

Resurrecting After A Ransomware Attack

Be Secure(d), And Prepared!



Active Directory

Jorge de Almeida Pinto

Senior Solutions Architect | Senior Incident Response Lead

SEMPERIS.COM



Jorge de Almeida Pinto

Senior Solutions Architect

Senior Incident Response Lead



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

Introducing
Me, Myself & I!

- 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.

SEMPERIS.COM

Introducing Semperis



Preparedness

Response

AD Security Assessment

AD Threat Mitigation

AD DR Planning & Exercise

Cyber-First AD Recovery

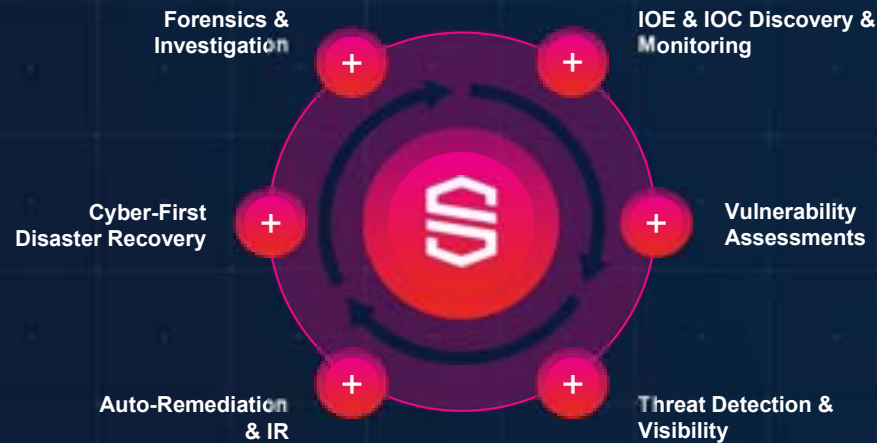
AD Incident Investigation & Attack Forensics

AD Threat Removal

Before an attack

During an attack

After an attack

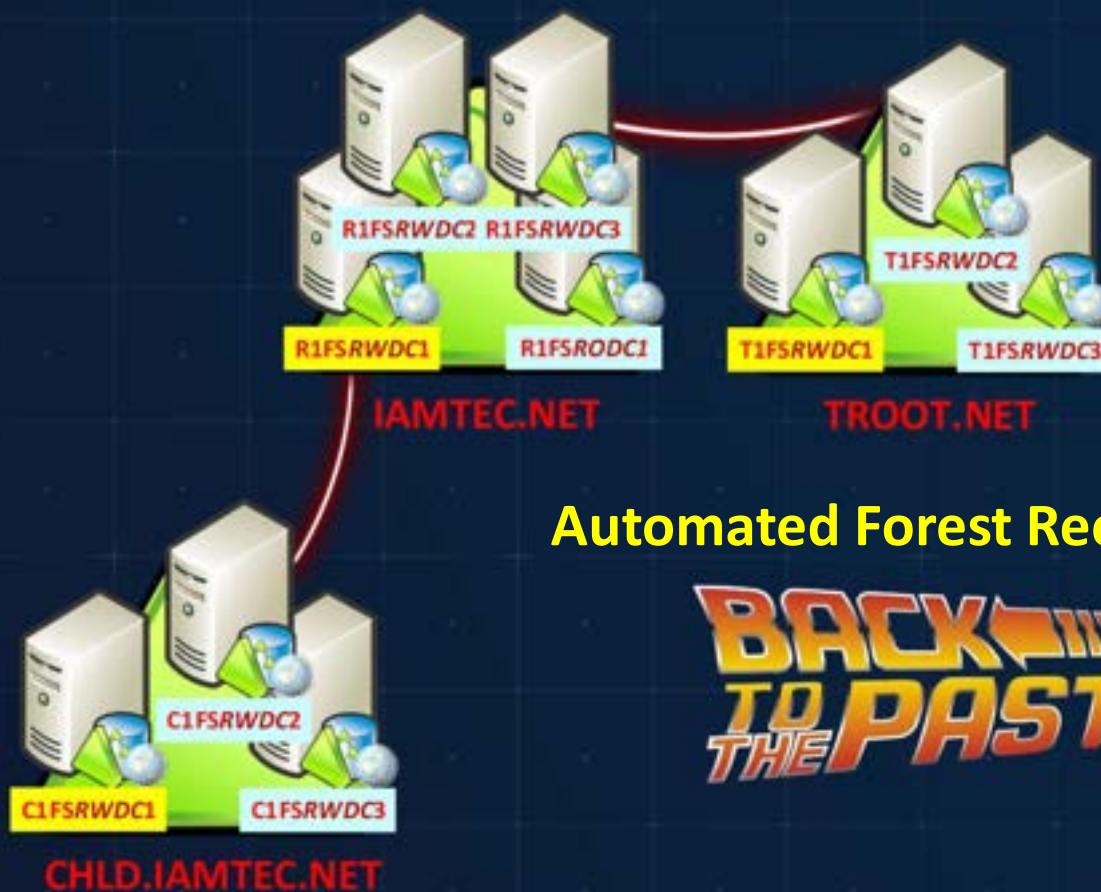


Agenda



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! – Automated Recovery, While Presenting



Securing & Protecting AD

Securing And Protecting AD

- Pro-Actively - Search And Fix
 - By looking for Indicators of Exposure (IoEs)
 - Account Hygiene - Settings and Passwords
 - Security Related Configurations in AD
 - “Invisible” attack paths
 - By looking for Indicators of Compromise (IoCs)
 - DC Shadow
 - Kerberoasting
 - ... and many more
- THINK 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](#)

***** 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,

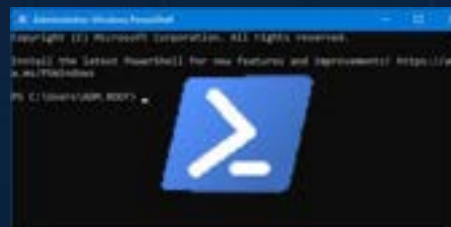
Details About Account Security And Password Hygiene (Without ReUsed Hashes Displayed!)

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

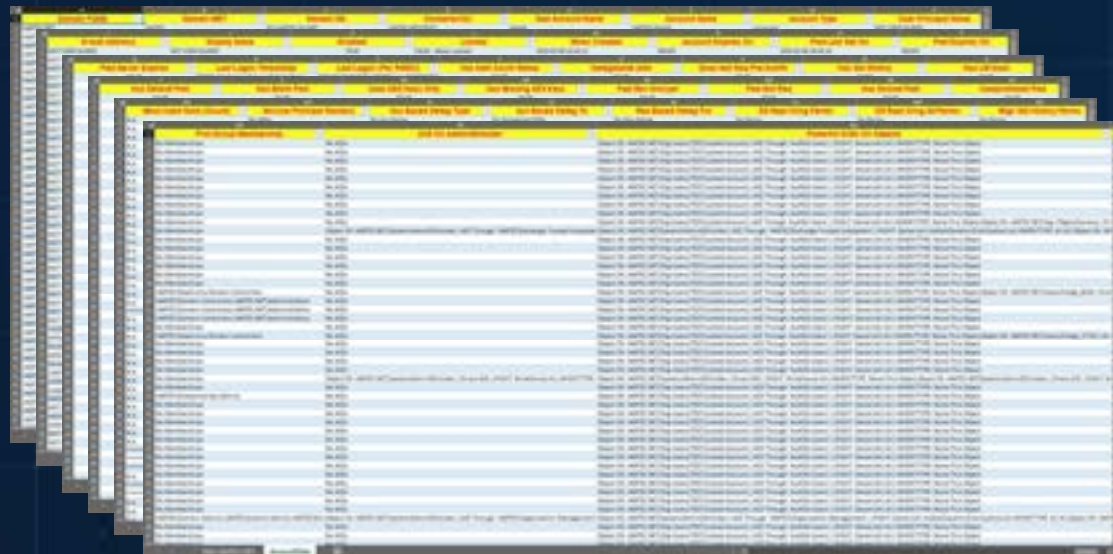
g AD



Detection Response (TDR) Tools!



➤ Do-It-Yourself in PowerShell



Securing And Protecting AD



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



PURPLE KNIGHT

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



ADDITIONAL IDEs FOUND			
Issue	Severity	Impact	Action
Active Directory Administrative Group used within the service units	Warning	Medium	Read More
Certificate templates with Exp-This-Access-Configurations	Warning	Medium	Read More
Changes in the Windows 2022 Certificate Policy Group membership	Warning	Medium	Read More
Check if legacy authentication is allowed	Warning	Medium	Read More
Computer to user accounts with unenforced delegation	Warning	Medium	Read More
Computers with password less (all over 90 days ago)	Warning	Medium	Read More
Enterprise rooted paths expose certificate templates	Warning	Medium	Read More
Enterprise trust attributes list	Warning	Medium	Read More
Domain trust in which party domain without operations	Warning	Medium	Read More

SECURITY INDICATOR

Evidence of Mimikatz DCSync attack

Severity: Critical | Score: 10 | LATEST ATTACK: Privileged Access | Defense: Evade

Description
DCSync attacks enable attackers that have achieved privileged domain access to request 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. The 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 malicious 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 DCSync may have been used to compromise your environment.

Management	CreatedDate	DistinguishedName	lastModified
	11-Jan-2022 19:28:27	CN=RYOXTADM.DU+Computer/CN=RID-SPIN-TO-ADD-DU+Org-Users/CN=66ATSC.DC=NET	19-Jun-2021 00:07:29

Showing 1 of 1

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

CRITICAL IDEs FOUND

- Certificate templates that allow requesters to spe...**
This indicator checks if certificate templates are enabling requesters to specify a subjectAltName in the CSR.
- 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 ...
- Non-default principals with GC Sync rights on the ...**
Any security principals with Replicate Changes All and Replicate Directory Changes permissions on the domain...
- 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.
- Users with permissions to set Server Trust Account**
Checks for permissions on the domain DC host that enables a user to set a LAC flag - Server_Trust_Account on computer ...

