semperis

TROOPERS CONFERENCE IN 2022

TROOPERS

JUNE 27 TO
JULY 01, 2022

semperis

Resurrecting After A Ransomware Attack
Be Secure(d), And Prepared!

TROOPERS CONFERENCE IN 2022

TROOPERS

JUNE 27 TO
JULY 01, 2022

Jorge de Almeida Pinto
Senior Solutions Architect
Product Manager Semperis ADFR
Incident Response Team Member

Me, Myself And I!

semperis

Microsoft Most Valuable Professional

Jorge de Almeida Pinto

Senior Solutions Architect
Product Manager Semperis ADFR
Incident Response Team Member

LinkedIn	http://tiny.cc/JorgeLinkedIn
Blog	http://tiny.cc/JQFKblog
Twitter	http://tiny.cc/JQFKtwitter
Website	https://www.semperis.com/
Blog	https://www.semperis.com/blog/
Podcast	https://hipconf.libsyn.com/
Contact	jorged@semperis.com

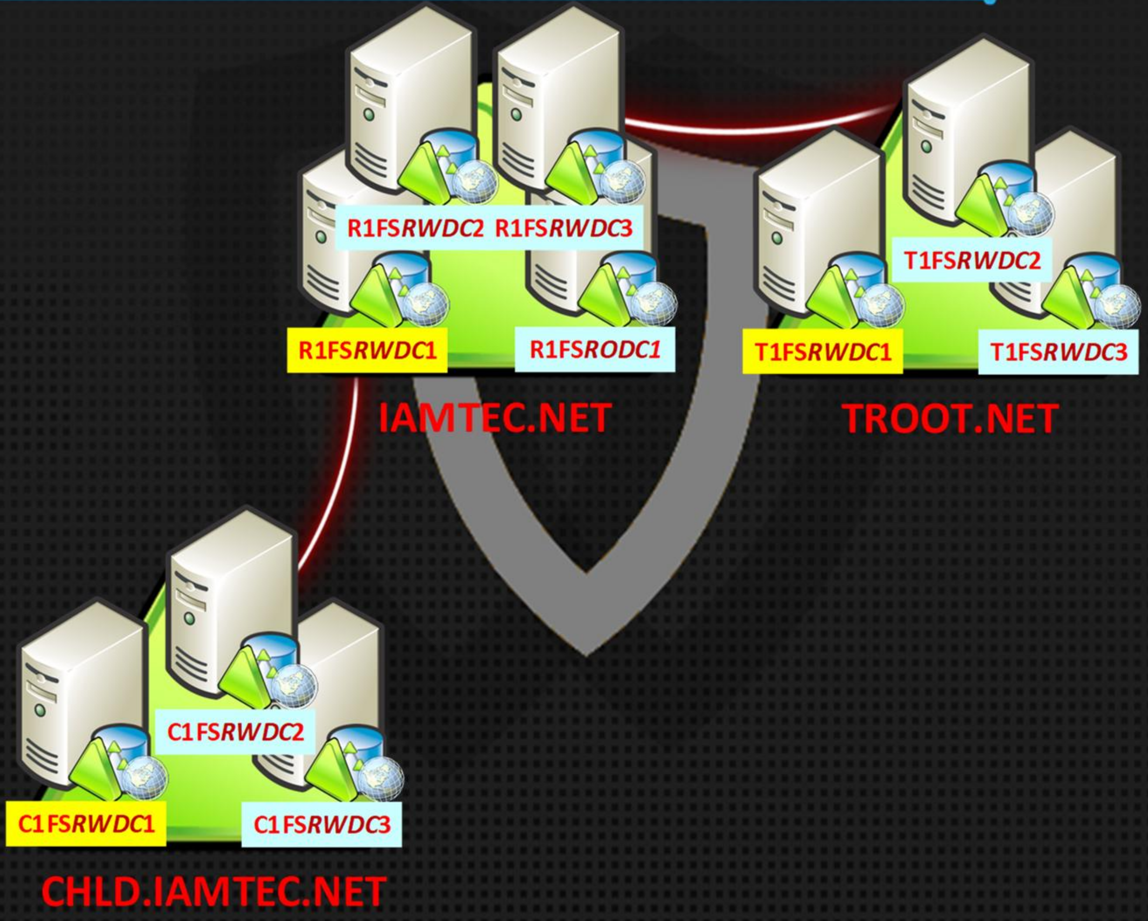
Architecting, designing, implementing and maintaining secure identity solutions
Technology Focus: Identity, Security And Recovery
Product Focus: AD, ADFS, AAD Connect, FIM/MIM, Azure AD Technologies.

Agenda

1. Securing & Protecting AD
2. AD DR Plan - Why?
3. AD DR Plan - Options
4. Real Life AD Incident/Recovery Scenario
5. Take Aways!

Demo! - While Presenting

semperis



semperis

Securing & Protecting AD

Securing And Protecting AD

semperis

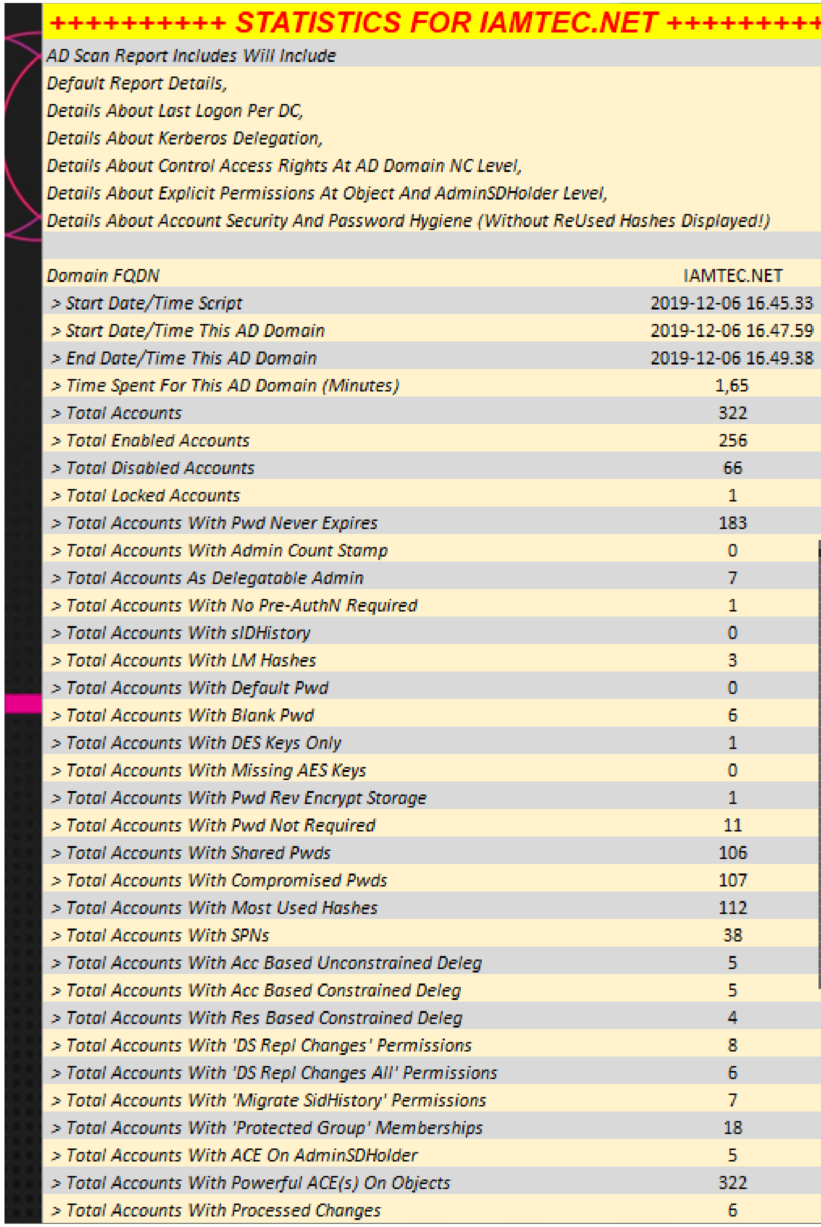
- ØPro-Actively - Search And Fix
  - ØBy looking for Indicators of Exposure (IoEs)
    - ØAccount Hygiene - Settings and Passwords
    - ØSecurity Related Configurations in AD
    - Ø"Invisible" attack paths
  - ØBy looking for Indicators of Compromise (IoCs)
    - ØDC Shadow
    - ØKerberoasting
    - Ø… and many more
  - ØTHINK and LOOK AT your (AD) environment as an attacker would

[Reading: Defenders Think in Lists. Attackers Think in Graphs]

[Video: Defenders Think in Lists. Attackers Think in Graphs]

rotecting AD

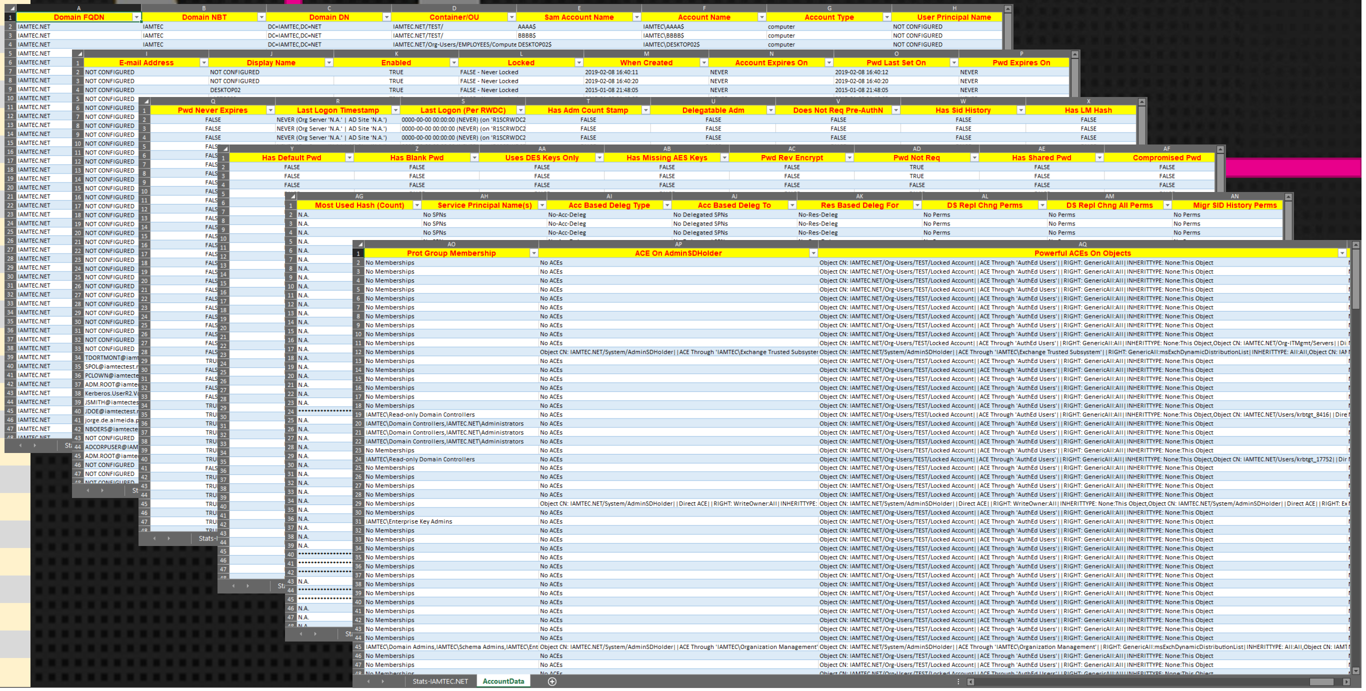
Threat Detection Response (TDR) Tools!



+++++++++++ STATISTICS FOR IAMTEC.NET +++++++++++

AD Scan Report Includes Will Include
Default Report Details,
Details About Last Logon Per DC,
Details About Kerberos Delegation,
Details About Control Access Rights At AD Domain NC Level,
Details About Explicit Permissions At Object And AdminSDHolder Level,
Details About Account Security And Password Hygiene (Without ReUsed Hashes Displayed!)

Domain FQDN	IAMTEC.NET
> Start Date/Time Script	2019-12-06 16.45.33
> Start Date/Time This AD Domain	2019-12-06 16.47.59
> End Date/Time This AD Domain	2019-12-06 16.49.38
> Time Spent For This AD Domain (Minutes)	1,65
> Total Accounts	322
> Total Enabled Accounts	256
> Total Disabled Accounts	66
> Total Locked Accounts	1
> Total Accounts With Pwd Never Expires	183
> Total Accounts With Admin Count Stamp	0
> Total Accounts As Delegatable Admin	7
> Total Accounts With No Pre-AuthN Required	1
> Total Accounts With sIDHistory	0
> Total Accounts With LM Hashes	3
> Total Accounts With Default Pwd	0
> Total Accounts With Blank Pwd	6
> Total Accounts With DES Keys Only	1
> Total Accounts With Missing AES Keys	0
> Total Accounts With Pwd Rev Encrypt Storage	1
> Total Accounts With Pwd Not Required	11
> Total Accounts With Shared Pwds	106
> Total Accounts With Compromised Pwds	107
> Total Accounts With Most Used Hashes	112
> Total Accounts With SPNs	38
> Total Accounts With Acc Based Unconstrained Deleg	5
> Total Accounts With Acc Based Constrained Deleg	5
> Total Accounts With Res Based Constrained Deleg	4
> Total Accounts With 'DS Repl Changes' Permissions	8
> Total Accounts With 'DS Repl Changes All' Permissions	6
> Total Accounts With 'Migrate SidHistory' Permissions	7
> Total Accounts With 'Protected Group' Memberships	18
> Total Accounts With ACE On AdminSDHolder	5
> Total Accounts With Powerful ACE(s) On Objects	322
> Total Accounts With Processed Changes	6



Domain FQDN	Domain NBT	Domain DN	Container/OU	Sam Account Name	Account Name	Account Type	User Principal Name
IAMTEC.NET	IAMTEC	DC=IAMTEC,DC=NET	IAMTEC.NET/TEST/	AAAA$	IAMTEC\AAAA$	computer	NOT CONFIGURED
IAMTEC.NET	IAMTEC	DC=IAMTEC,DC=NET	IAMTEC.NET/TEST/	BBBB$	IAMTEC\BBBB$	computer	NOT CONFIGURED
IAMTEC.NET	IAMTEC	DC=IAMTEC,DC=NET	IAMTEC.NET/Org-Users/EMPLOYEES/Compute	DESKTOP02$	IAMTEC\DESKTOP02$	computer	NOT CONFIGURED

