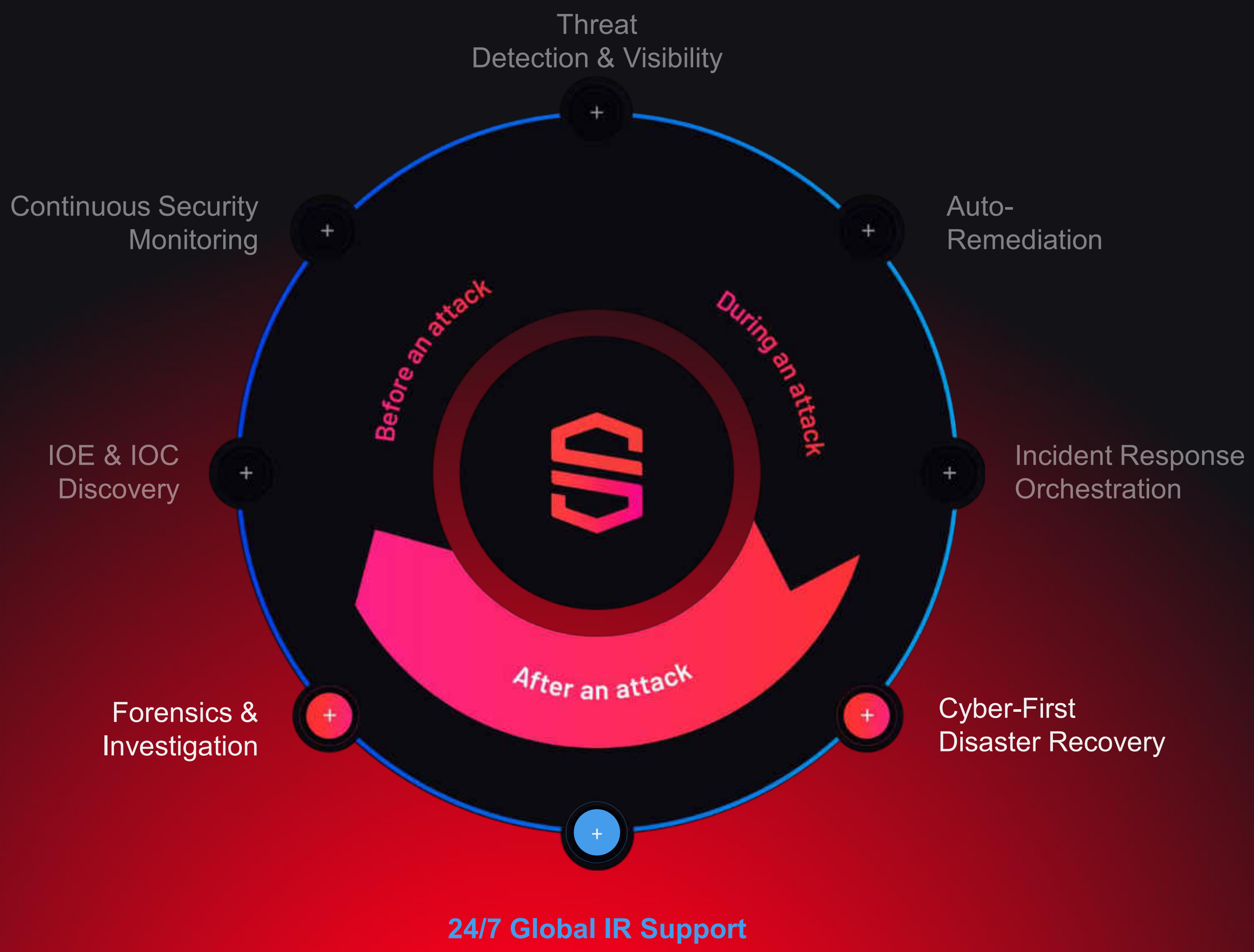
semperis

DURING attack


Threat Detection & Visibility
Auto-Remediation
Incident Response Orchestration
Cyber-First Disaster Recovery
24/7 Global IR Support
Forensics & Investigation
IOE & IOC Discovery
Continuous Security Monitoring
Before an attack
During an attack
After an attack

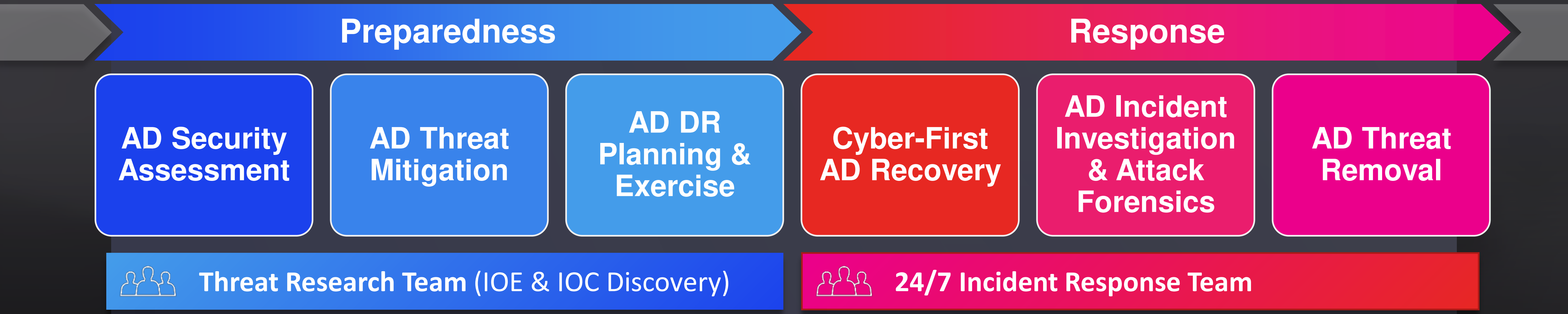
semperis

POST attack



semperis

BREACH PREPAREDNESS & RESPONSE SERVICES



Preparedness

- AD Security Assessment
- AD Threat Mitigation
- AD DR Planning & Exercise

Response

- Cyber-First AD Recovery
- AD Incident Investigation & Attack Forensics
- AD Threat Removal

Threat Research Team (IOE & IOC Discovery)

24/7 Incident Response Team

- Battle-tested experts and industry-leading tools
- Comprehensive services for every stage of the IR lifecycle
- 24/7 global incident response support team
- Help customers with or without Semperis products

semperis

Questions

Oliver Keizers

AVP EMEA Central, Semperis

KKR

INSIGHT PARTNERS

Microsoft Partner
Enterprise Cloud Alliance
Microsoft Accelerator Alumni
Microsoft Co-Sell