Securing And Protecting AD

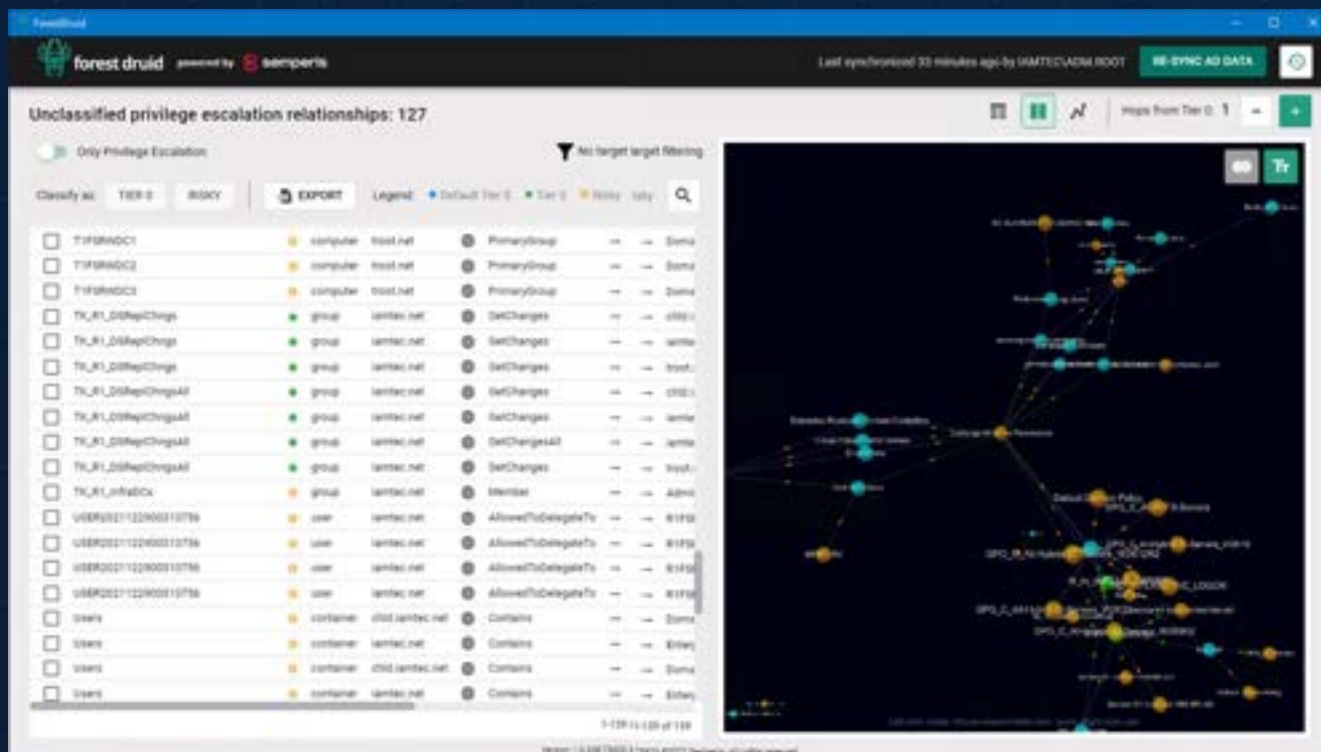


➤ How? - You ask? – Threat Detection Response (TDR) Tools!



FOREST DRUID

- Extraction of AD data through “Collector” command-line tool, or GUI
- Imported/Processed by Forest Druid UI-tool to visualize attack-path(s) (INSIDE-OUT!)



Securing And Protecting AD

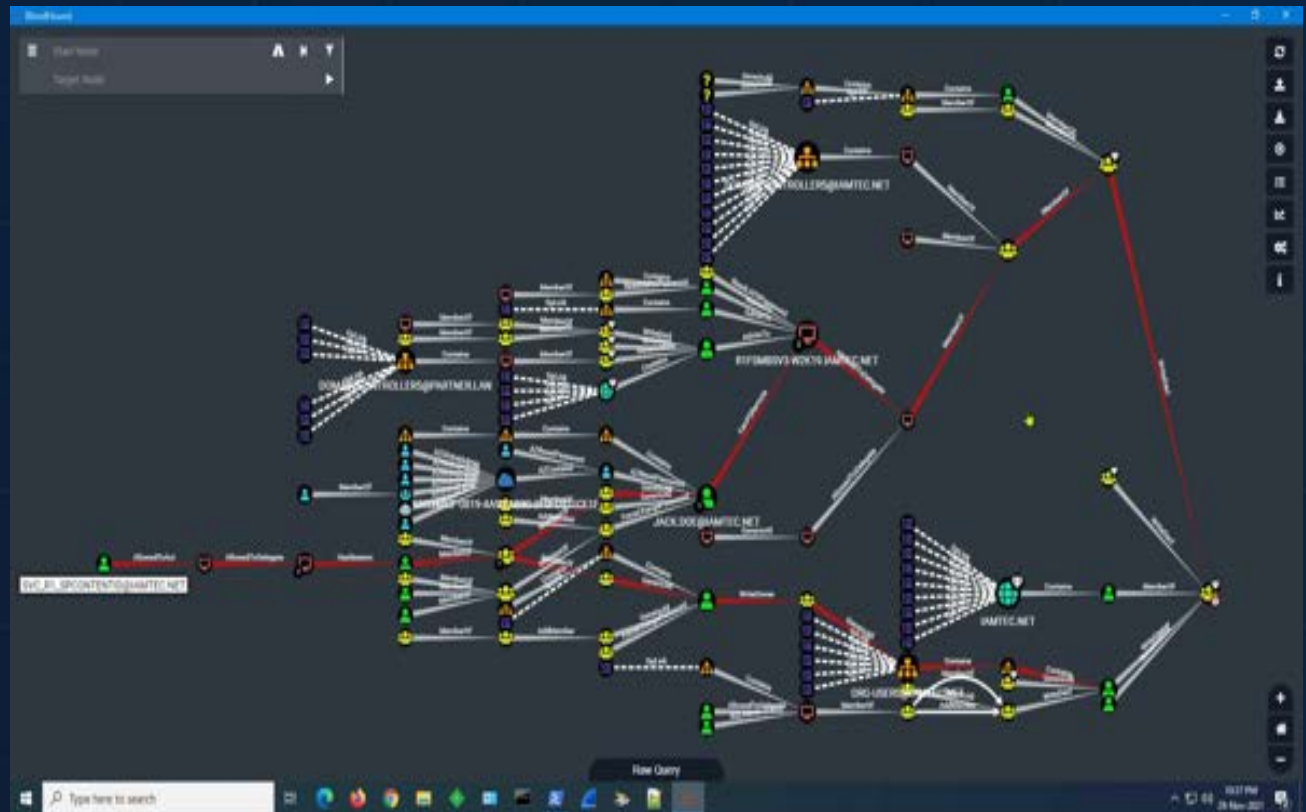


➤ How? - You ask? – Threat Detection Response (TDR) Tools!



BLOODHOUND

- Extraction of AD data through “SharpHound” command-line tool
- Imported/Processed by BloodHound UI-tool to visualize attack-path(s) (**OUTSIDE-IN**)



Securing And Protecting

➤ How? - You ask? – Threat



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

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. 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.

Compare with statistics Privacy notice

<p>State Objects : 91 / 100 It is about operations created to user or computer objects. 10 rules identified</p>	<p>Trusts : 21 / 100 It is about links between two Active Directories. 1 rule identified</p>
<p>Privileged Accounts : 100 / 100 It is about administrators of the Active Directory. 17 rules identified</p>	<p>Anomalies : 100 / 100 It is about specific security-related points. 15 rules identified</p>

Risk model

State Objects	Privileged accounts	Trusts	Anomalies
Service user authentication	Administer local users	Self trust protocol	Self
Service user accounts	Self Check	Self checking	Selflog
Client configuration	Admin console	Selfcheck	Selfcheck self-log
Service log	Admin console	Self check protocol	Selfcheck self-log
Self authentication protocol	Selfcheck Check	Trust source	Self group operations
Selfchecking	Selfcheck change	Trust self check	Selfcheck selflog
Selfcheck	Selfcheck console		Selfcheck selfcheck
Selfcheck management	Selfcheck console		Selfcheck selfcheck