E-mail Address	Display Name	Enabled	Locked	When Created	Account Expires On	Pwd Last Set On	Pwd Expires On
NOT CONFIGURED	NOT CONFIGURED	TRUE	FALSE - Never Locked	2019-02-08 16:40:11	NEVER	2019-02-08 16:40:12	NEVER
NOT CONFIGURED	NOT CONFIGURED	TRUE	FALSE - Never Locked	2019-02-08 16:40:20	NEVER	2019-02-08 16:40:20	NEVER
NOT CONFIGURED	DESKTOP02	TRUE	FALSE - Never Locked	2015-01-08 21:48:05	NEVER	2015-01-08 21:48:05	NEVER

Pwd Never Expires	Last Logon Timestamp	Last Logon (Per RWDC)	Has Adm Count Stamp	Delegatable Adm	Does Not Req Pre-AuthN	Has Sid History	Has LM Hash
FALSE	NEVER (Org Server 'N.A.' | AD Site 'N.A.')	0000-00-00 00:00:00 (NEVER) (on 'R1SCRWDC2	FALSE	FALSE	FALSE	FALSE	FALSE
FALSE	NEVER (Org Server 'N.A.' | AD Site 'N.A.')	0000-00-00 00:00:00 (NEVER) (on 'R1SCRWDC2	FALSE	FALSE	FALSE	FALSE	FALSE
FALSE	NEVER (Org Server 'N.A.' | AD Site 'N.A.')	0000-00-00 00:00:00 (NEVER) (on 'R1SCRWDC2	FALSE	FALSE	FALSE	FALSE	FALSE

Has Default Pwd	Has Blank Pwd	Uses DES Keys Only	Has Missing AES Keys	Pwd Rev Encrypt	Pwd Not Req	Has Shared Pwd	Compromised Pwd
FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE
FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE
FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE

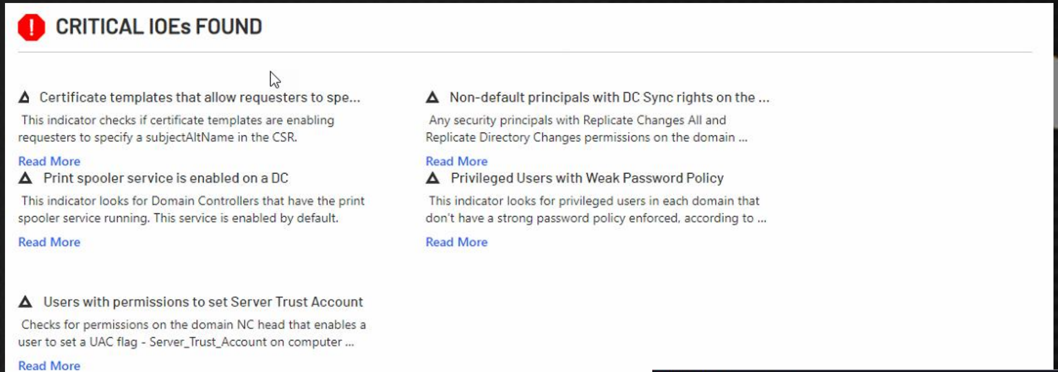
Most Used Hash (Count)	Service Principal Name(s)	Acc Based Deleg Type	Acc Based Deleg To	Res Based Deleg For	DS Repl Chng Perms	DS Repl Chng All Perms	Migr SID History Perms
N.A.	No SPNs	No-Acc-Deleg	No Delegated SPNs	No-Res-Deleg	No Perms	No Perms	No Perms
N.A.	No SPNs	No-Acc-Deleg	No Delegated SPNs	No-Res-Deleg	No Perms	No Perms	No Perms
N.A.	No SPNs	No-Acc-Deleg	No Delegated SPNs	No-Res-Deleg	No Perms	No Perms	No Perms

Prot Group Membership	ACE On AdminSDHolder	Powerful ACEs On Objects
No Memberships	No ACEs	Object CN: IAMTEC.NET/Org-Users/TEST/Locked Account| |ACE Through 'AuthEd Users'| |RIGHT: GenericAll:All| INHERITTYPE: None:This Object
No Memberships	No ACEs	Object CN: IAMTEC.NET/Org-Users/TEST/Locked Account| |ACE Through 'AuthEd Users'| |RIGHT: GenericAll:All| INHERITTYPE: None:This Object
No Memberships	No ACEs	Object CN: IAMTEC.NET/Org-Users/TEST/Locked Account| |ACE Through 'AuthEd Users'| |RIGHT: GenericAll:All| INHERITTYPE: None:This Object
No Memberships	No ACEs	Object CN: IAMTEC.NET/Org-Users/TEST/Locked Account| |ACE Through 'AuthEd Users'| |RIGHT: GenericAll:All| INHERITTYPE: None:This Object
No Memberships	No ACEs	Object CN: IAMTEC.NET/Org-Users/TEST/Locked Account| |ACE Through 'AuthEd Users'| |RIGHT: GenericAll:All| INHERITTYPE: None:This Object
No Memberships	No ACEs	Object CN: IAMTEC.NET/Org-Users/TEST/Locked Account| |ACE Through 'AuthEd Users'| |RIGHT: GenericAll:All| INHERITTYPE: None:This Object
No Memberships	No ACEs	Object CN: IAMTEC.NET/Org-Users/TEST/Locked Account| |ACE Through 'AuthEd Users'| |RIGHT: GenericAll:All| INHERITTYPE: None:This Object
No Memberships	No ACEs	Object CN: IAMTEC.NET/Org-Users/TEST/Locked Account| |ACE Through 'AuthEd Users'| |RIGHT: GenericAll:All| INHERITTYPE: None:This Object
No Memberships	No ACEs	Object CN: IAMTEC.NET/Org-Users/TEST/Locked Account| |ACE Through 'AuthEd Users'| |RIGHT: GenericAll:All| INHERITTYPE: None:This Object

Securing And Protecting AD

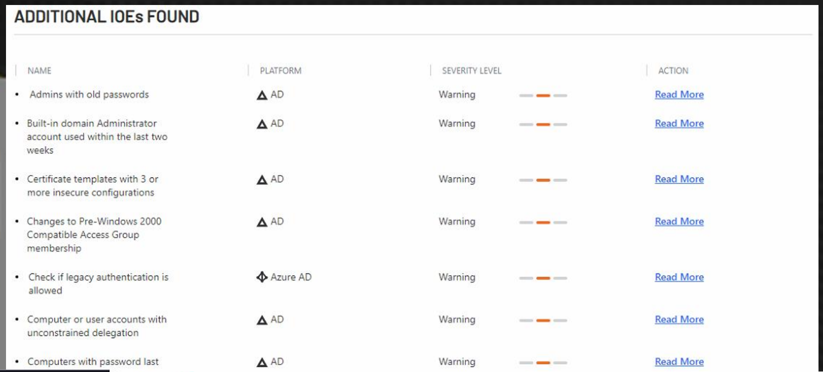
semperis

ØHow? - You ask? – Threat Detection Response (TDR) Tools!



CRITICAL IOEs FOUND

- Certificate templates that allow requesters to spe...
  This indicator checks if certificate templates are enabling requesters to specify a subjectAltName in the CSR.
  Read More
- Non-default principals with DC Sync rights on the ...
  Any security principals with Replicate Changes All and Replicate Directory Changes permissions on the domain ...
  Read More
- Print spooler service is enabled on a DC
  This indicator looks for Domain Controllers that have the print spooler service running. This service is enabled by default.
  Read More
- Privileged Users with Weak Password Policy
  This indicator looks for privileged users in each domain that don't have a strong password policy enforced, according to ...
  Read More
- Users with permissions to set Server Trust Account
  Checks for permissions on the domain NC head that enables a user to set a UAC flag - Server_Trust_Account on computer ...
  Read More

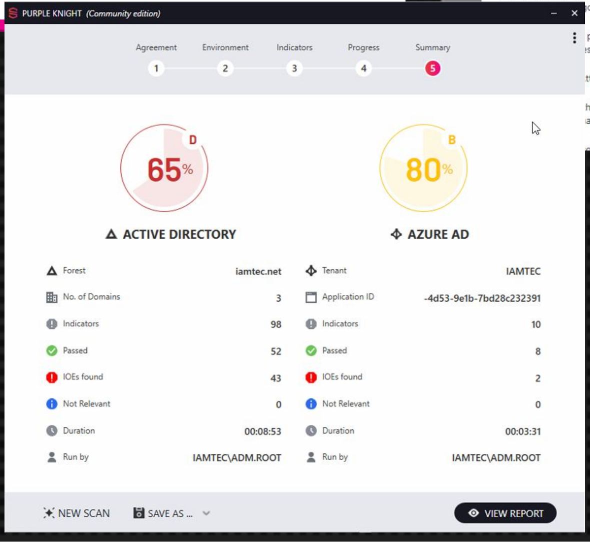


ADDITIONAL IOEs FOUND

NAME	PLATFORM	SEVERITY LEVEL	ACTION
Admins with old passwords	AD	Warning	Read More
Built-in domain Administrator account used within the last two weeks	AD	Warning	Read More
Certificate templates with 3 or more insecure configurations	AD	Warning	Read More
Changes to Pre-Windows 2000 Compatible Access Group membership	AD	Warning	Read More
Check if legacy authentication is allowed	Azure AD	Warning	Read More
Computer or user accounts with unconstrained delegation	AD	Warning	Read More
Computers with password last	AD	Warning	Read More

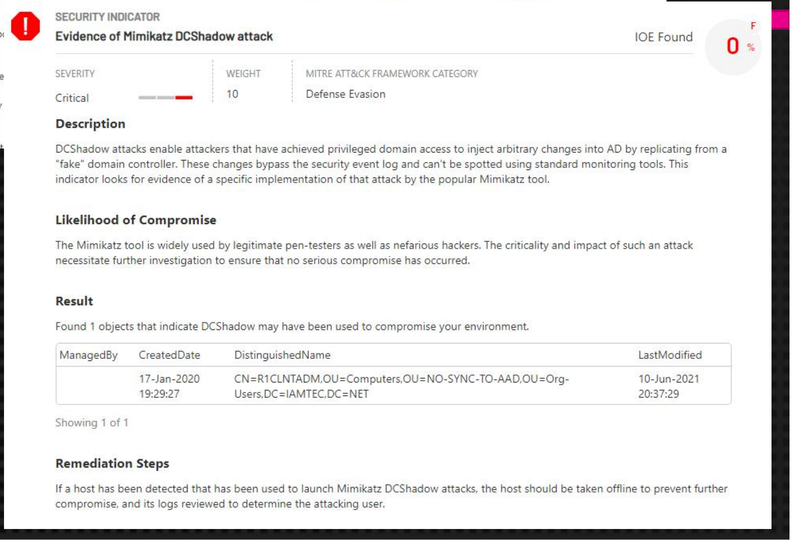
PURPLE KNIGHT

- Ø Powerful UI-tool for evaluating sec. posture of AD forest & AAD Tenant
- Ø Continuously updated with new vulnerability checks



PURPLE KNIGHT *(Community edition)*

ACTIVE DIRECTORY		AZURE AD	
Forest	iamtec.net	Tenant	IAMTEC
No. of Domains	3	Application ID	-4d53-9e1b-7bd28c232391
Indicators	98	Indicators	10
Passed	52	Passed	8
IOEs found	43	IOEs found	2
Not Relevant	0	Not Relevant	0
Duration	00:08:53	Duration	00:03:31
Run by	IAMTEC\ADM.ROOT	Run by	IAMTEC\ADM.ROOT



SECURITY INDICATOR

Evidence of Mimikatz DCShadow attack

IOE Found

SEVERITY: Critical

WEIGHT: 10

MITRE ATT&CK FRAMEWORK CATEGORY: Defense Evasion

Description

DCShadow attacks enable attackers that have achieved privileged domain access to inject arbitrary changes into AD by replicating from a "fake" domain controller. These changes bypass the security event log and can't be spotted using standard monitoring tools. This indicator looks for evidence of a specific implementation of that attack by the popular Mimikatz tool.

Likelihood of Compromise

The Mimikatz tool is widely used by legitimate pen-testers as well as nefarious hackers. The criticality and impact of such an attack necessitate further investigation to ensure that no serious compromise has occurred.

Result

Found 1 objects that indicate DCShadow may have been used to compromise your environment.

ManagedBy	CreatedDate	DistinguishedName	LastModified
	17-Jan-2020 19:29:27	CN=R1CLNTADM,OU=Computers,OU=NO-SYNC-TO-AAD,OU=Org-Users,DC=IAMTEC,DC=NET	10-Jun-2021 20:37:29

Showing 1 of 1

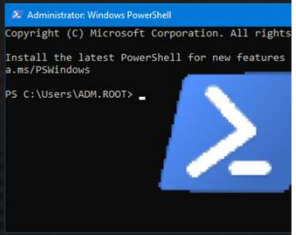
Remediation Steps

If a host has been detected that has been used to launch Mimikatz DCShadow attacks, the host should be taken offline to prevent further compromise, and its logs reviewed to determine the attacking user.

Securing

semperis

ØHow? - Yo nse (TDR) Tools!

