semperis

Resurrecting After A Ransomware Attack

Be Secure(d), And Prepared!

Jorge de Almeida Pinto

Senior Solutions Architect | Senior Incident Response Lead

Introducing Me, Myself & I!

Microsoft MVP Most Valuable Professional

semperis

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

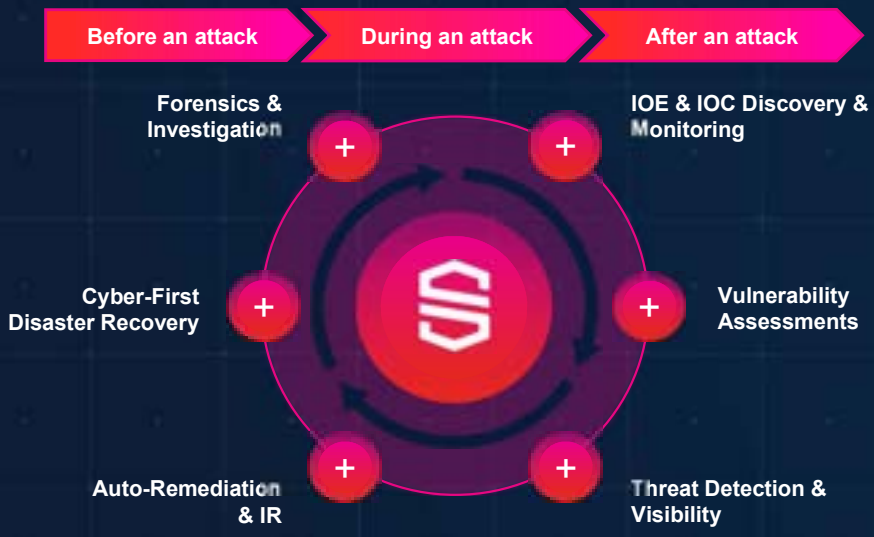
- Architecting, designing, implementing and maintaining secure identity solutions
- Technology Focus: Identity, Security And Recovery
- Product Focus: AD, ADFS, AAD Connect, FIM/MIM, Azure AD Technologies.