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

emperis

Securing And Protecting AD



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



- Command-line tool to enumerate misconfigurations in Active Directory Certificate Services (AD CS).

```
Administrator: Command Prompt

Certify

v1.0.0

[*] Action: Find certificate templates
[*] Using the search base 'CN=Configuration,DC=IARTEC,DC=NET'
[*] Listing info about the Enterprise CA 'PNI-ROOT-CA-IARTEC'

Enterprise Ca Name      : PNI-ROOT-CA-IARTEC
DNS Hostname           : IPRNASRV.IARTEC.NET
Fullname                : IPRNASRV.IARTEC.NET\PNI-ROOT-CA-IARTEC
Flags                  : SUPPORTS_NT_AUTHENTICATION, CA_SERVICE_TYPE_ADVANCED
Cert SubjectName       : CN=PNI-ROOT-CA-IARTEC, DC=IARTEC, DC=NET
Cert Thumbprint        : 35AF342383863268A8688199A878205A81376
Cert Serial            : 808C378D1A0C8847AC884F93481F8
Cert Start Date        : 12/26/2014 3:21:11 PM
Cert End Date          : 12/26/2014 3:41:08 PM
Cert Chain              : CN=PNI-ROOT-CA-IARTEC,DC=IARTEC,DC=NET
[*] UserSpecifiedName : SDTP_ATTRIBUTES,OBJECTS,NAME set, enrollees can specify subject Alternative Names!
CA Permissions
  Owner: NT AUTHORITY\Administrators 5-1-5-32-544

Access Rights      Principal
-----
Allow Enroll      NT AUTHORITY\Authenticated Users 5-1-5-32-544
Allow ManageCA, ManageCertificates  NT AUTHORITY\Administrators 5-1-5-32-544
Allow ManageCA, ManageCertificates  IARTEC\Domain Admins 5-1-5-21-963889158-2862672812-2629964136-512
Allow ManageCA, ManageCertificates  IARTEC\Enterprise Admins 5-1-5-21-963889158-2862672812-2629964136-519

Enrollment Agent Restrictions : None
```

```
Administrator: Command Prompt

[*] Vulnerable Certificates Templates :

CA Name      : IPRNASRV.IARTEC.NET\PNI-ROOT-CA-IARTEC
Template Name : ADPItemsLineAgentCertificate
Schema Version : 4
Validity Period : 2 years
Renewal Period : 6 weeks
wPKI-Certificate-Name-Flag : ENROLLEE_SUPPLIES_SUBJECT
wPKI-Enrollment-Flag : NONE
Authorized Signatures Required : 0
Application Policies : Certificate Request Agent
AllowEnrollmentCoverage : Certificate Request Agent
wPKI-Certificate-application-policy : Certificate Request Agent
Permissions
Enrollment Permissions
  Enrollment Rights : IARTEC\IWC_RI_ADFS 5-1-5-21-963889158-2862672812-2629964136-1394
  AutoEnrollment Rights : IARTEC\IWC_RI_ADFS 5-1-5-21-963889158-2862672812-2629964136-1394
  All Extended Rights : NT AUTHORITY\Authenticated Users 5-1-5-11
  Keyset Control Permissions
  Issues
  Full Control Principals
  WriteOwner Principals

Writeable Principals
  IARTEC\IWC_RI_ADFS 5-1-5-21-963889158-2862672812-2629964136-1394
  IARTEC\Enterprise Admins 5-1-5-21-963889158-2862672812-2629964136-519
  IARTEC\IWC_RI_PKI-CertEnroll-Flags 5-1-5-21-963889158-2862672812-2629964136-1312
  NT AUTHORITY\Authenticated Users 5-1-5-11

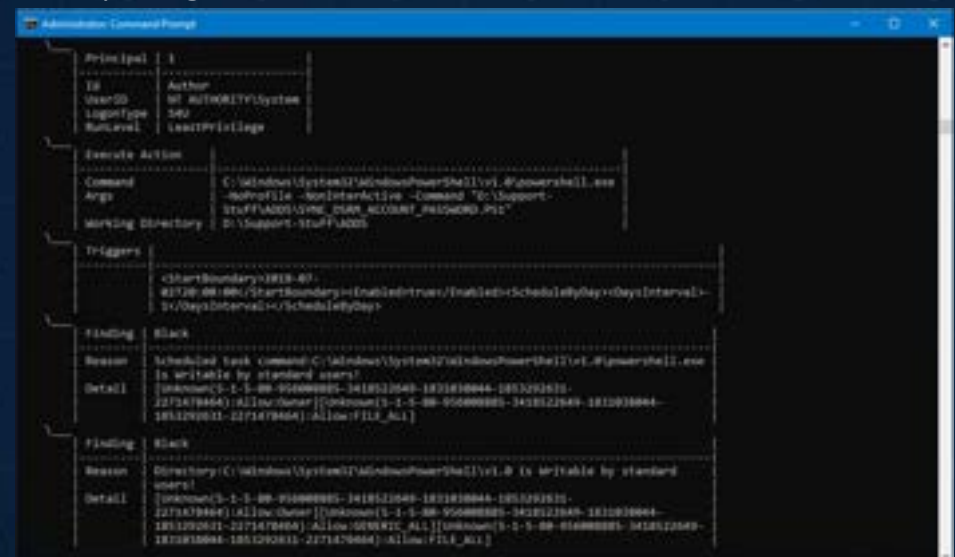
WriteProperty Principals
  IARTEC\Domain Admins 5-1-5-21-963889158-2862672812-2629964136-512
  IARTEC\Enterprise Admins 5-1-5-21-963889158-2862672812-2629964136-519
  IARTEC\IWC_RI_PKI-CertEnroll-Flags 5-1-5-21-963889158-2862672812-2629964136-1312
  NT AUTHORITY\Authenticated Users 5-1-5-11
```


Securing And Protecting AD

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



- Command-line tool to enumerate (relevant) settings in AD GPOs to identify exploitable misconfigurations
- Parses GPO config files from SYSVOL, and looks at other files referenced within GPOs, like scripts, MSI packages, exes, etc.



AD DR Plan - Why?

AD DR Plan - Why?

- In Many Cases....AD Has The Keys To The KINGDOM!

If Active Directory isn't secure, nothing is!

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



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

AD DR Plan - Why?

➤ Business Reasoning



➤ Regulations:

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



➤ Complexity:

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

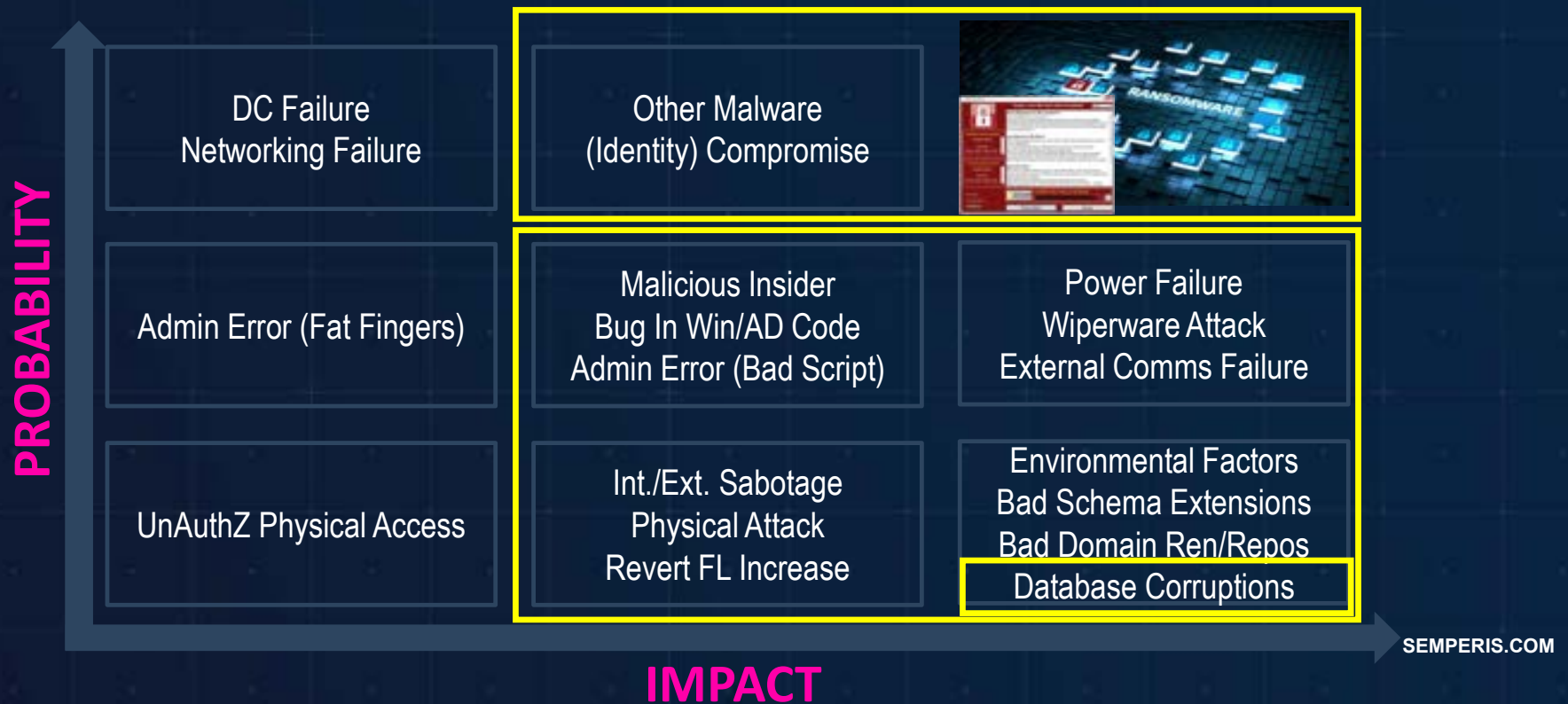


➤ Risk Management:

- Previous: “unlikely”; Now: “very common” → very high impact
- AD Down? → Acceptable follow-up risks and costs?

AD DR Plan - Why?