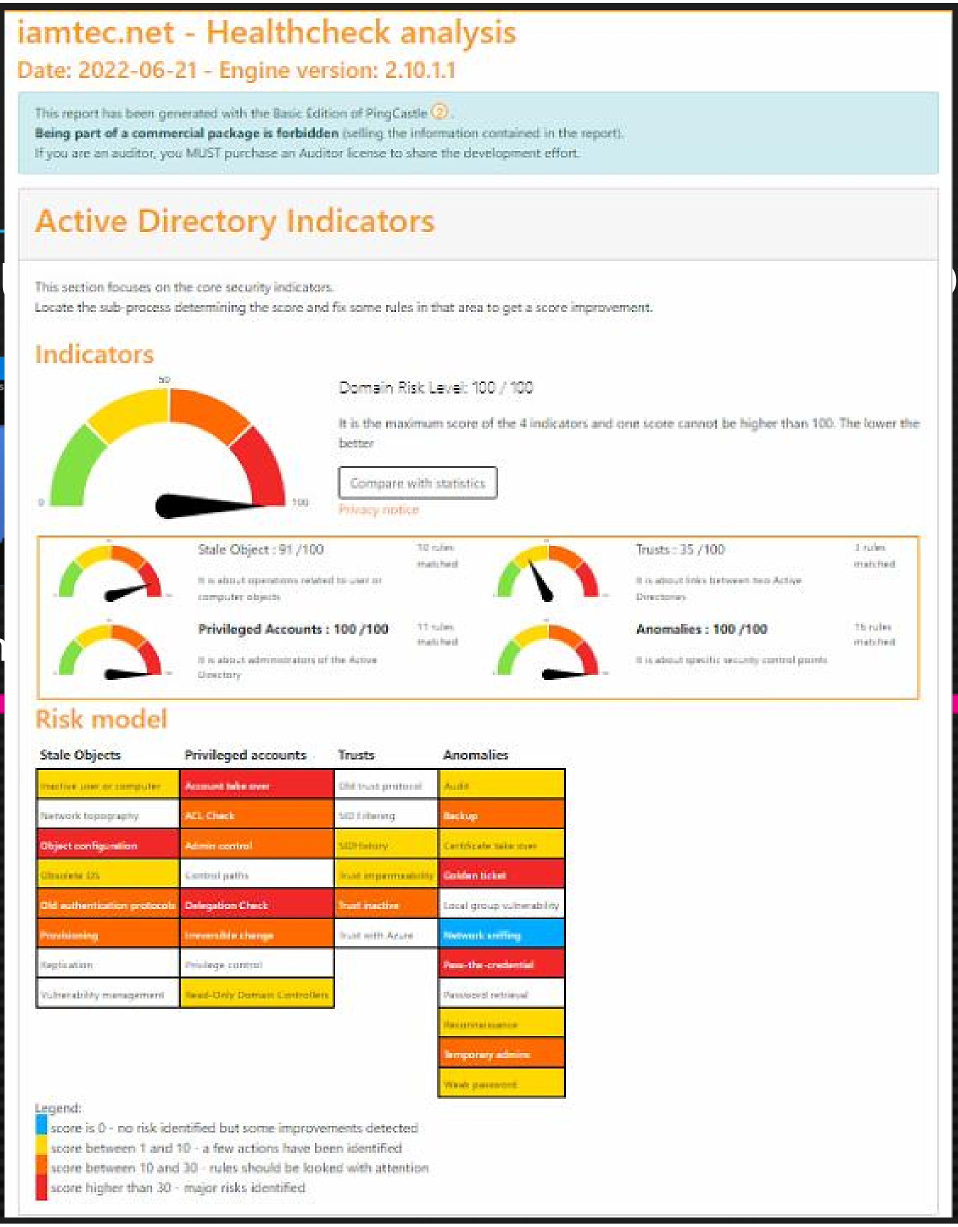


```
Administrator: Windows PowerShell
Copyright (C) Microsoft Corporation. All rights
Install the latest PowerShell for new features
a.ms/PSWindows
PS C:\Users\ADM.ROOT> _
```

Ø Do-It-Yourself in

PURPLE KNIGHT

- Ø Powerful UI-tool for evaluating security posture of an AD forest
- Ø Continuously updated with new vulnerability checks



iamtec.net - Healthcheck analysis

Date: 2022-06-21 - Engine version: 2.10.1.1

This report has been generated with the Basic Edition of PingCastle ②.
Being part of a commercial package is forbidden (selling the information contained in the report).
If you are an auditor, you MUST purchase an Auditor license to share the development effort.

Active Directory Indicators

This section focuses on the core security indicators.
Locate the sub-process determining the score and fix some rules in that area to get a score improvement.

Indicators

Domain Risk Level: 100 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

Stale Object : 91 /100 — 10 rules matched
It is about operations related to user or computer objects

Trusts : 35 /100 — 3 rules matched
It is about links between two Active Directories

Privileged Accounts : 100 /100 — 11 rules matched
It is about administrators of the Active Directory

Anomalies : 100 /100 — 16 rules matched
It is about specific security control points

Risk model

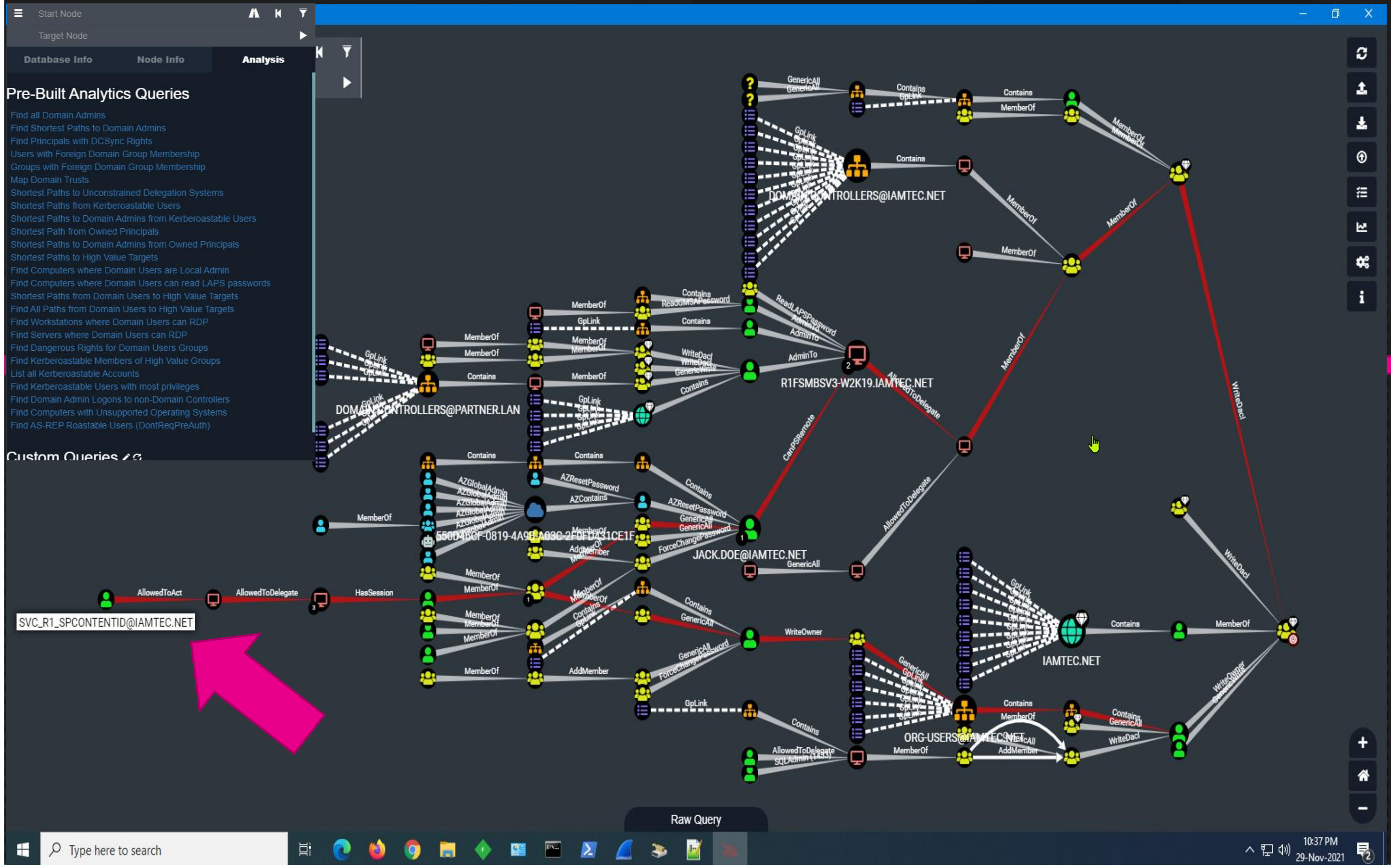
Stale Objects	Privileged accounts	Trusts	Anomalies
🟨 Inactive user or computer	🟥 Account take over	⬜ Old trust protocol	🟨 Audit
⬜ Network topography	🟧 ACL Check	⬜ SID Filtering	🟧 Backup
🟥 Object configuration	🟧 Admin control	🟨 SIDHistory	🟨 Certificate take over
🟨 Obsolete OS	⬜ Control paths	🟨 Trust impermeability	🟥 Golden ticket
🟧 Old authentication protocols	🟥 Delegation Check	🟧 Trust inactive	⬜ Local group vulnerability
🟧 Provisioning	🟧 Irreversible change	⬜ Trust with Azure	🟦 Network sniffing
⬜ Replication	⬜ Privilege control		🟥 Pass-the-credential
⬜ Vulnerability management	🟨 Read-Only Domain Controllers		⬜ Password retrieval
			🟨 Reconnaissance
			🟧 Temporary admins
			🟨 Weak password

Legend:
🟦 score is 0 - no risk identified but some improvements detected
🟨 score between 1 and 10 - a few actions have been identified
🟧 score between 10 and 30 - rules should be looked with attention
🟥 score higher than 30 - major risks identified

Securing And Protecting AD

semperis

ØHow? - You ask? – Threat Detection Response (TDR) Tools!



Pre-Built Analytics Queries

- Find all Domain Admins
- Find Shortest Paths to Domain Admins
- Find Principals with DCSync Rights
- Users with Foreign Domain Group Membership
- Groups with Foreign Domain Group Membership
- Map Domain Trusts
- Shortest Paths to Unconstrained Delegation Systems
- Shortest Paths from Kerberoastable Users
- Shortest Paths to Domain Admins from Kerberoastable Users
- Shortest Path from Owned Principals
- Shortest Paths to Domain Admins from Owned Principals
- Shortest Paths to High Value Targets
- Find Computers where Domain Users are Local Admin
- Find Computers where Domain Users can read LAPS passwords
- Shortest Paths from Domain Users to High Value Targets
- Find All Paths from Domain Users to High Value Targets
- Find Workstations where Domain Users can RDP
- Find Servers where Domain Users can RDP
- Find Dangerous Rights for Domain Users Groups
- Find Kerberoastable Members of High Value Groups
- List all Kerberoastable Accounts
- Find Kerberoastable Users with most privileges
- Find Domain Admin Logons to non-Domain Controllers
- Find Computers with Unsupported Operating Systems
- Find AS-REP Roastable Users (DontReqPreAuth)

Custom Queries

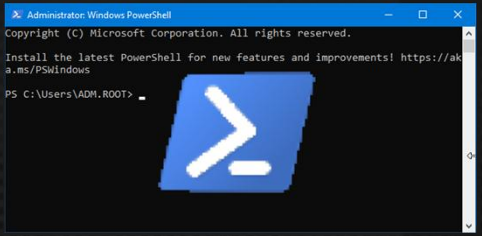
BLOODHOUND

- Ø Extraction of AD data through SharpHound command-line tool
- Ø Imported/Processed by BloodHound UI-tool to visualize attack-path(s)

Securing And Protecting AD

semperis

ØHow? - You ask? – Threat Detection Response (TDR) Tools!



```
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://ak
a.ms/PSWindows

PS C:\Users\ADM.ROOT> _
```

- Ø Do-It-Yourself in PowerShell

- Ø ...and many other free/paid TDR tools

PURPLE KNIGHT

- Ø Powerful UI-tool for evaluating security posture of an AD forest
- Ø Continuously updated with new vulnerability checks

PING CASTLE

- Ø Command-Line tool for evaluation security posture of an AD domain

BLOODHOUND

- Ø Extraction of AD data through SharpHound command-line tool
- Ø Imported/Processed by BloodHound UI-tool to visualize attack-path(s)

AD DR Plan - Why?

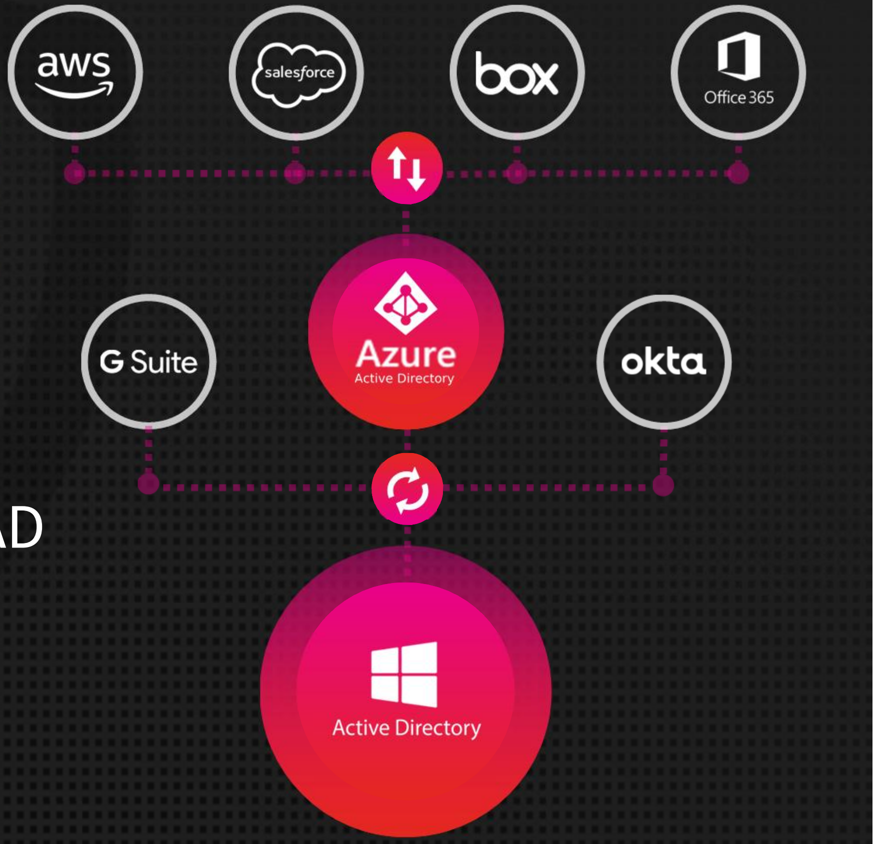
AD DR Plan - Why?

semperis

Ø AD Has The Keys To The KINGDOM!

If Active Directory isn’t secure, nothing is!

- Ø 80% of all breaches involve credential abuse
- Ø Systematic/historical weakness make AD a soft target
- Ø Cloud identity extends from AD
- Ø Zero trust model assumes hybrid AD integrity

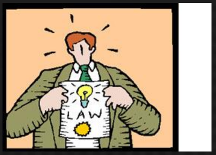


For **90% of enterprises**, IDENTITY starts with AD

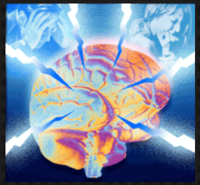
AD DR Plan - Why?

semperis

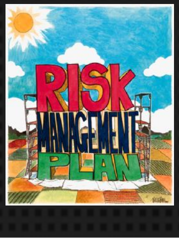
- Ø Business Reasoning



- Ø Regulations:
  - Ø Business continuity (e.g., banks, health care, utility, etc.)



- Ø Complexity:
  - Ø May look simple, difficult in practice!
  - Ø Reinstalling/recovering 1 DC is easy! Recovering many, in distributed environment? What about outsourcing?



- Ø Risk Management:
  - Ø Previous: “unlikely”; Now: “very common” à very high impact
  - Ø No AD? à Acceptable follow-up risks and costs?

AD DR Plan - Why?

semperis

- Business Reasoning
  - Probability/Impact of Scenarios

PROBABILITY ↑ / IMPACT →			
	DC Failure Networking Failure	Other Malware	
	Admin Error (Fat Fingers)	Malicious Insider Bug In Win/AD Code Admin Error (Bad Script)	Power Failure Wiperware Attack External Comms Failure
	UnAuthZ Physical Access	Int./Ext. Sabotage Physical Attack Revert FL Increase	Environmental Factors Bad Schema Extensions Bad Domain Ren/Repos

PROBABILITY

IMPACT

AD DR Plan - Options

AD DR Plan - Options

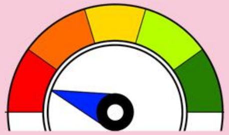
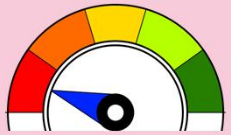
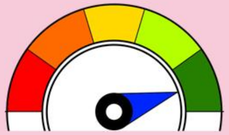
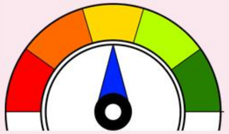
semperis

	MSFT Default AD DR Plan -= Manual =-	Customized AD DR Plan -= Semi Automated, a.k.a. D-I-Y =-	Customized AD DR Plan -= Fully Automated =-
Focus	Core only, no dependencies	Comms, logistics, pre/post, core, dependencies	
Text/Tools	High/None	Medium/E.g. PowerShell	Low/Commercial tool (AD focussed)
Risk Mitigation/Pre/Post-Tasks	Not described	Described	
Core Tasks	Described, unclear sequence	Described, clear sequence	
Orchestration Backup/Rstre/AD	Backup: Auto | Restore: None | AD: None	Backup: Auto | Restore: None | AD: Semi	Backup: Auto | Restore: Auto | AD: Auto
Backup Type (Size)	WSB (Large) + Custom (Large) (AD Integrated?! -> **L**)		Propriety (Small) + Non-AD-I

AD FOREST RECOVERY WITH NO AUTOMATION
AD FOREST RECOVERY WITH AUTOMATION

AD DR Plan - Options

semperis

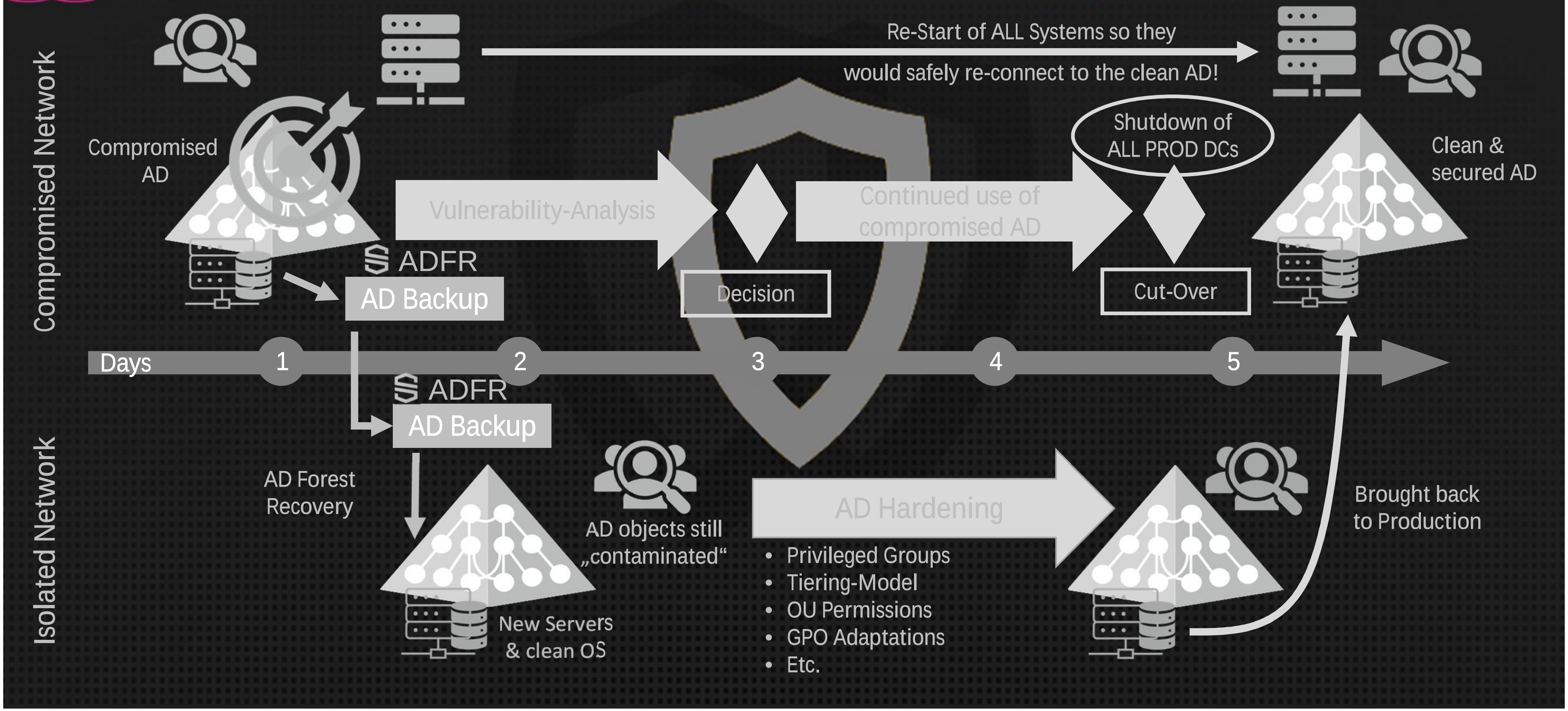
	MSFT Default AD DR Plan -= Manual =-	Customized AD DR Plan -= Semi Automated, a.k.a. D-I-Y =-	Customized AD DR Plan -= Fully Automated =-
High Level Way Of Working	Restore initial RWDC, clone, redeploy		Whatever you choose
Security Assessment	None or Separate		Integrated or Separate
Skills Required			
Complexity DR Plan/Test			
Recovery Time Objective (RTO)			

Ø Have you also thought about:

- Ø Where to store your plan/code/tools?
- Ø Credentials required during recovery?
- Ø Impact of recovery on Hybrid connections? (AuthN/Sync)
- Ø AuthN method for AAD – Fed, PTA or PHS?

Real Life AD Incident/Recovery Scenario

Real Life AD Incident/Recovery Scenario



Compromised Network

Compromised AD

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

Vulnerability-Analysis

Decision

Continued use of compromised AD

Shutdown of ALL PROD DCs

Cut-Over

Clean & secured AD

ADFR AD Backup

Days 1 2 3 4 5

Isolated Network

ADFR AD Backup

AD Forest Recovery

AD objects still „contaminated“

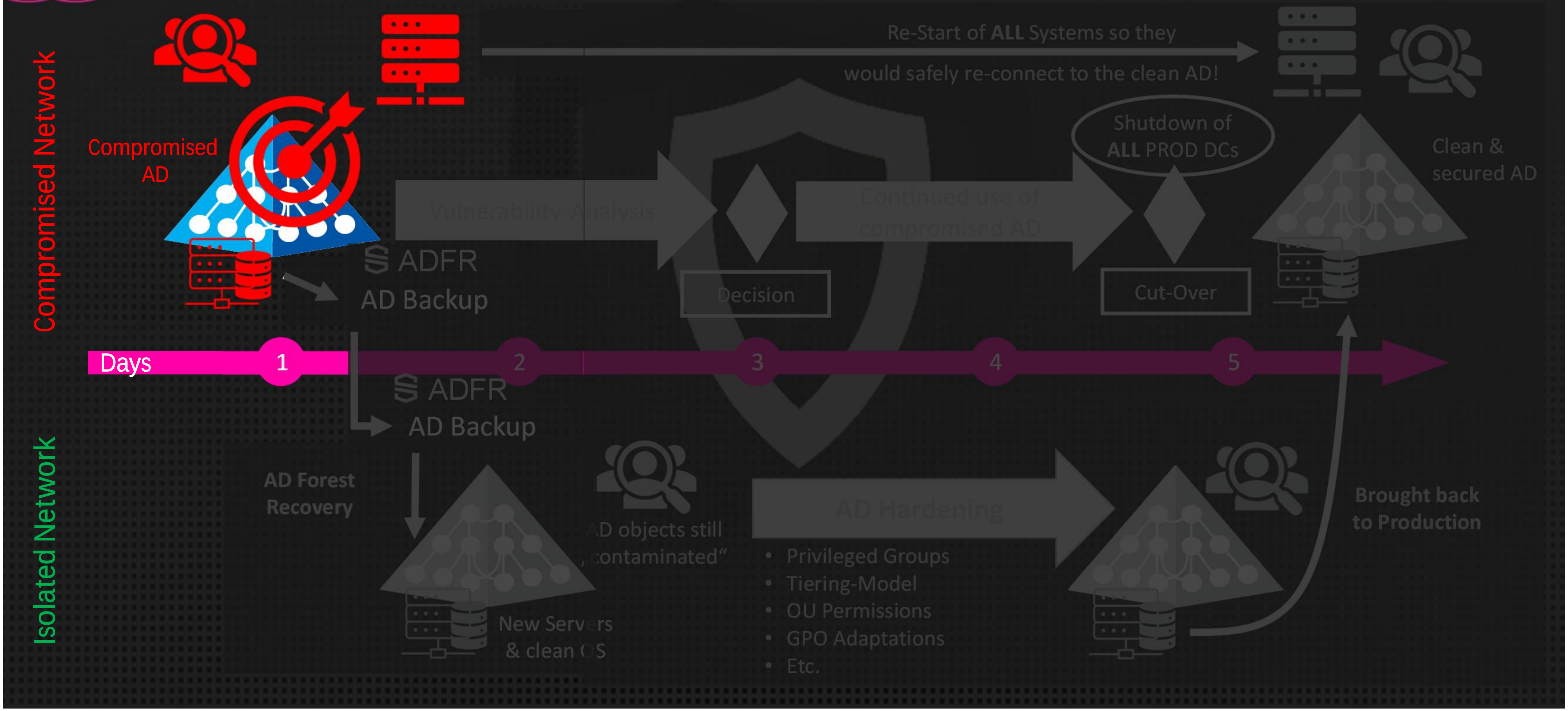
New Servers & clean OS

AD Hardening

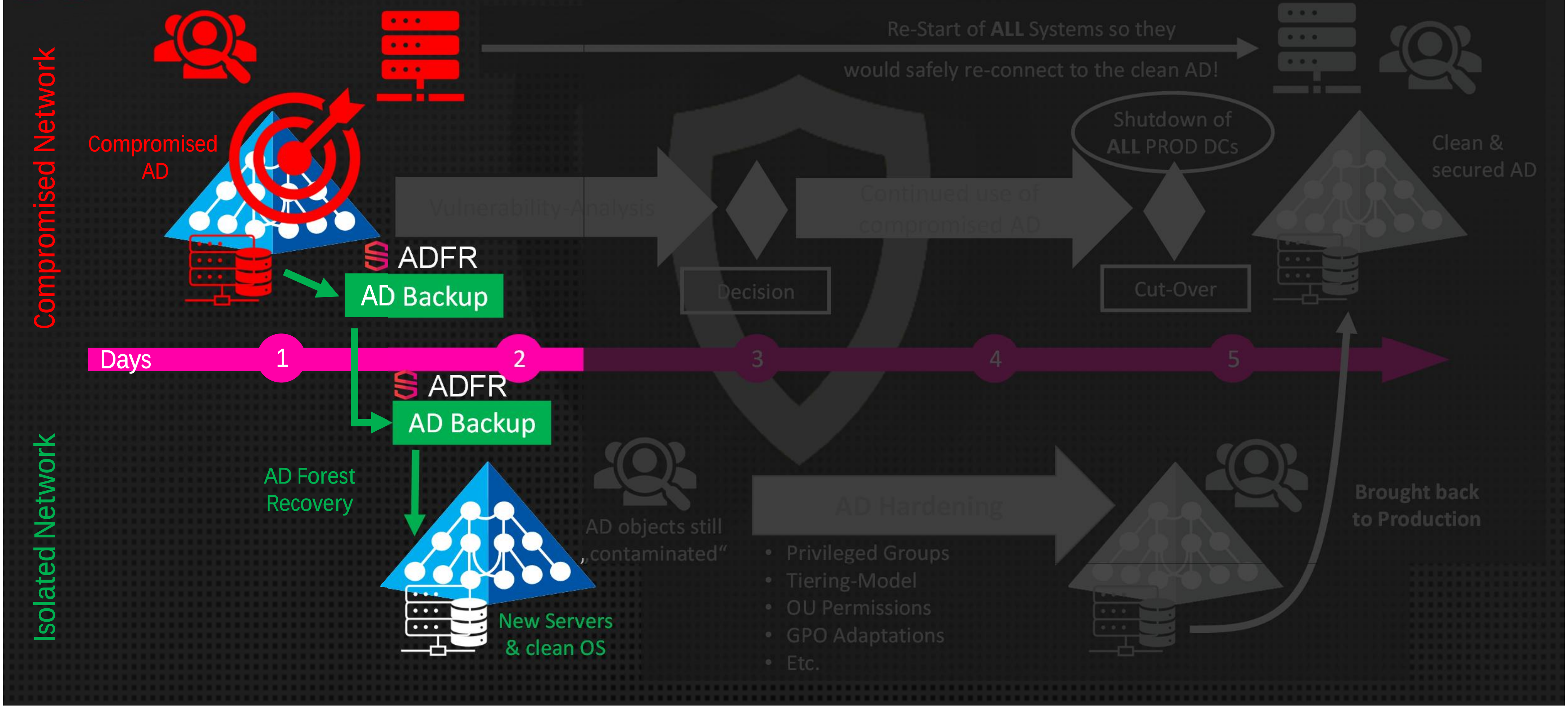
- Privileged Groups
- Tiering-Model
- OU Permissions
- GPO Adaptations
- Etc.