- Business Reasoning
 - Probability/Impact of Scenarios



AD DR Plan - Options

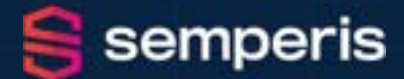
AD DR Plan - Options



	MSFT Default AD DR Plan - Manual (NO Automations) -	Customized AD DR Plan - SEMI Automated, a.k.a. D-I-Y -	Customized AD DR Plan - FULLY Automated -
<i>Focus</i>	Core only, no dependencies	Comms, logistics, pre/post, core, dependencies	
<i>Text/Tools</i>	High/None	Medium/E.g. PowerShell	Low/Commercial tool (AD focused, ADFR)
<i>Risk Mitigation/Pre/Post-Tasks</i>	Not described	Described	
<i>Core Tasks</i>	Described, unclear sequence	Described, clear sequence	
<i>Orchestration Backup/Rstre/AD</i>	Backup: Auto Restore: None AD: None	Backup: Auto Restore: None AD: Semi	Backup: Auto Restore: Auto AD: Auto (No AD Integration/Dependency!)
<i>Backup Type (Size)</i>	WSB (Large) + Custom (Large) (AD Integrated?! -> ☹️)		Propriety (Small) + Non-AD-I



AD DR Plan - Options



	MSFT Default AD DR Plan - Manual (NO Automations) -	Customized AD DR Plan - SEMI Automated, a.k.a. D-I-Y -	Customized AD DR Plan - FULLY Automated -
<i>High Level Way Of Working</i>	Restore initial RWDC, clone, redeploy		Whatever you choose
<i>Security Assessment</i>	None or Separate		Integrated or Separate
<i>Skills Required</i>			
<i>Complexity DR Plan/Test</i>			
<i>Recovery Time Objective (RTO)</i>			

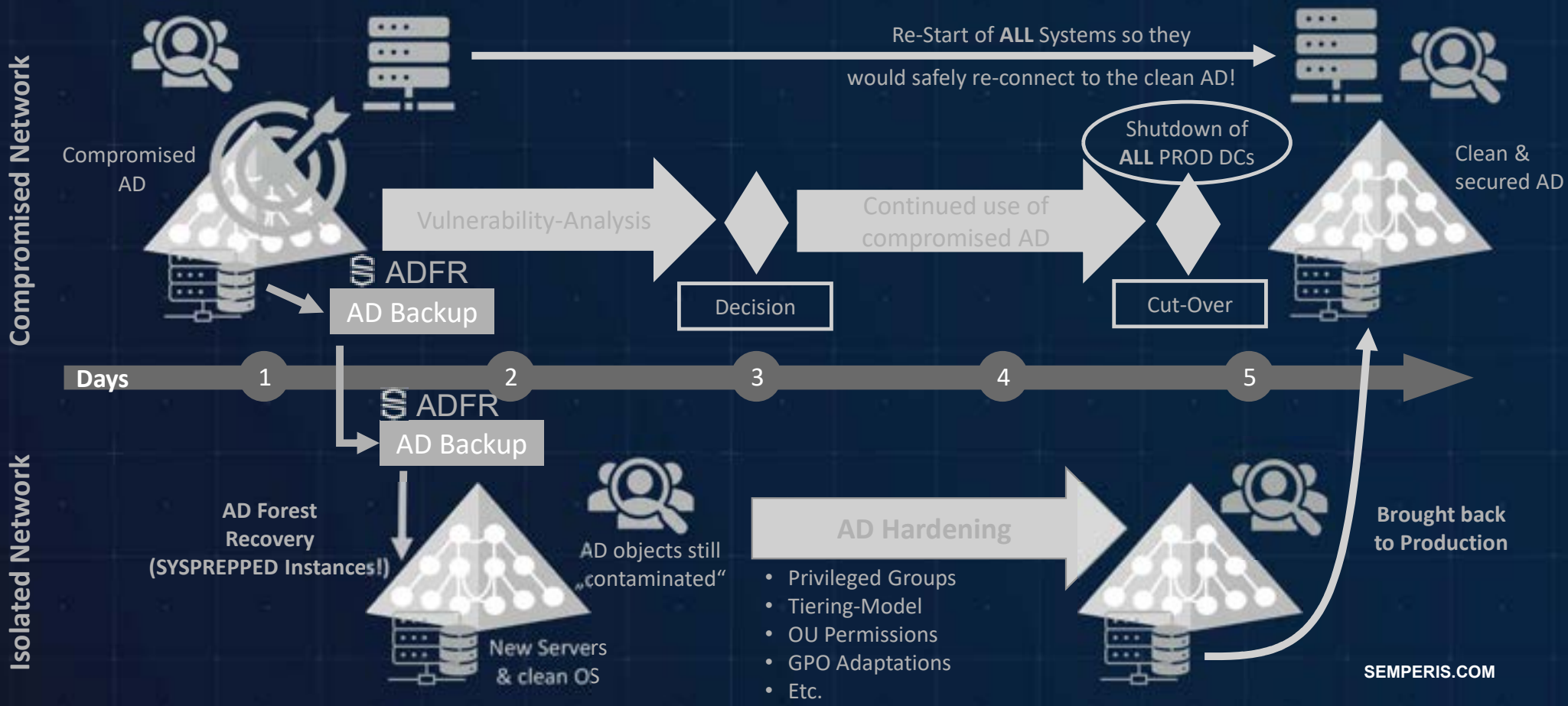
➤ Have you also thought about:

- Where to store your plan/code/tools?
- Credentials required during recovery?
- Dependency on AD, RE: authentication and authorization?
- Impact of recovery on Sync with AAD – Connect Sync or Cloud Sync
- Impact of recovery on AuthN method for AAD – Fed, PTA or PHS?

...AND So Much More!!!

Real Life AD Incident/Recovery Scenario

Real Life AD Incident/Recovery Scenario (1)



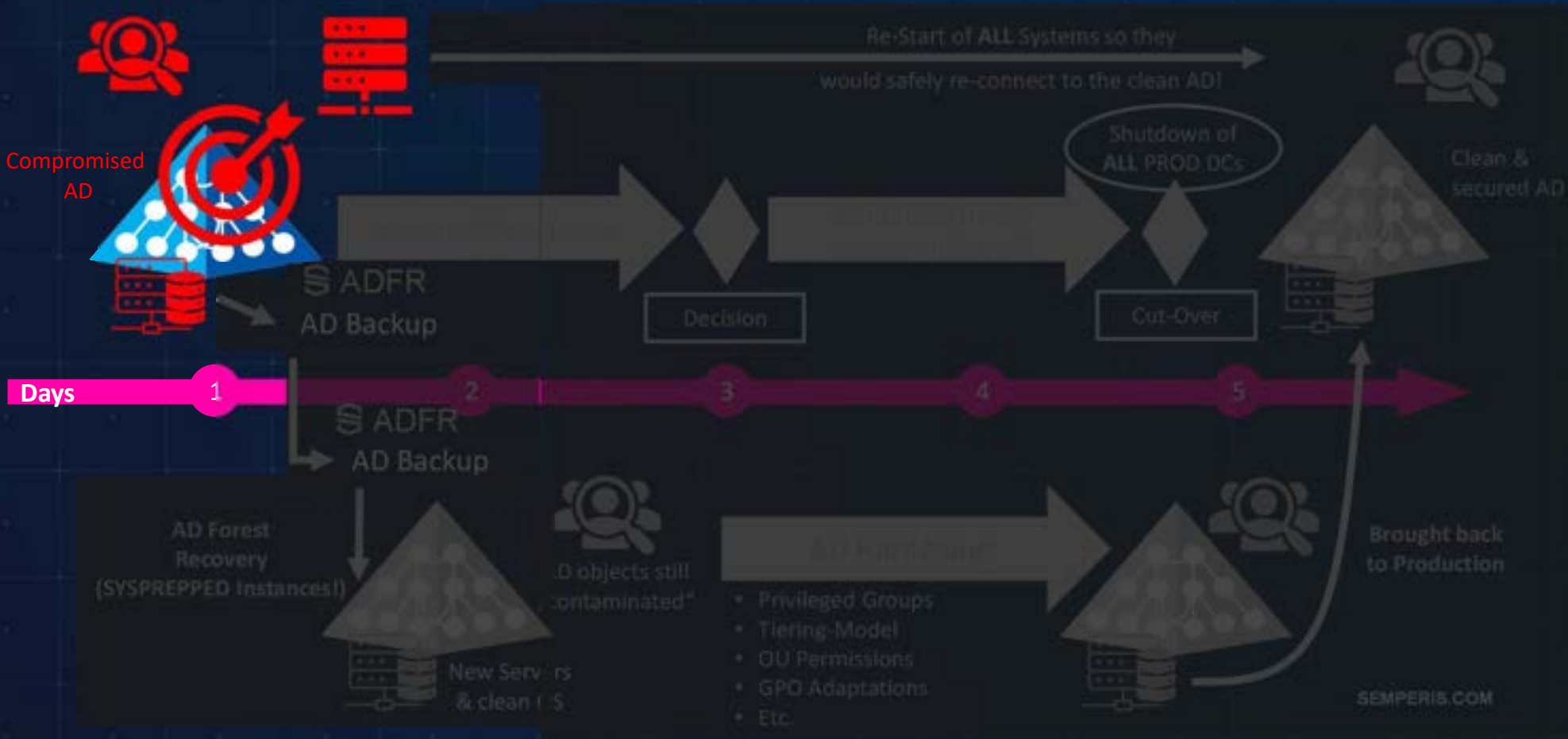
Real Life AD Incident/Recovery Scenario (1)