Brought back to Production

Real Life AD Incident/Recovery Scenario
> Oops, *You’ve Been BREACHED !!!*



Real Life AD Incident/Recovery Scenario
> *PHASE I - SAFETY NET For AD*



Compromised Network

Isolated Network

Compromised AD

ADFR

AD Backup

Days

1

2

3

4

5

ADFR

AD Backup

AD Forest Recovery

New Servers & clean OS

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

Vulnerability Analysis

Decision

Continued use of compromised AD

Shutdown of **ALL** PROD DCs

Cut-Over

Clean & secured AD

AD objects still „contaminated"

AD Hardening

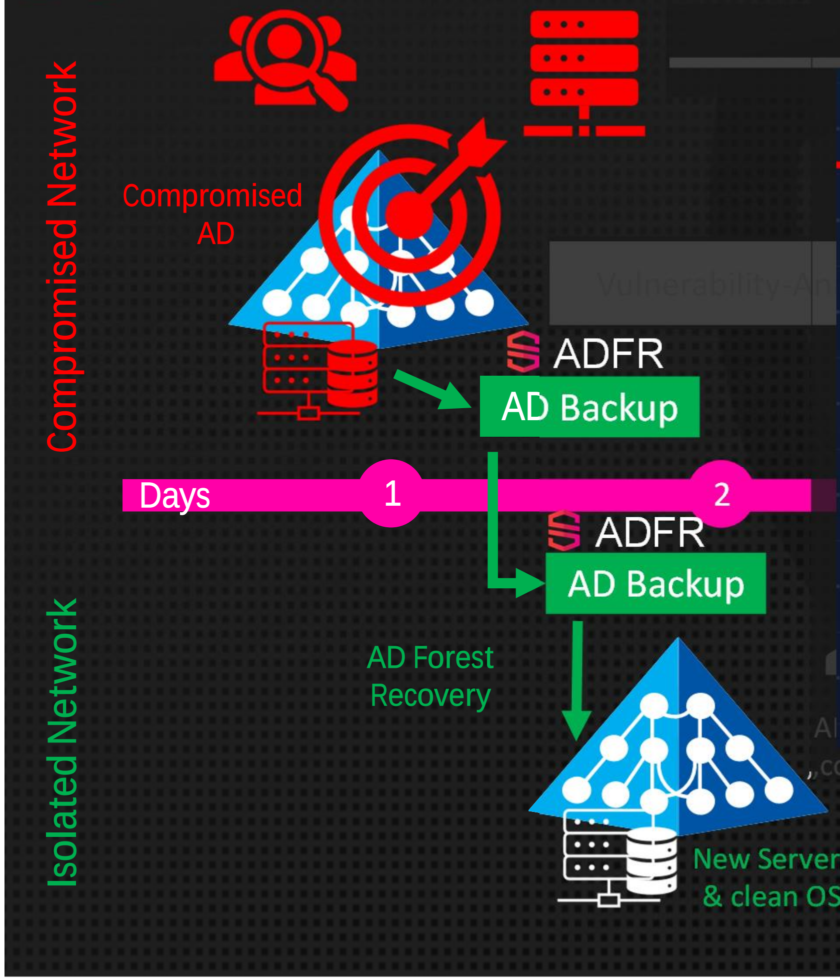
- Privileged Groups
- Tiering-Model
- OU Permissions
- GPO Adaptations
- Etc.

Brought back to Production

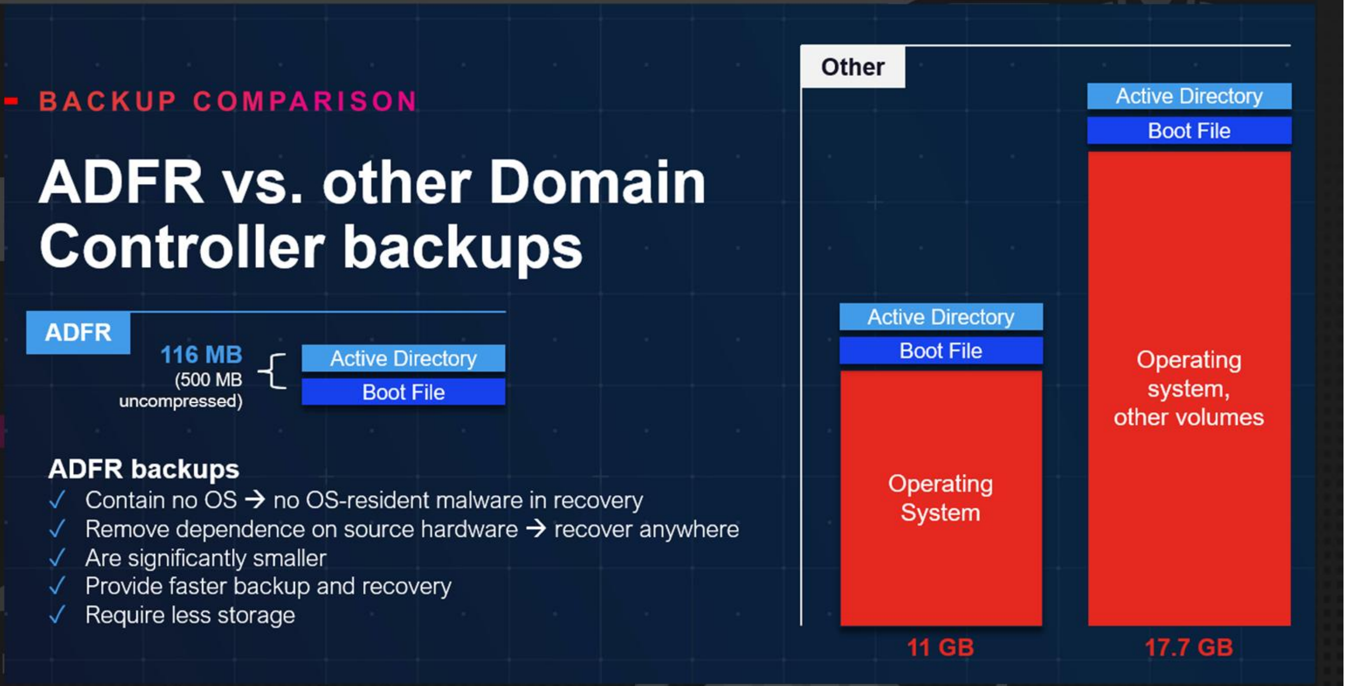
Real Life AD Incident/Recovery Scenario

> *PHASE I - SAFETY NET For AD*

semperis



Re-Start of **ALL** Systems so they



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

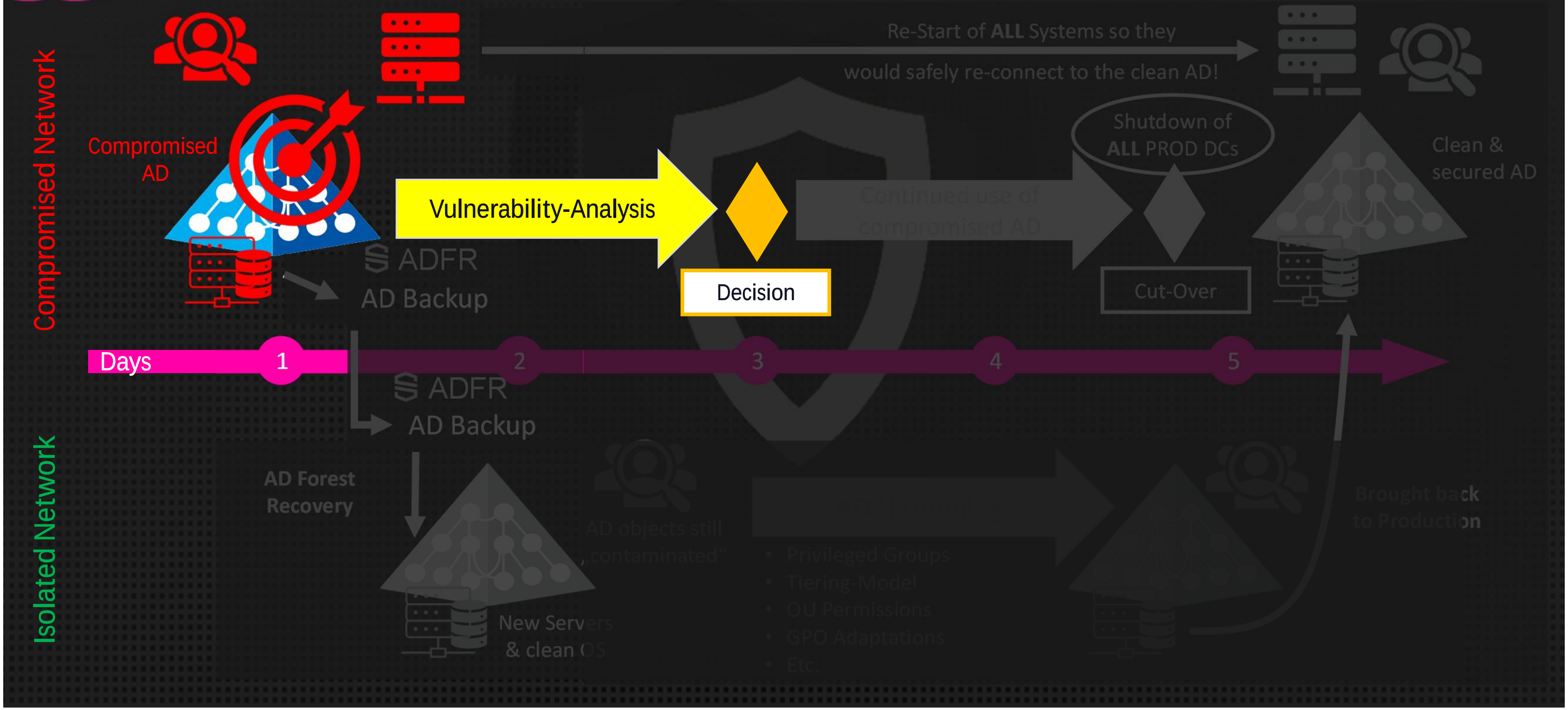
Al
„contaminated“

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

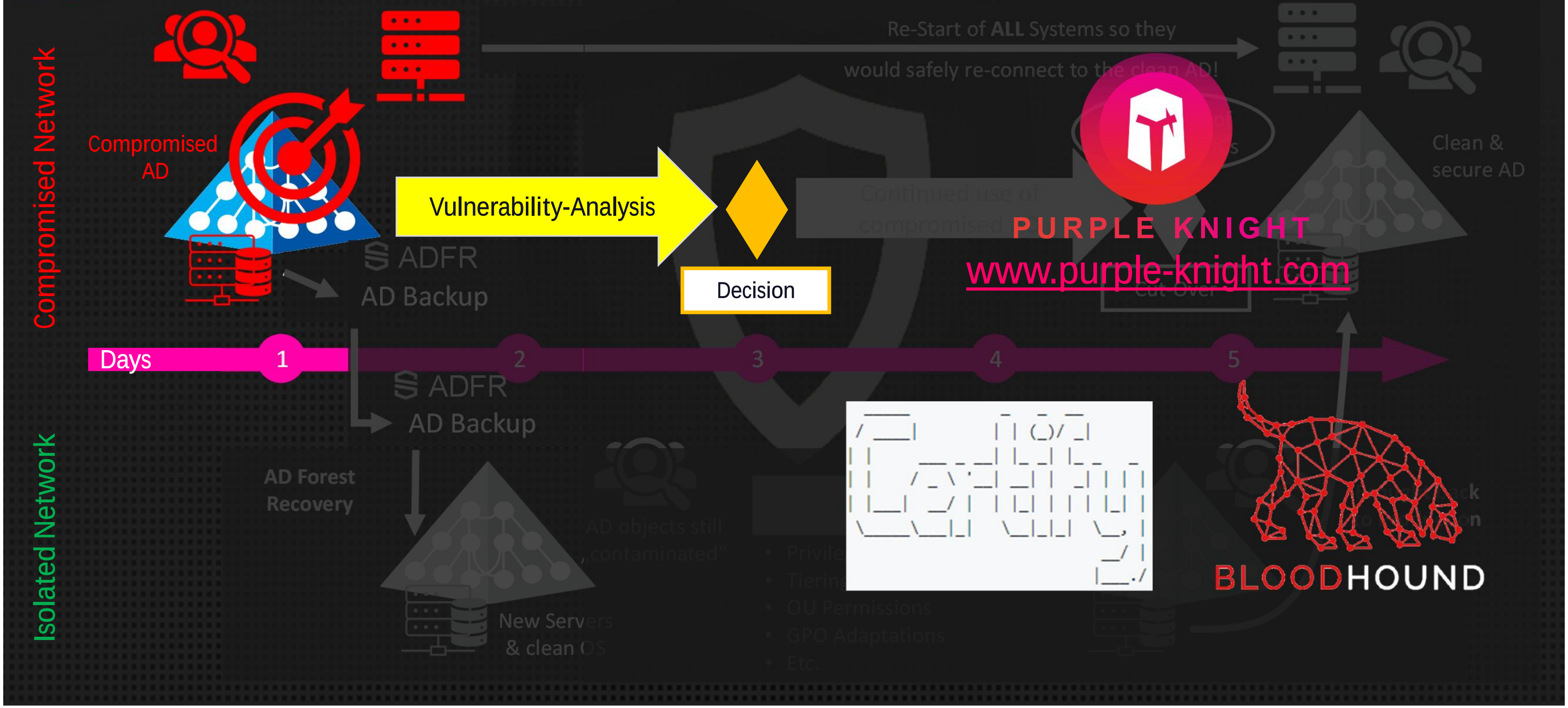
Real Life AD Incident/Recovery Scenario

> *PHASE II – AD Vulnerability Analysis*

semperis

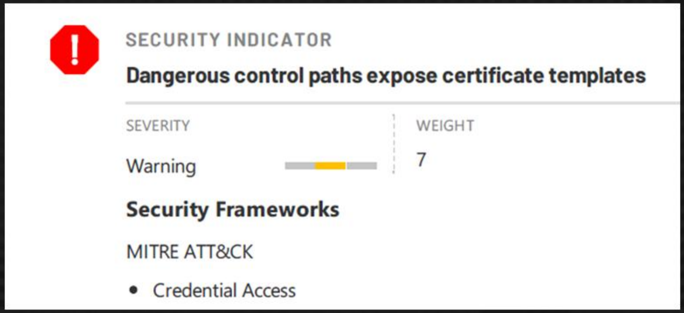


Real Life AD Incident/Recovery Scenario
> *PHASE II – AD Vulnerability Analysis*



Real Life AD Incident/Recovery Scenario
> Dubious Permissions & >1 Attackers

semperis



SECURITY INDICATOR

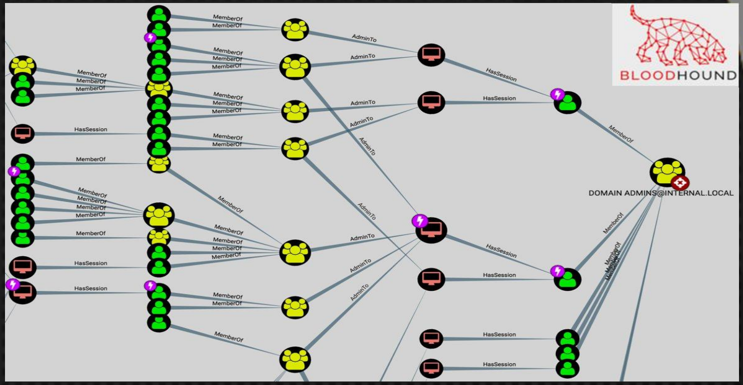
Dangerous control paths expose certificate templates

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!

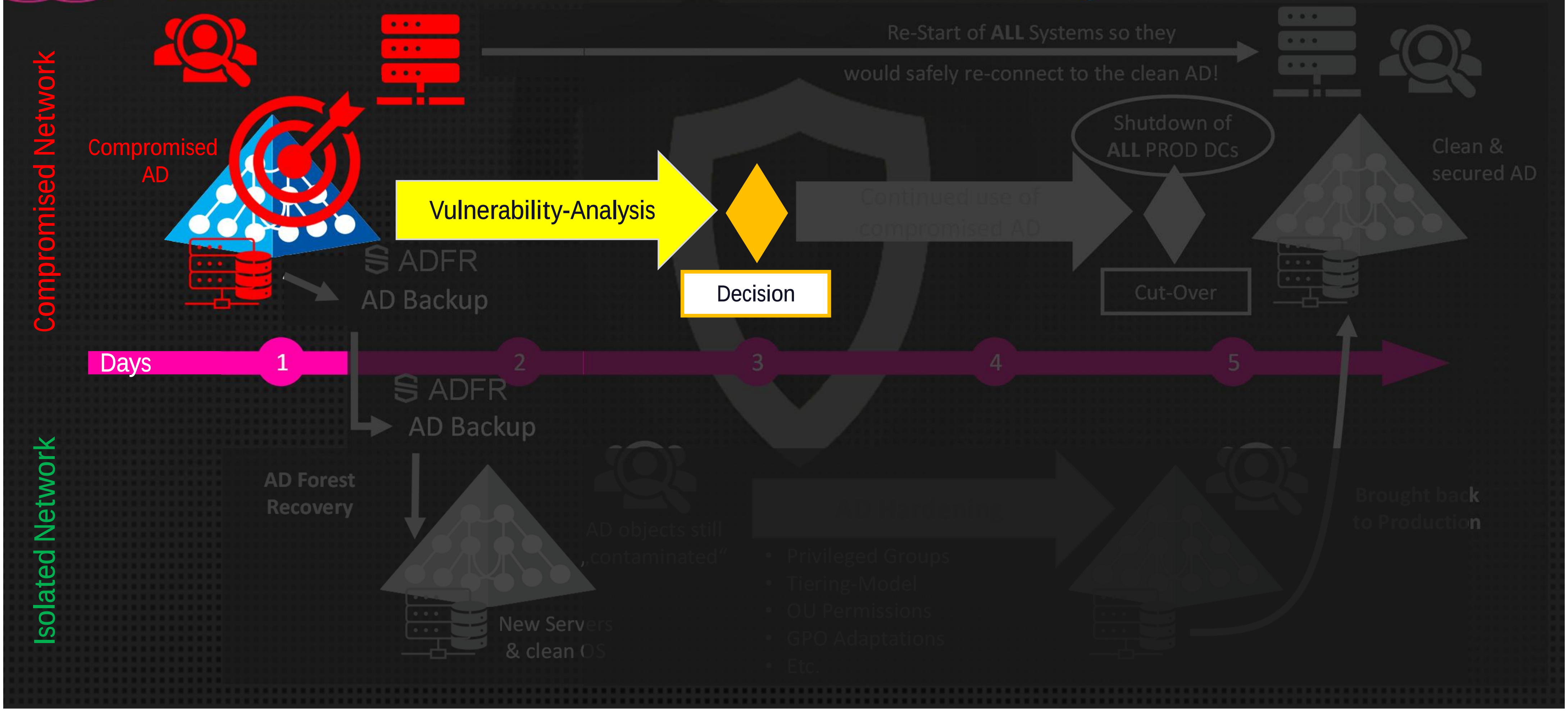
A special helpdesk account was granted the rights to reset the password of everyone in the domain.

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!

Real Life AD Incident/Recovery Scenario
> *PHASE II – AD Vulnerability Analysis*

semperis



Compromised Network

Isolated Network

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

Compromised AD

Vulnerability-Analysis

Decision

Continued use of compromised AD

Shutdown of **ALL** PROD DCs

Cut-Over

Clean & secured AD

ADFR AD Backup

Days 1 2 3 4 5

ADFR AD Backup

AD Forest Recovery

New Servers & clean OS

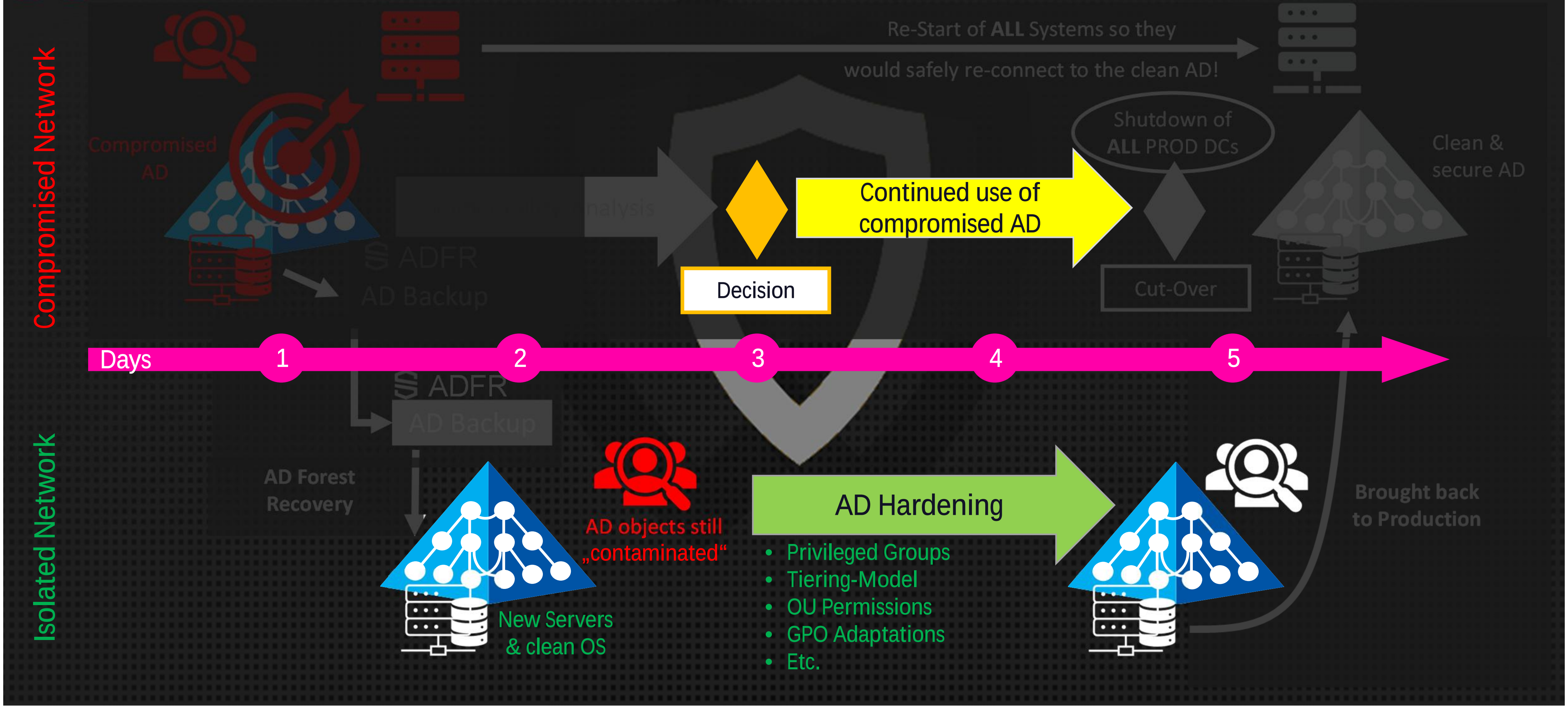
AD objects still „contaminated"

AD Hardening

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

Brought back to Production

Real Life AD Incident/Recovery Scenario
> PHASE III - Devide And Conquer!



Compromised Network

Compromised AD

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

nalysis

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

Isolated Network

ADFR AD Backup

AD Forest Recovery

New Servers & clean OS

AD objects still „contaminated“

AD Hardening

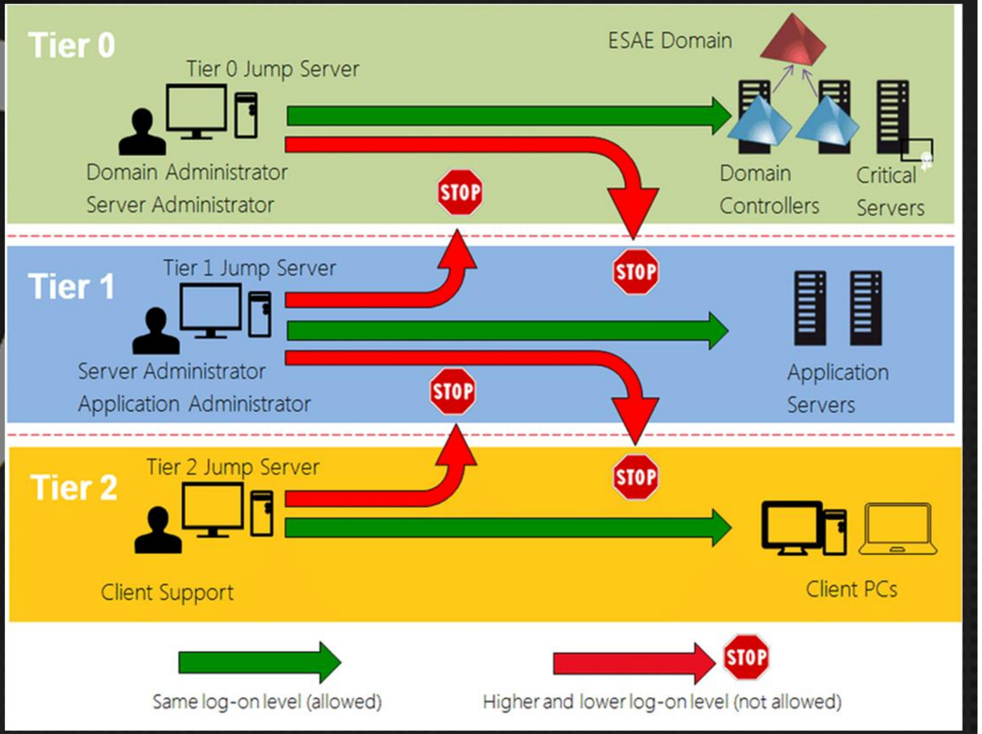
- Privileged Groups
- Tiering-Model
- OU Permissions
- GPO Adaptations
- Etc.

Brought back to Production

Real Life AD Incident/Recovery Scenario
> AD Hardening Speedway…

semperis

- Ø1.5 days available to harden AD
  - ØTiering-Model (w/o MFA)
  - ØCleaned up Privileged Groups
  - ØNEW accounts in Privileged Groups
  - ØProtected Users group
  - ØNo Privileged Accounts with SPNs
  - ØOU/AdminSDHolder Permissions
  - ØGPO Adaptations
  - Ø…



Tier 0

ESAE Domain

Tier 0 Jump Server

Domain Administrator
Server Administrator

STOP

Domain Controllers

Critical Servers

Tier 1

Tier 1 Jump Server

STOP

Server Administrator
Application Administrator

STOP

Application Servers

Tier 2

Tier 2 Jump Server

STOP

Client Support

Client PCs

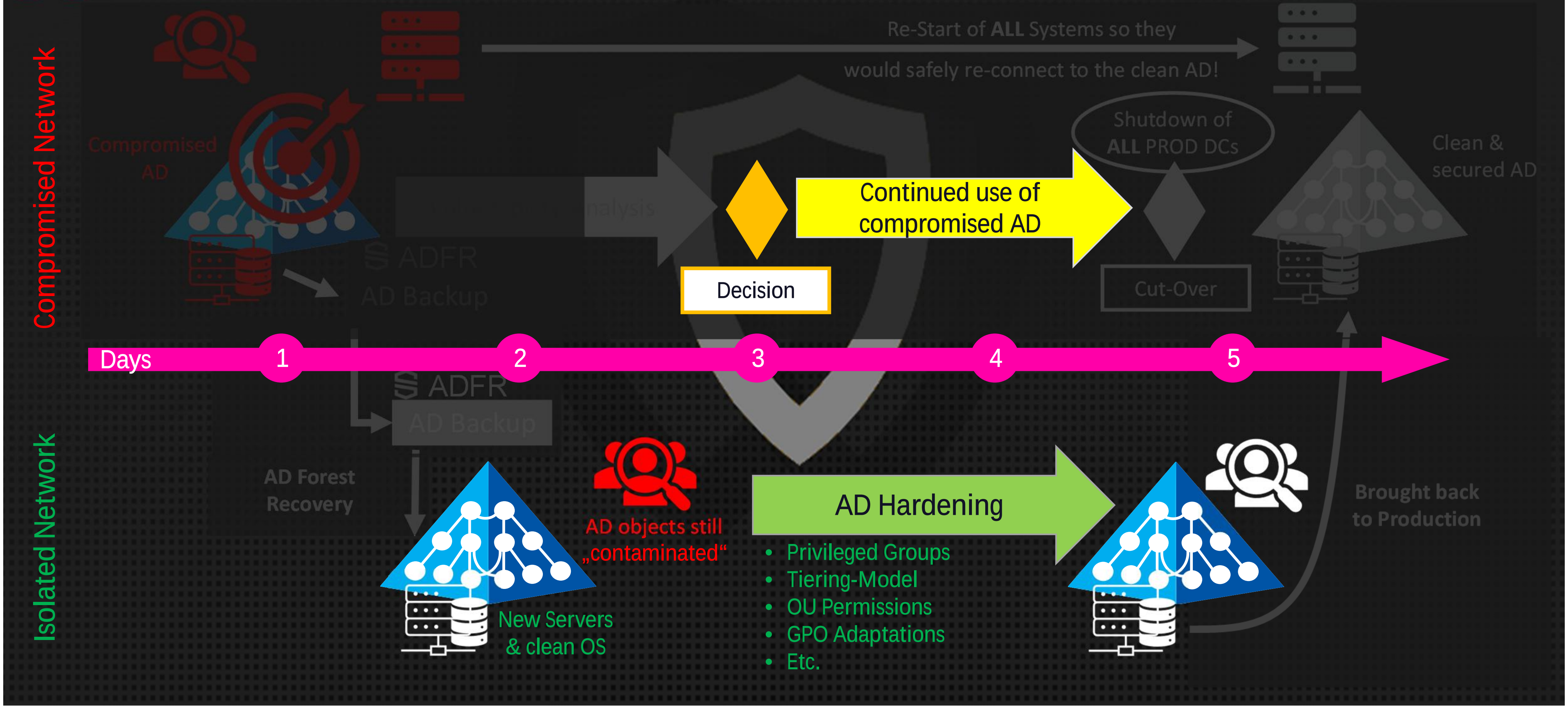
Same log-on level (allowed)

STOP

Higher and lower log-on level (not allowed)