> *Oops, You've Been BREACHED !!!*



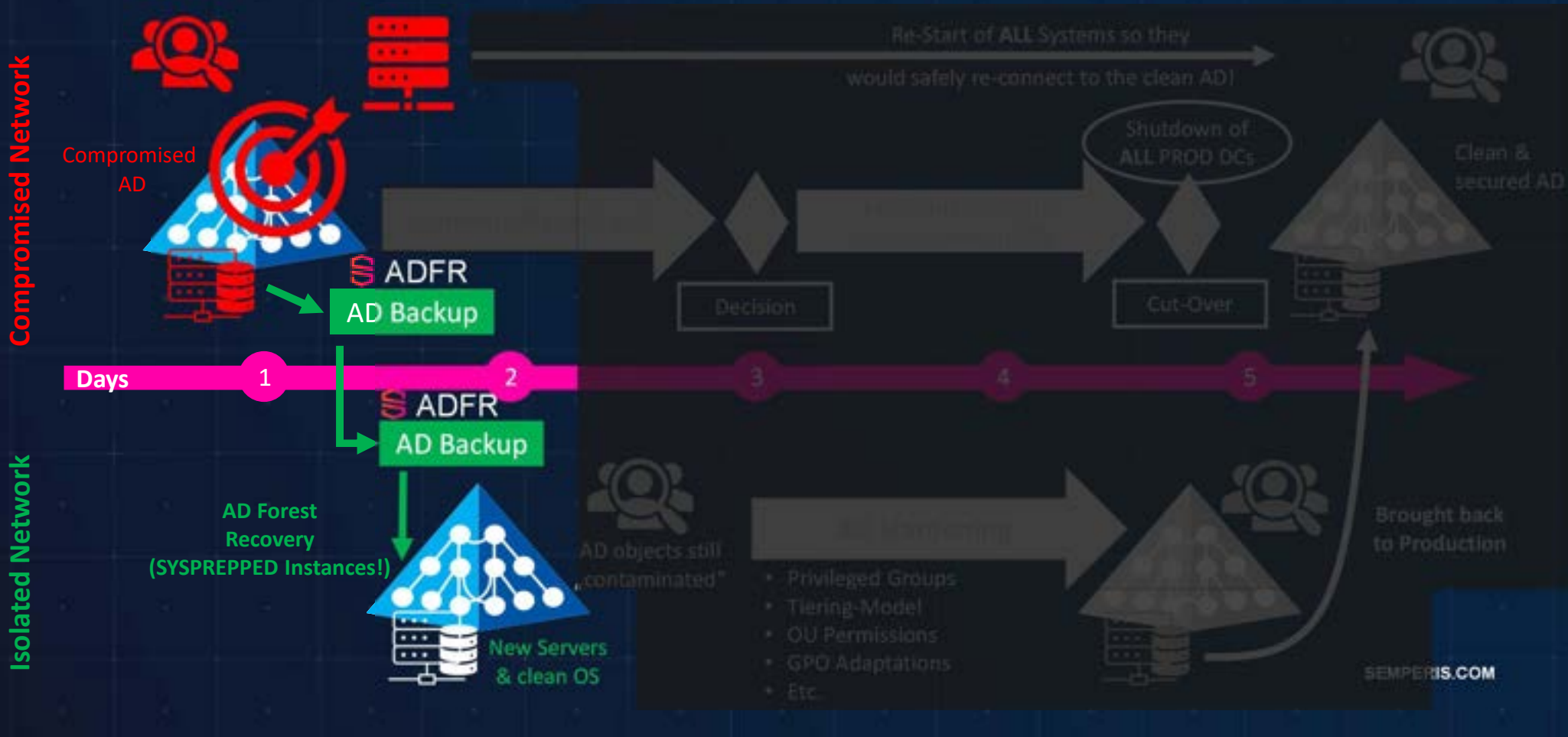
Compromised Network

Isolated Network



Real Life AD Incident/Recovery Scenario (1)

> PHASE I - SAFETY NET For AD



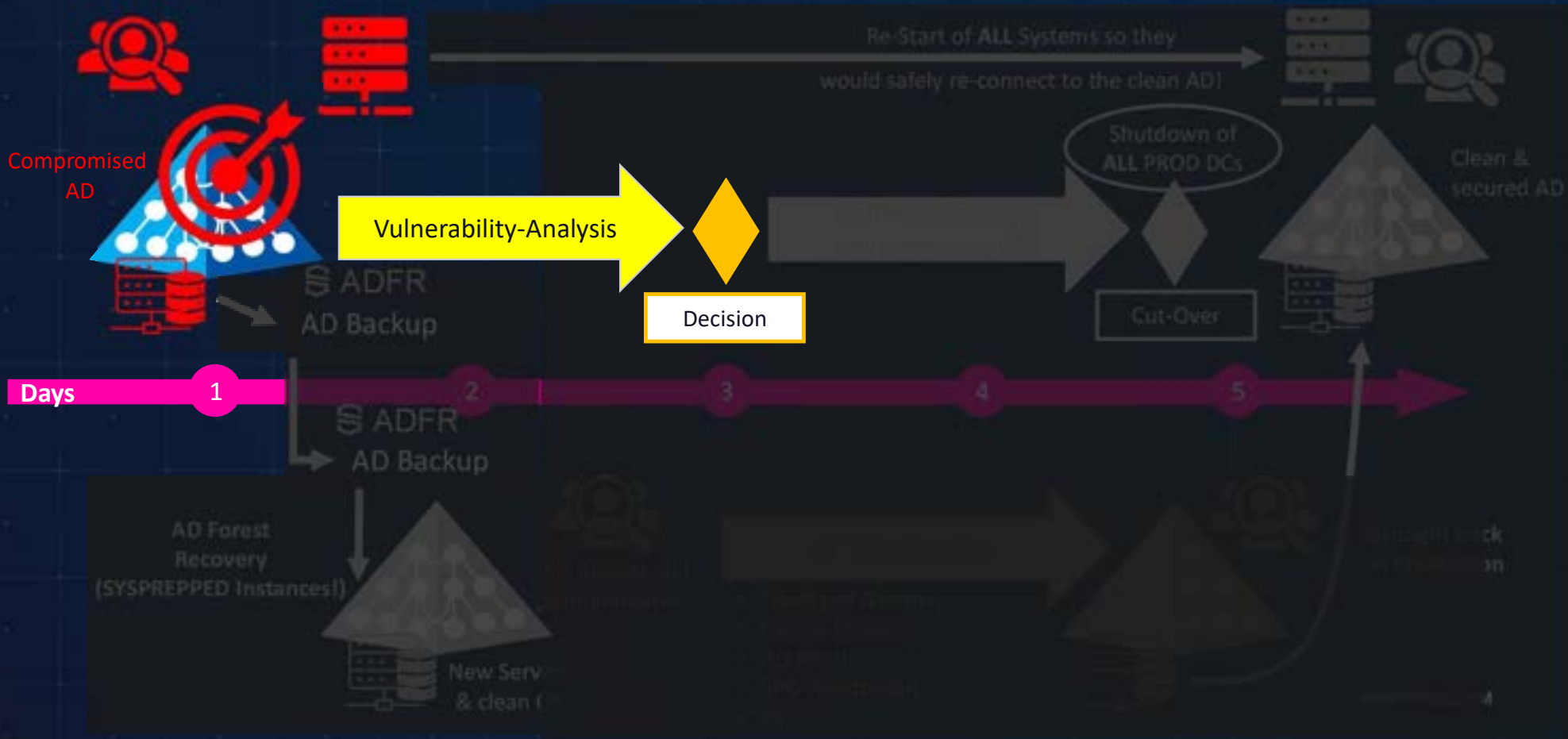
Real Life AD Incident/Recovery Scenario (1)

> PHASE II – AD Vulnerability Analysis



Compromised Network

Isolated Network



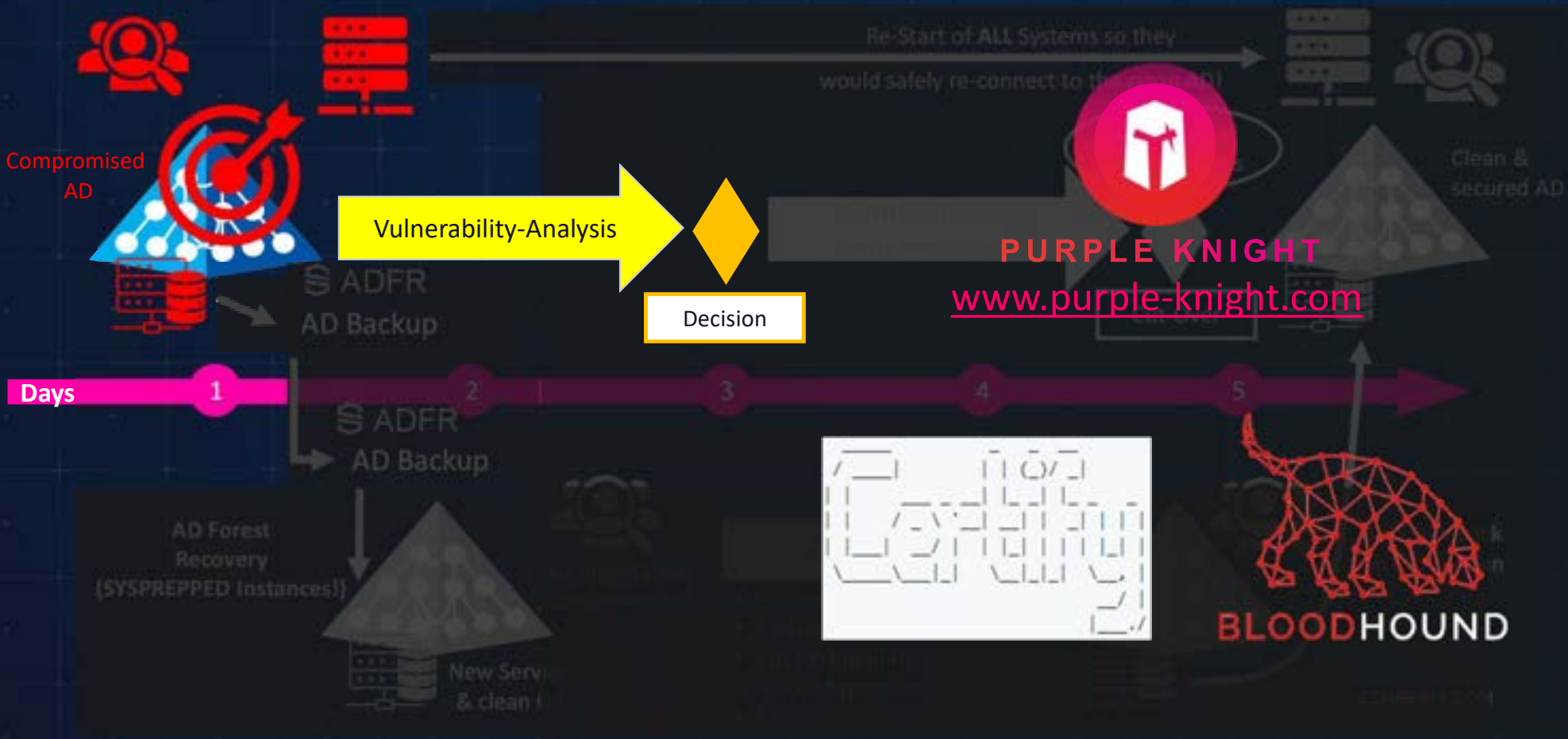
Real Life AD Incident/Recovery Scenario (1)