Real Life AD Incident/Recovery Scenario
> PHASE III - Device And Conquer!

semperis

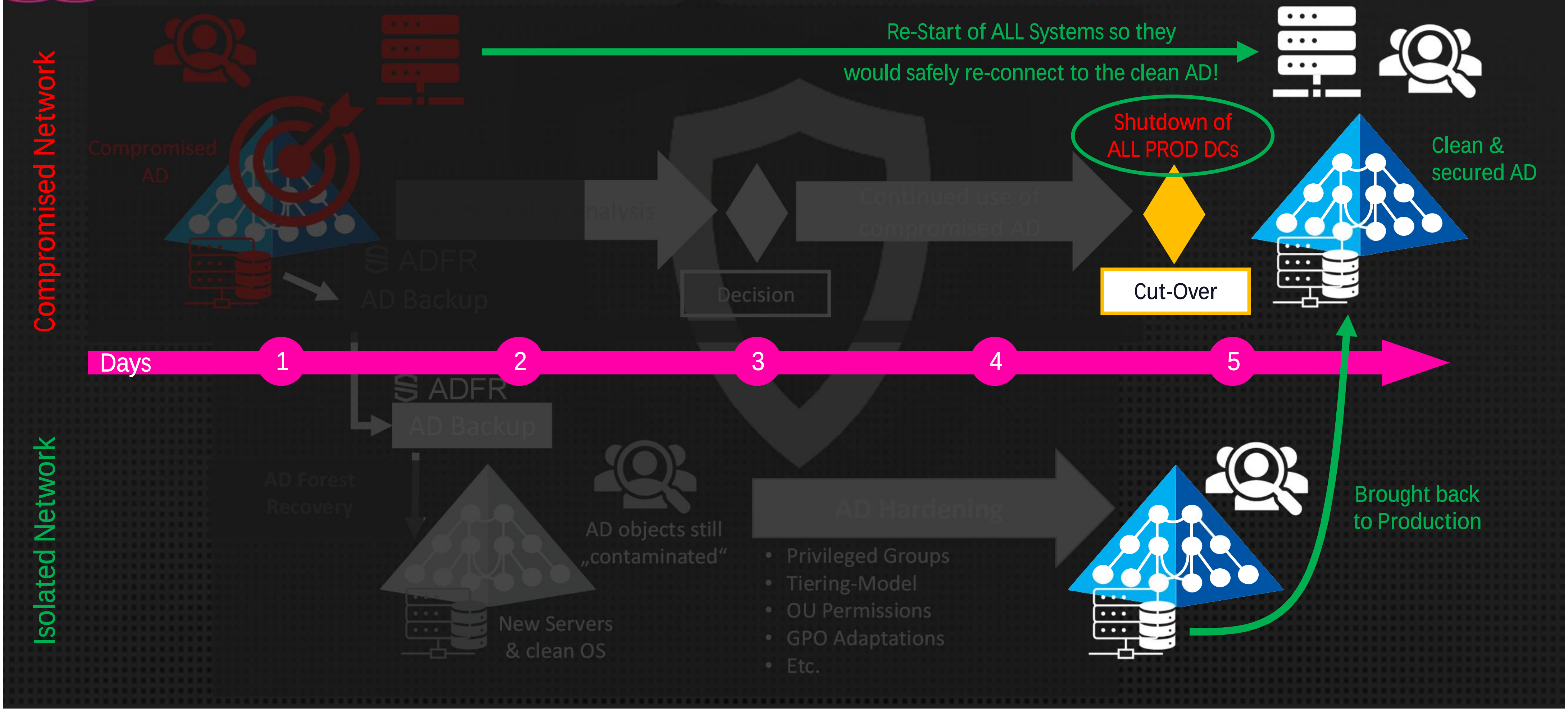


Compromised Network
Isolated Network
Compromised AD
Re-Start of **ALL** Systems so they would safely re-connect to the clean AD!
ADFR AD Backup
nalysis
Shutdown of **ALL** PROD DCs
Clean & secured AD
Decision
Continued use of compromised AD
Cut-Over
Days
1
2
3
4
5
ADFR AD Backup
AD Forest Recovery
AD objects still „contaminated“
New Servers & clean OS
AD Hardening
Brought back to Production

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

Real Life AD Incident/Recovery Scenario
> PHASE IV - Hardened AD Back To Prod

semperis



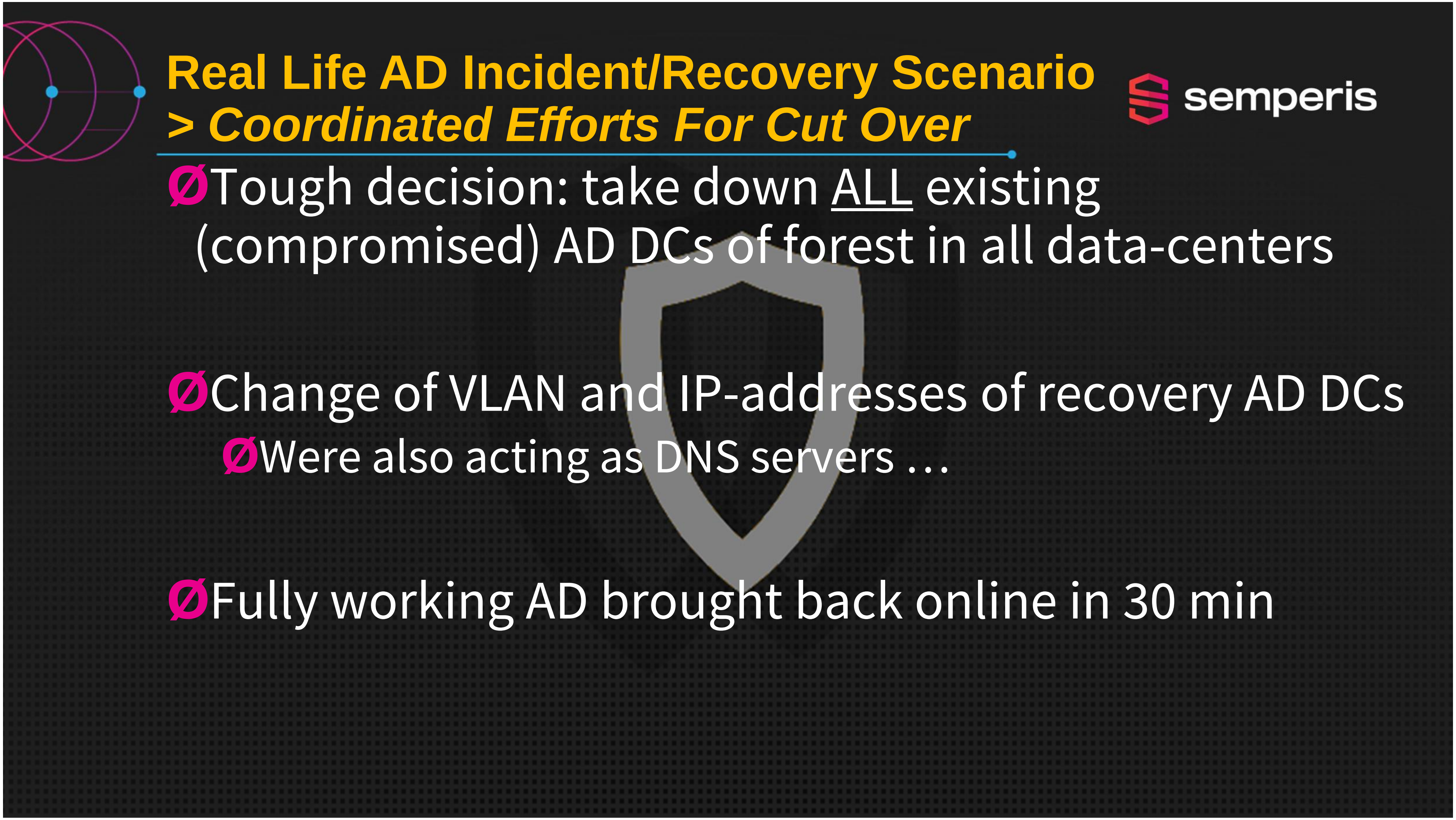
- Privileged Groups
- Tiering-Model
- OU Permissions
- GPO Adaptations
- Etc.

Real Life AD Incident/Recovery Scenario

> This Experience Felt Like…

semperis

Saudi's Again Changing Wheels Tyres while driving!



Real Life AD Incident/Recovery Scenario
> Coordinated Efforts For Cut Over

semperis

- ØTough decision: take down ALL existing (compromised) AD DCs of forest in all data-centers
- ØChange of VLAN and IP-addresses of recovery AD DCs
  - ØWere also acting as DNS servers …
- ØFully working AD brought back online in 30 min

Real Life AD Incident/Recovery Scenario
> Coordinated Efforts For Cut Over

semperis

ØFully Automated Recovery

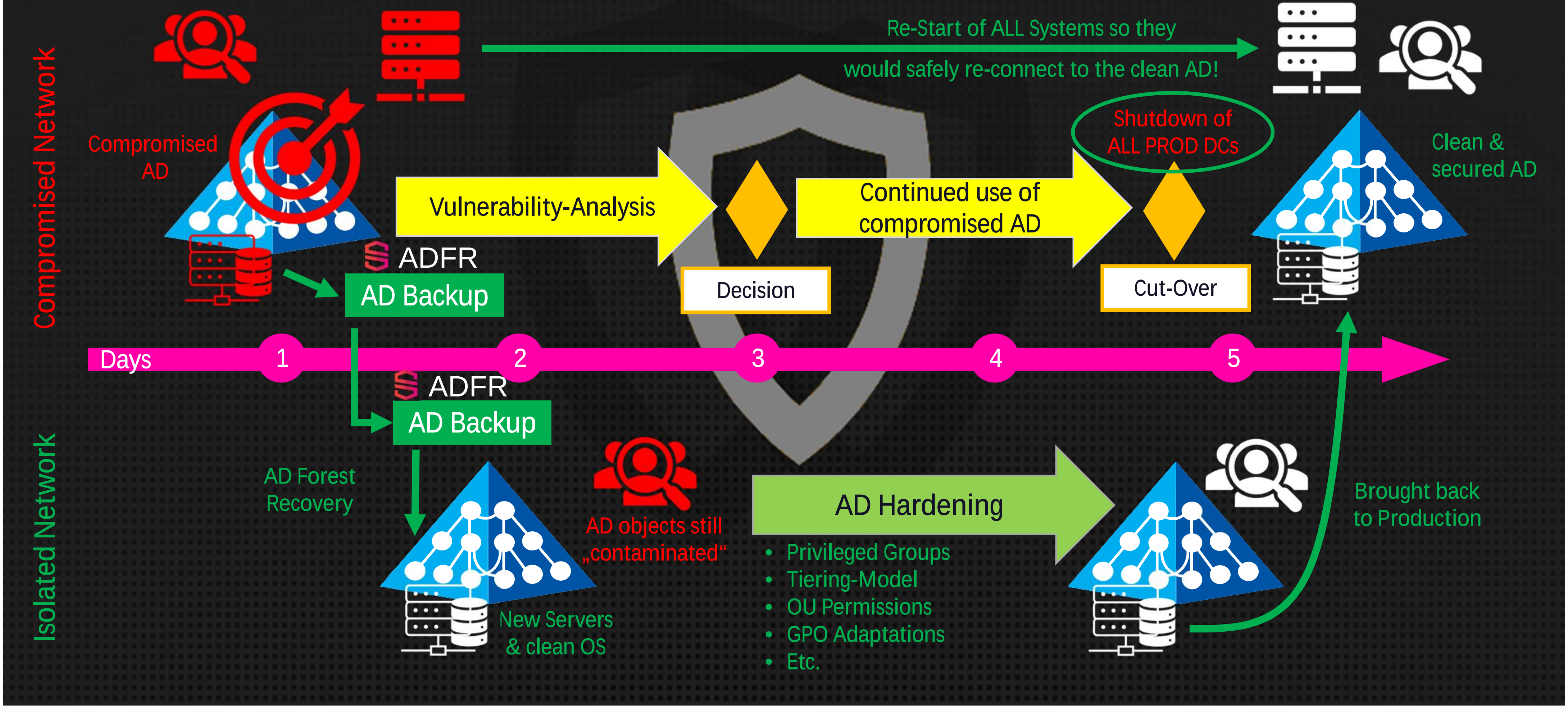
ØRestored DCs + Repromoted DCs + AD Service Steps

ØEDR Team had in parallel taken down more than 20 C2 (!) systems and blocked 100’s of external IPs

ØRebooted all servers and clients to ensure killing any existing process and to re-create secure channel with recovered AD