> PHASE II – AD Vulnerability Analysis



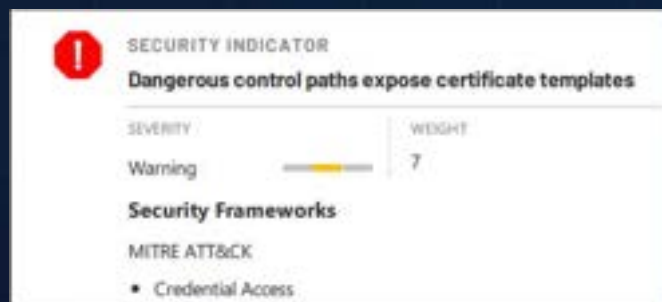
Compromised Network

Isolated Network

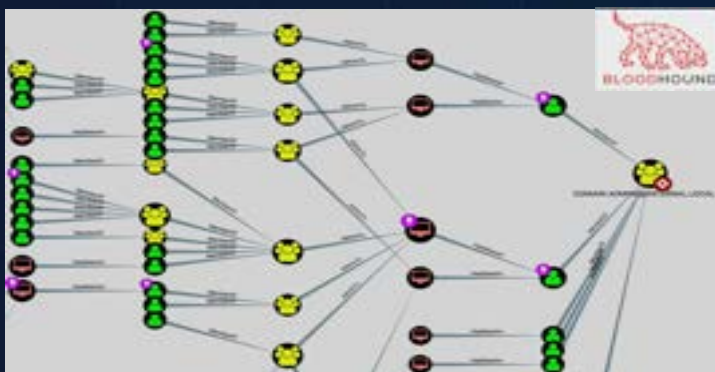


Real Life AD Incident/Recovery Scenario (1)

> Dubious Permissions & >1 Attackers



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!

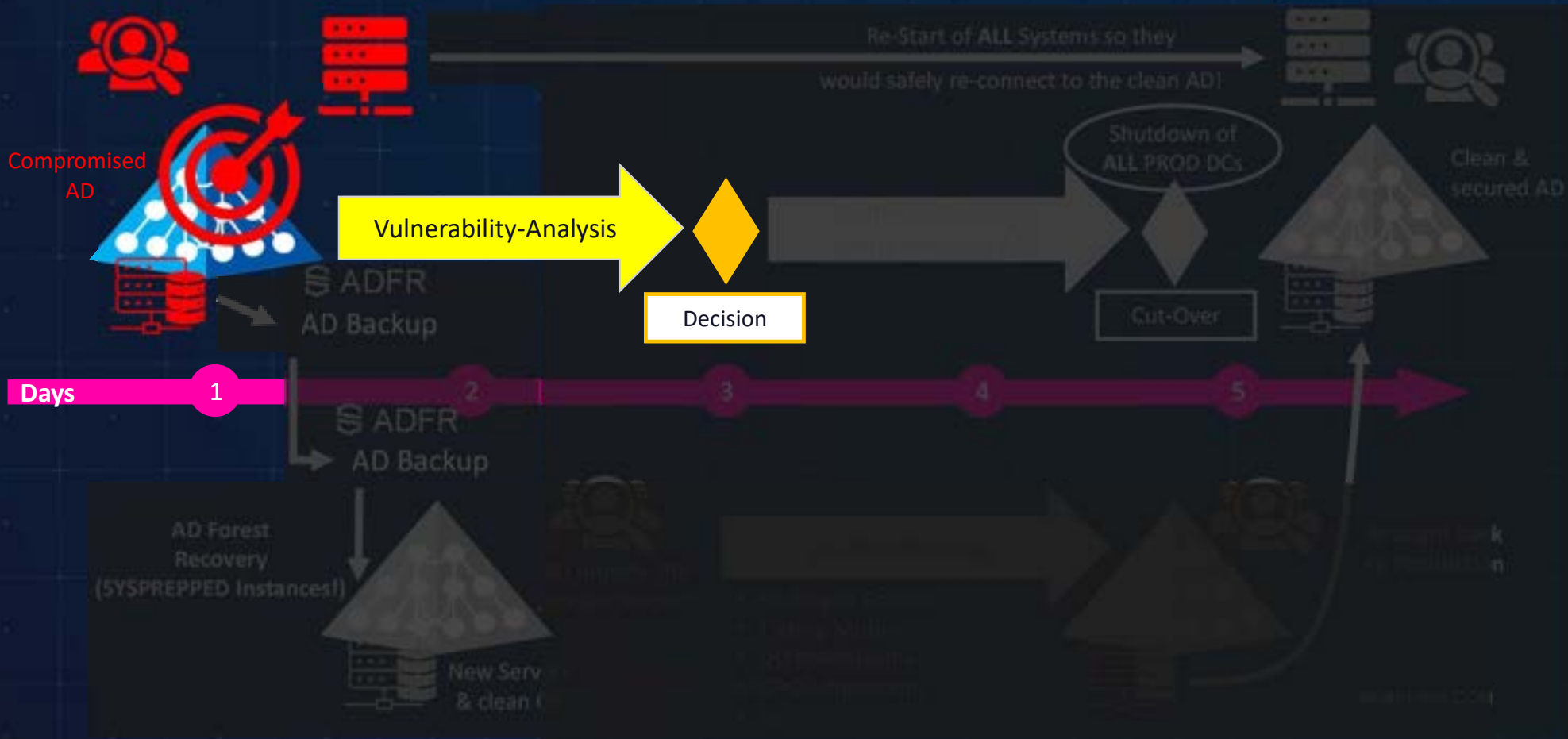
Real Life AD Incident/Recovery Scenario (1)

> PHASE II – AD Vulnerability Analysis



Compromised Network

Isolated Network



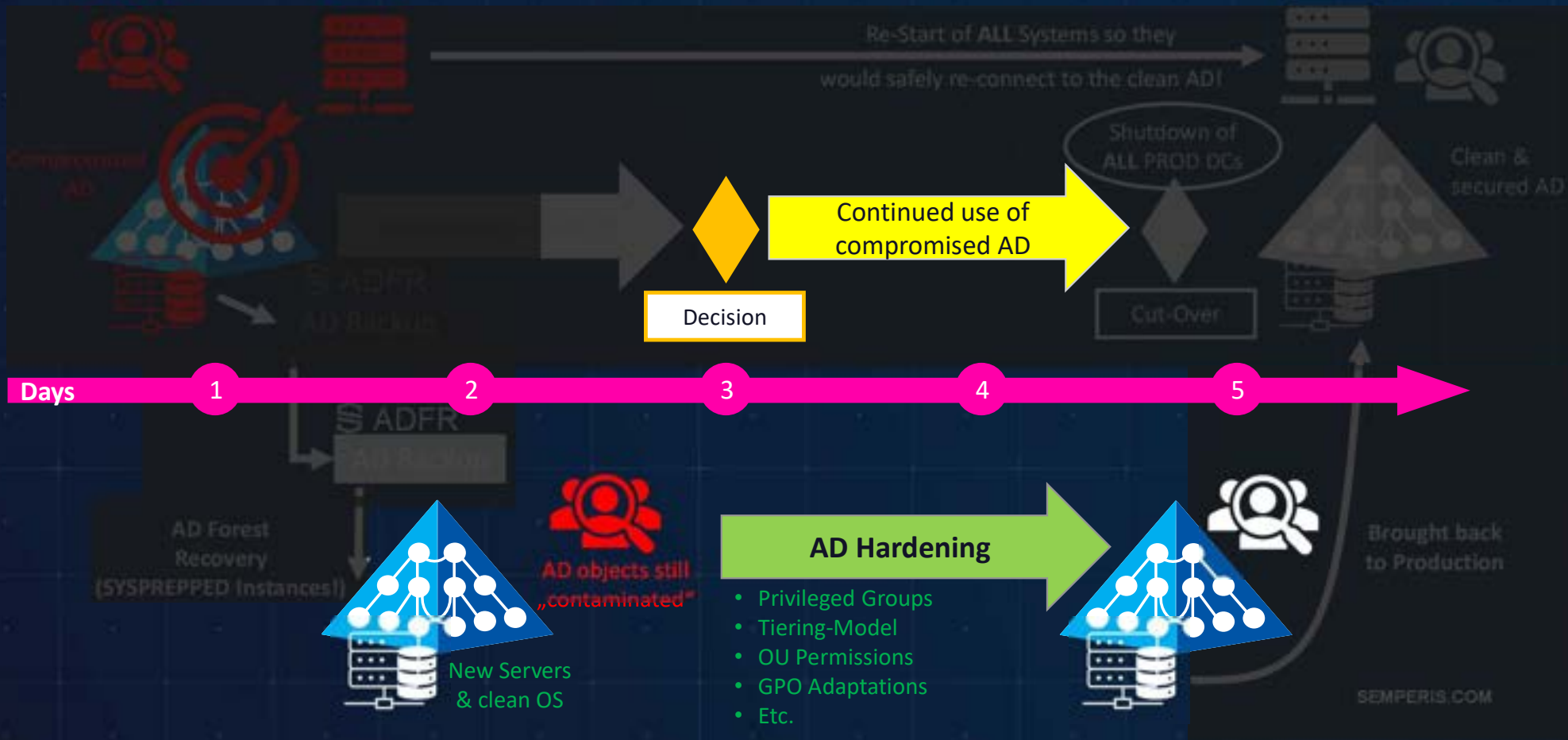
Real Life AD Incident/Recovery Scenario (1)

> PHASE III - Divide And Conquer!