Real Life AD Incident/Recovery Scenario
> *In The End – They Survived! J*

semperis



Compromised Network

Isolated Network

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

Compromised AD

ADFR

AD Backup

Vulnerability-Analysis

Decision

Continued use of compromised AD

Shutdown of ALL PROD DCs

Cut-Over

Clean & secured AD

Days 1 2 3 4 5

ADFR

AD Backup

AD Forest Recovery

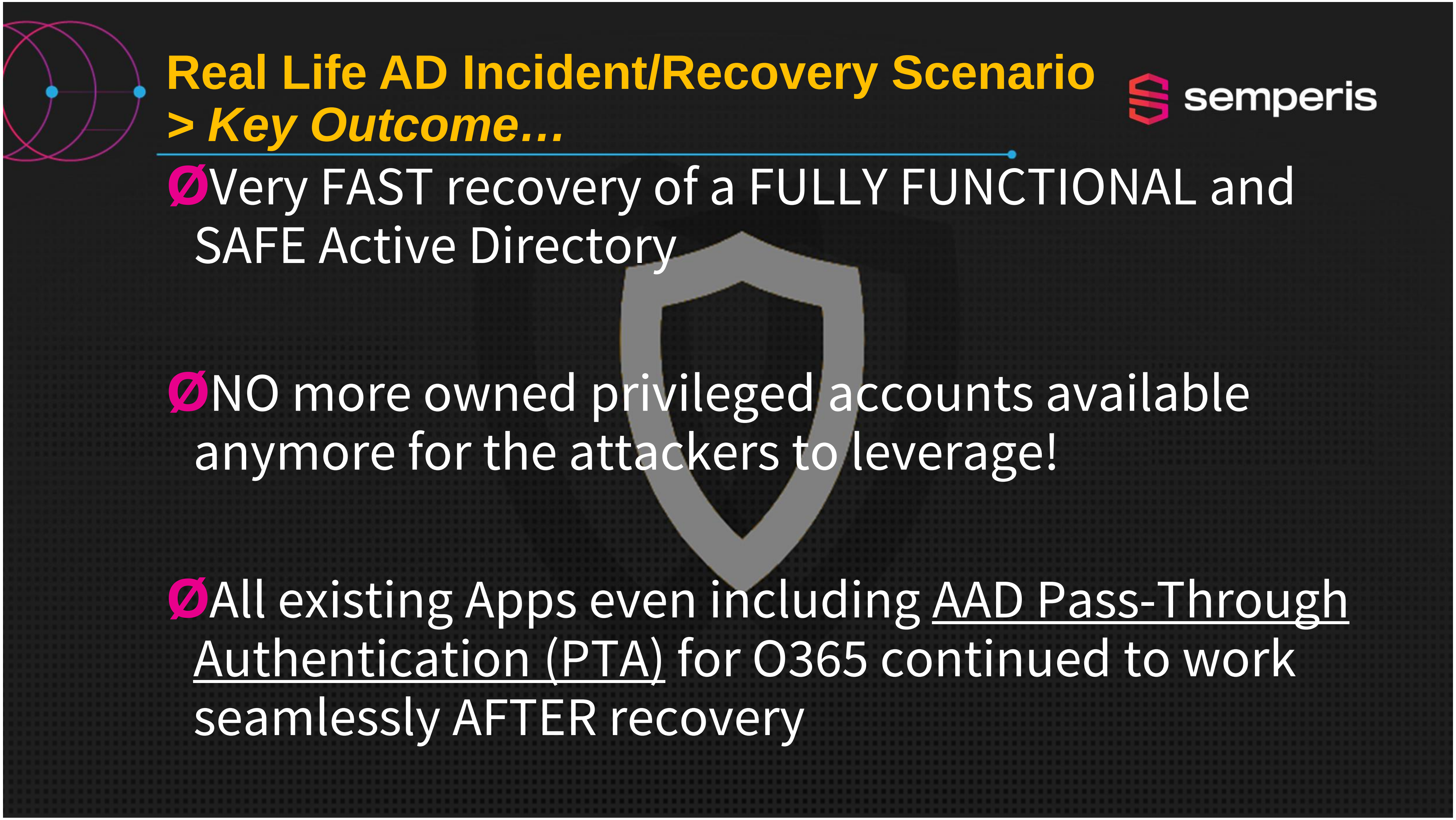
New Servers & clean OS

AD objects still „contaminated“

AD Hardening

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

Brought back to Production



Real Life AD Incident/Recovery Scenario

> Key Outcome…

semperis

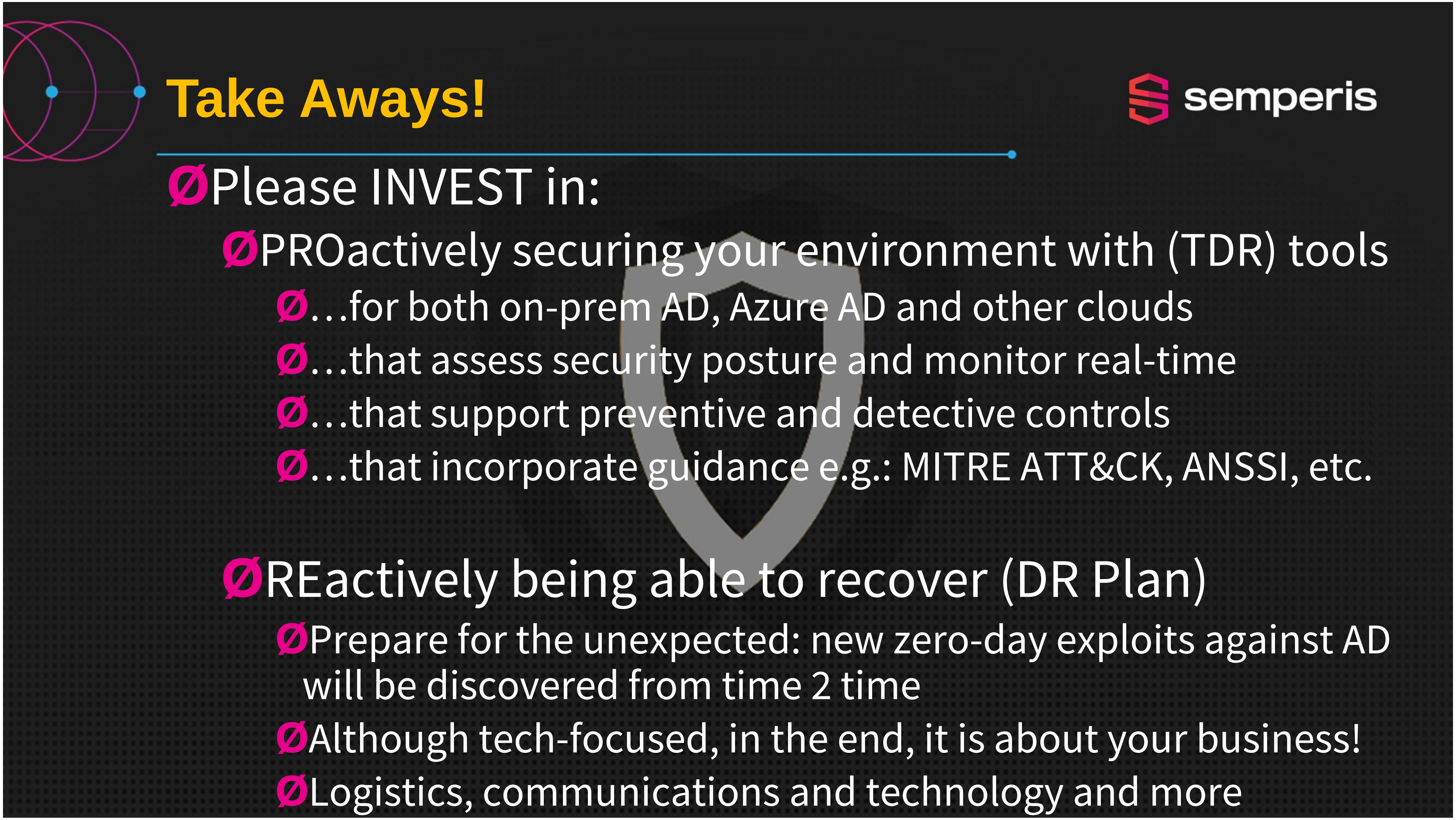
ØVery FAST recovery of a FULLY FUNCTIONAL and SAFE Active Directory

ØNO more owned privileged accounts available anymore for the attackers to leverage!

ØAll existing Apps even including AAD Pass-Through Authentication (PTA) for O365 continued to work seamlessly AFTER recovery

semperis

Take Aways!



Take Aways!

semperis

- ØPlease INVEST in:
  - ØPROactively securing your environment with (TDR) tools
    - Ø…for both on-prem AD, Azure AD and other clouds
    - Ø…that assess security posture and monitor real-time
    - Ø…that support preventive and detective controls
    - Ø…that incorporate guidance e.g.: MITRE ATT&CK, ANSSI, etc.
  - ØREactively being able to recover (DR Plan)
    - ØPrepare for the unexpected: new zero-day exploits against AD will be discovered from time 2 time
    - ØAlthough tech-focused, in the end, it is about your business!
    - ØLogistics, communications and technology and more

Take Aways!

semperis

ØSEEK HELP if needed, BEFORE attack/breach

ØAUTOMATE as much as possible

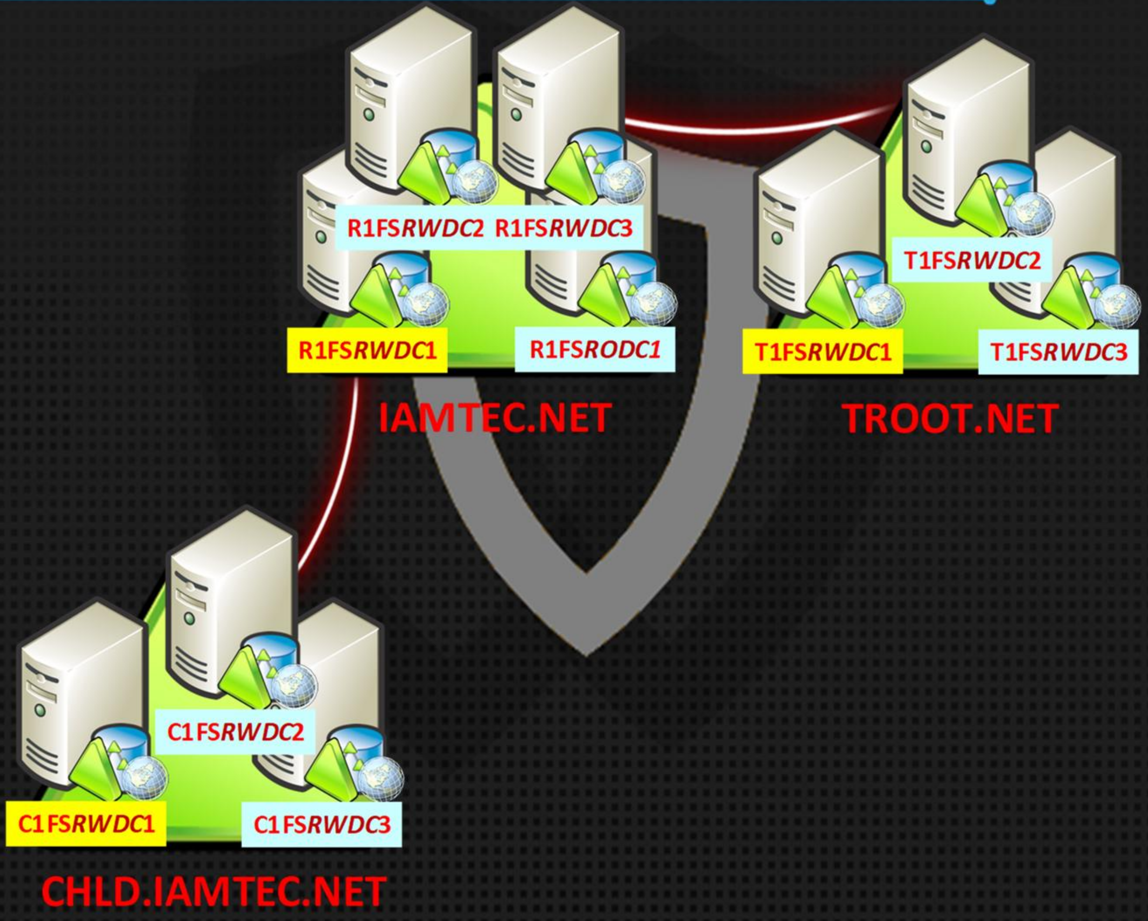
- Ø AD recovery is more than restoring single/multiple DCs
- Ø Consider 3rd party tool (= BEST Insurance, Fastest RTO!)

ØHave Quality Assurance Check on DR plan!

- Ø It is NOT just about recovery, it needs to be secure too!
- Ø Perform periodic DR drills

Demo! - While Presenting

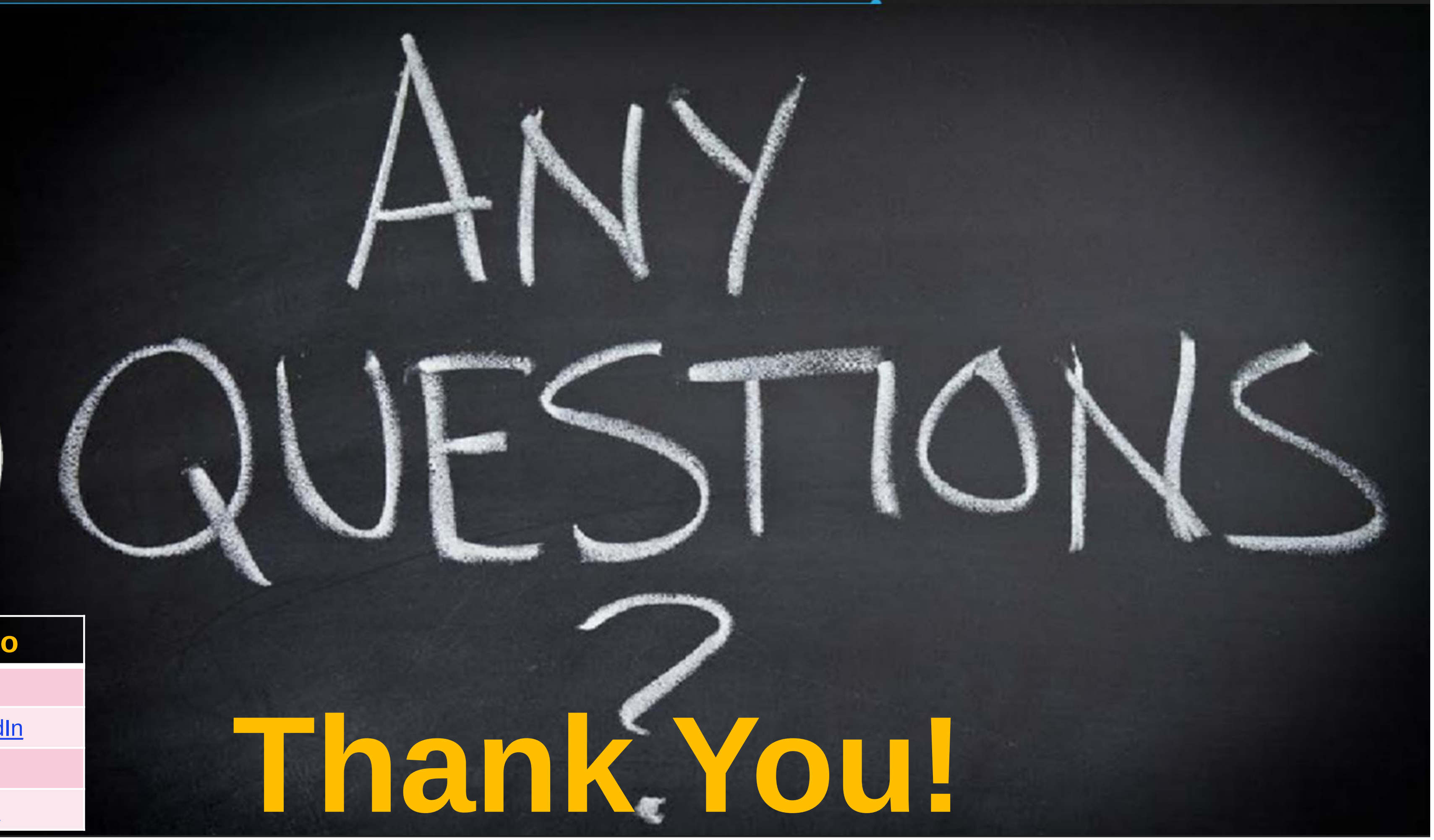
semperis



Questions? – Get In Touch!

semperis

Jorge de Almeida Pinto	
Contact	jorged@semperis.com
LinkedIn	http://tiny.cc/JorgeLinkedIn
Blog	http://tiny.cc/JQFKblog
Twitter	http://tiny.cc/JQFKtwitter



Thank You!