Compromised Network

Isolated Network

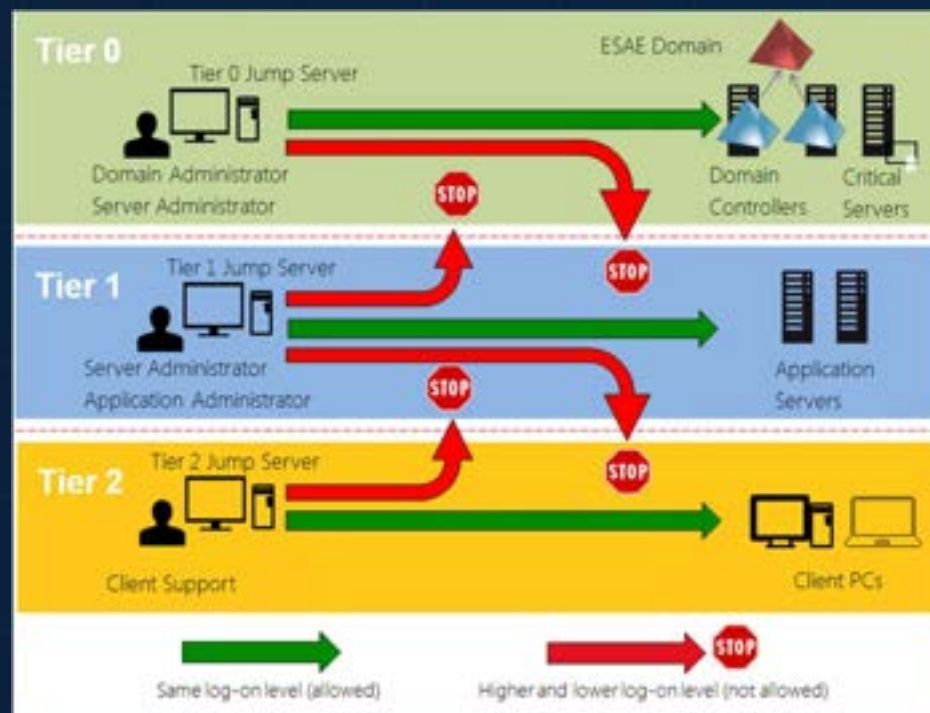


Real Life AD Incident/Recovery Scenario (1)

> AD Hardening Speedway...



- 1.5 days available to harden AD
 - Tiering-Model (w/o MFA)
 - Cleaned up Privileged Groups
 - NEW accounts in Privileged Groups
 - Protected Users group
 - No Privileged Accounts with SPNs
 - OU/AdminSDHolder Permissions
 - GPO Adaptations
 - ...



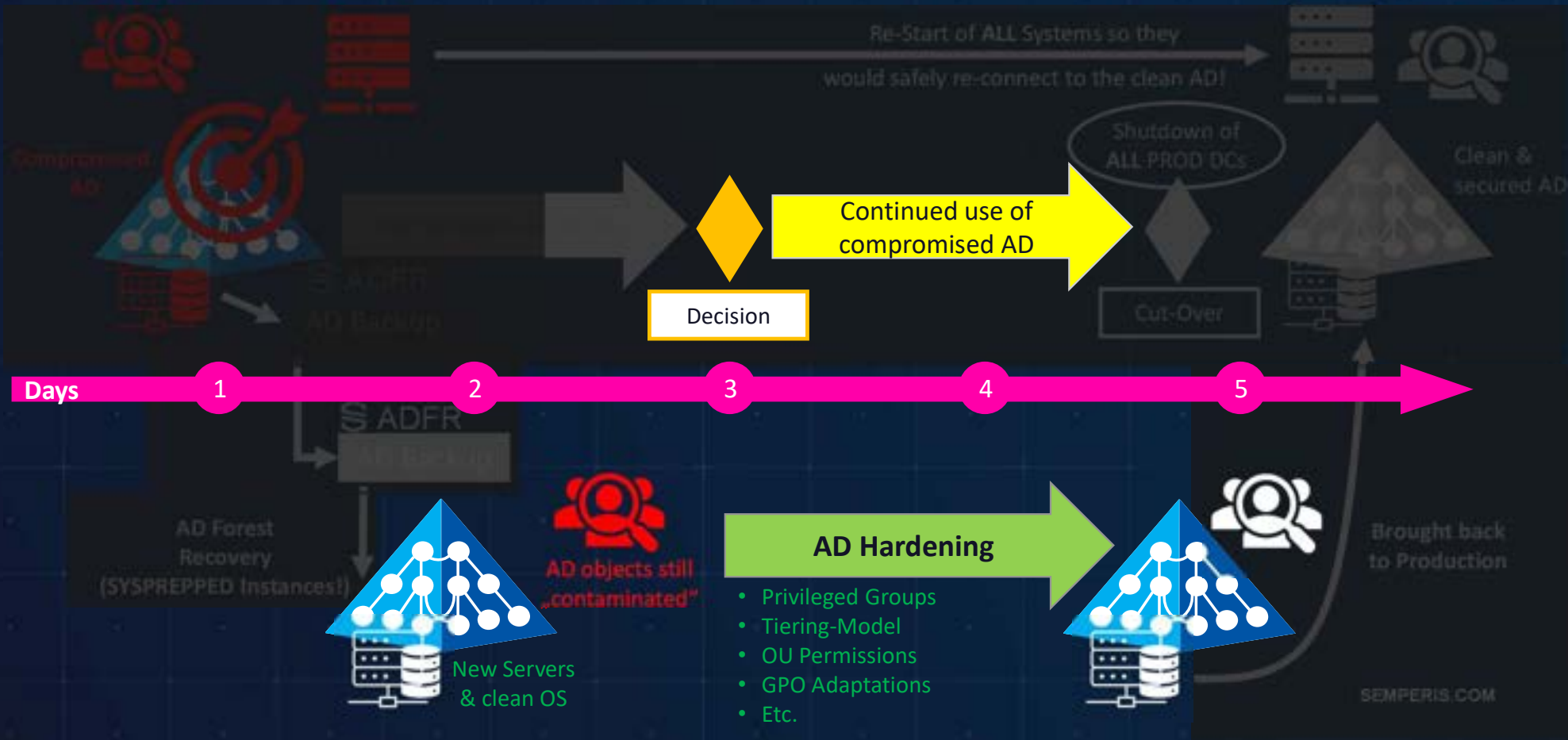
Real Life AD Incident/Recovery Scenario (1)

> PHASE III - Divide And Conquer!



Compromised Network

Isolated Network



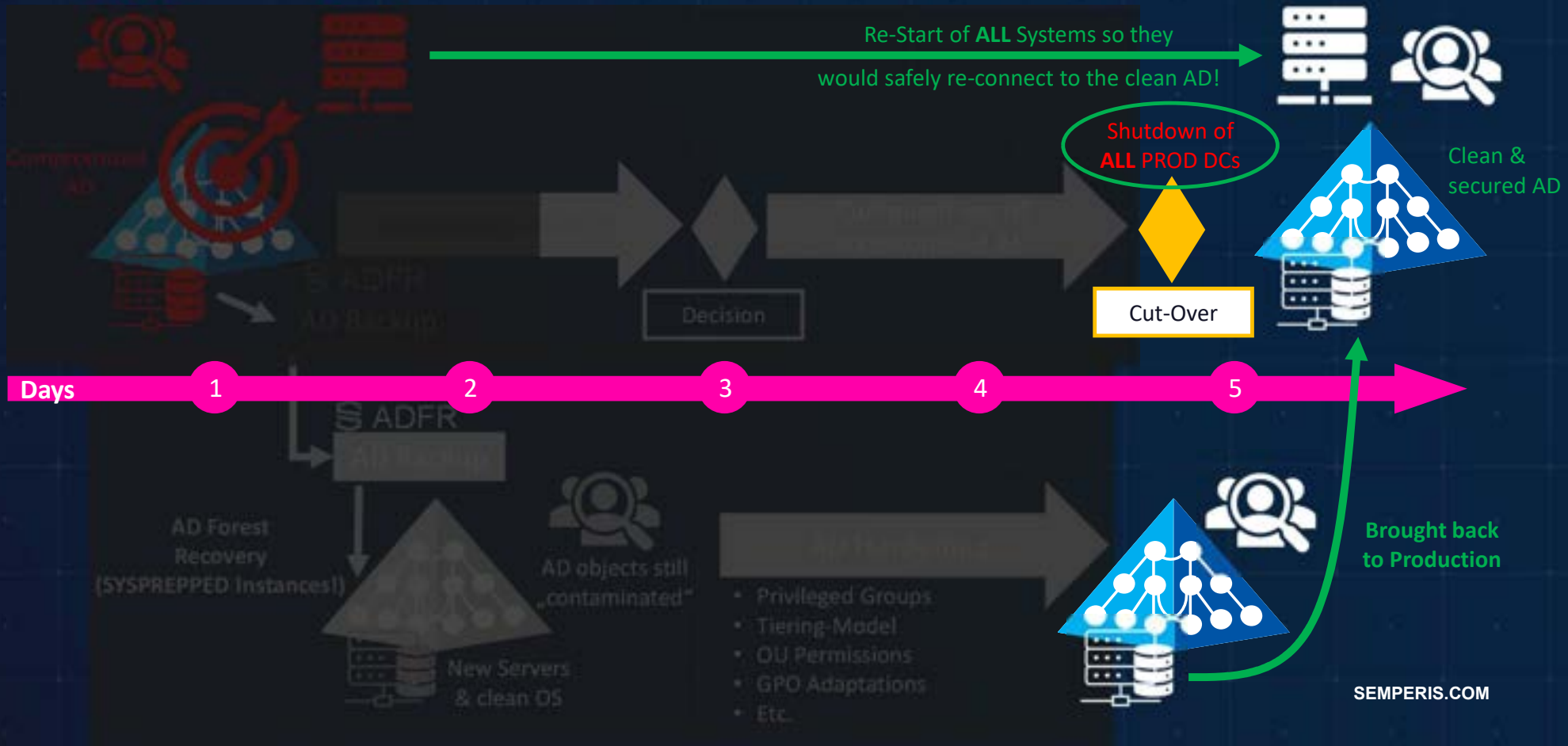
Real Life AD Incident/Recovery Scenario (1)

> PHASE IV - Hardened AD Back To Production



Compromised Network

Isolated Network



Real Life AD Incident/Recovery Scenario (1)

> *This Experience Felt Like...*



SEMPERIS.COM

SOURCE: Saudi's Again Changing Wheels Tyres while driving!

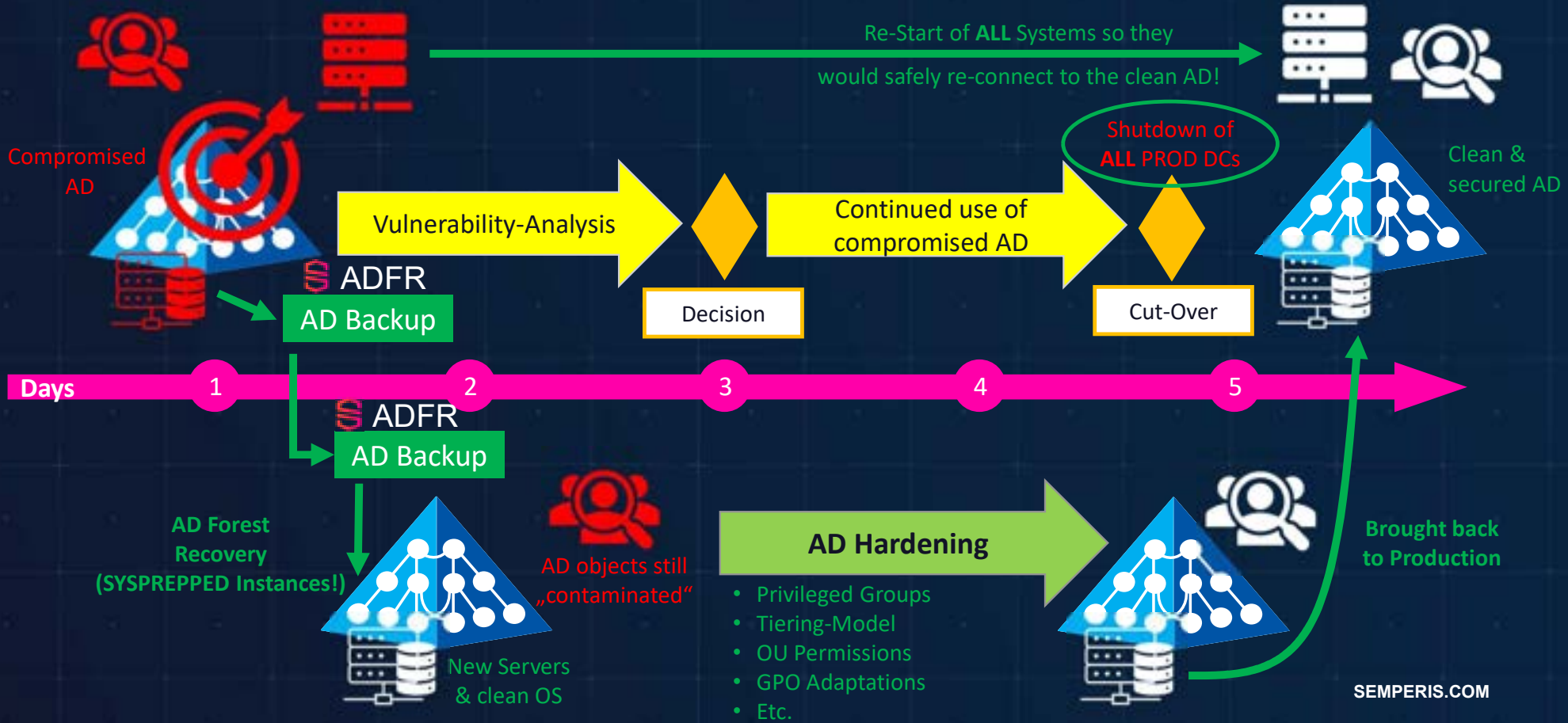
Real Life AD Incident/Recovery Scenario (1)

> *In The End – They Survived!* 😊



Compromised Network

Isolated Network



Take Aways!

Take Aways!



➤ Please INVEST in:

➤ **PRO**actively securing your environment with (TDR) tools

- ...for both on-prem AD, Azure AD and other clouds
- ...that assess security posture and monitor real-time
- ...that support preventive and detective controls
- ...that incorporate guidance e.g.: MITRE ATT&CK, ANSSI, etc.

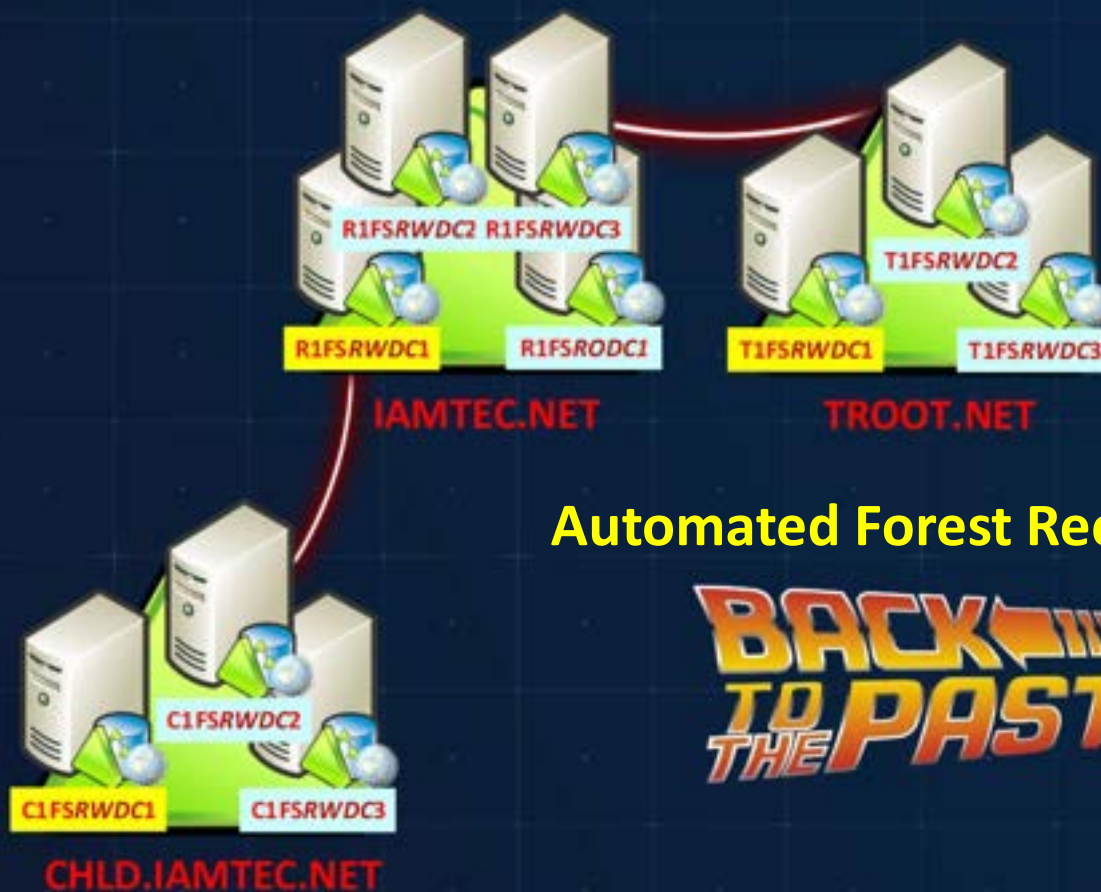
➤ **RE**actively being able to recover (DR Plan)

- Prepare for the unexpected: new zero-day exploits against AD will be discovered from time 2 time
- Although tech-focused, in the end, it is about your business!
- Logistics, communications and technology and more

Take Aways!

- SEEK HELP if needed, BEFORE the attack/breach
- AUTOMATE as much as possible
 - AD recovery is more than restoring single/multiple DCs
 - Consider 3rd party tool (= BEST Insurance, Fastest RTO!)
- Have Quality Assurance Check on DR plan!
 - It is NOT just about recovery; it needs to be secure too!
 - Perform periodic DR drills

Demo! – Automated Recovery, While Presenting



Questions? – Get In Touch!



ANY
QUESTIONS
?

Thank You!

Jorge de Almeida Pinto

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