Introducing Semperis

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



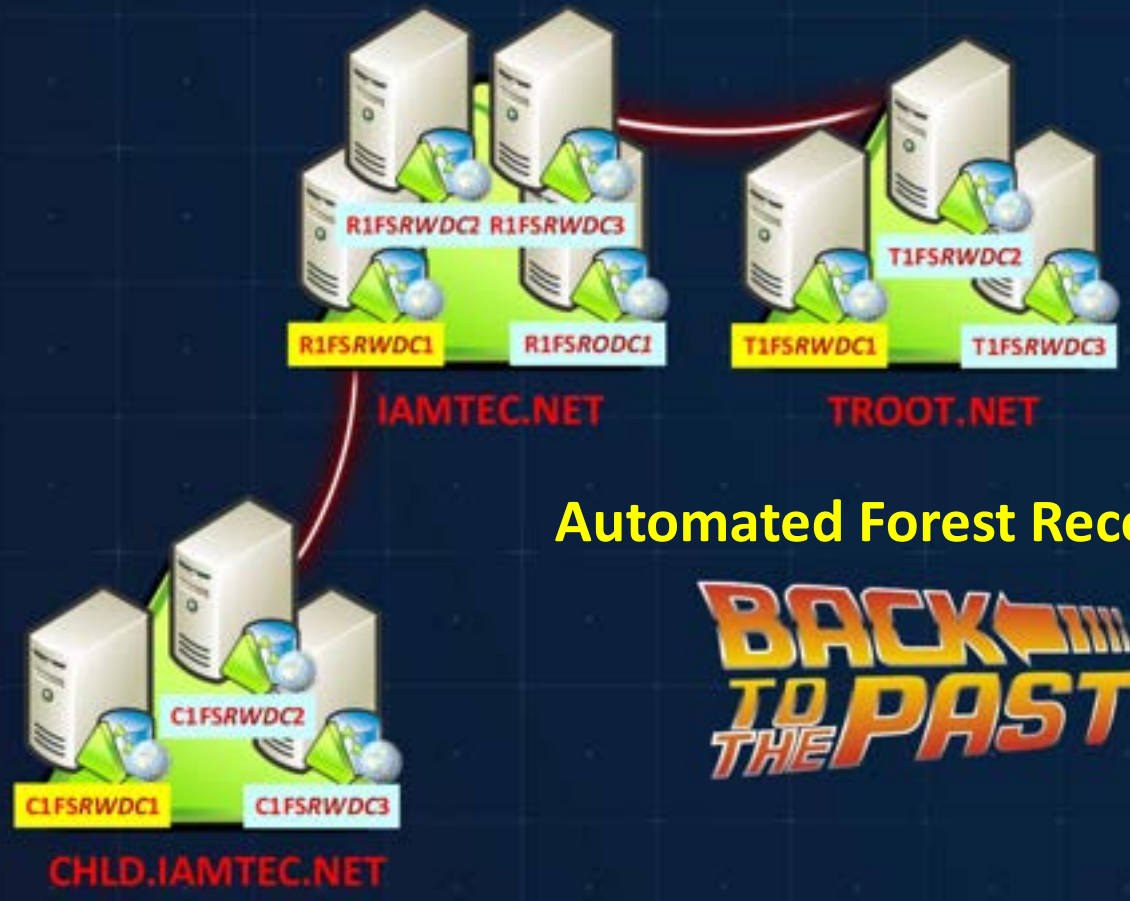
SEMPERIS.COM

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

semperis



Automated Forest Recovery

BACK TO THE PAST

Securing & Protecting AD

Securing And Protecting AD

semperis

- 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

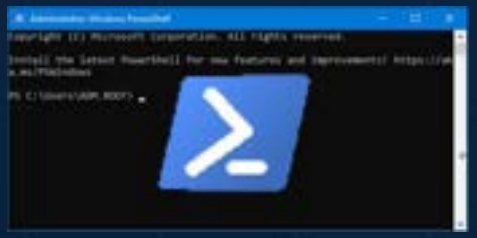
Reading: Defenders Think in Lists. Attackers Think in Graphs
Video: Defenders Think in Lists. Attackers Think in Graphs

++++++++++ 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

semperis

Detection Response (TDR) Tools!



- Do-It-Yourself in PowerShell

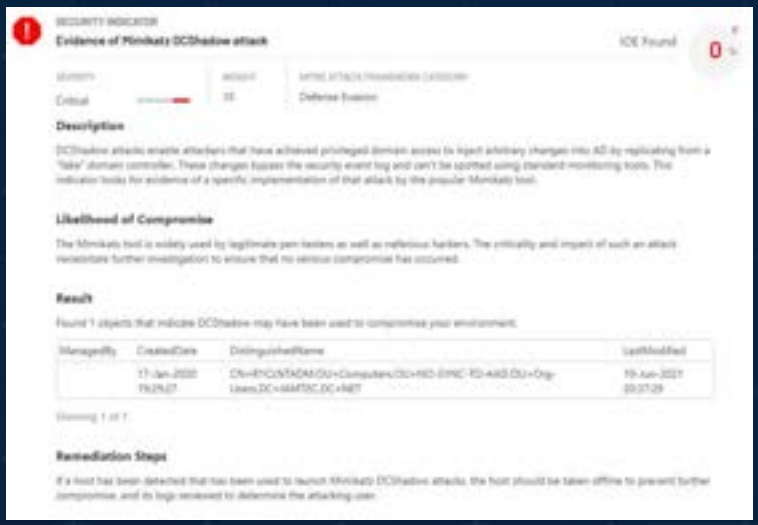
Securing And Protecting AD

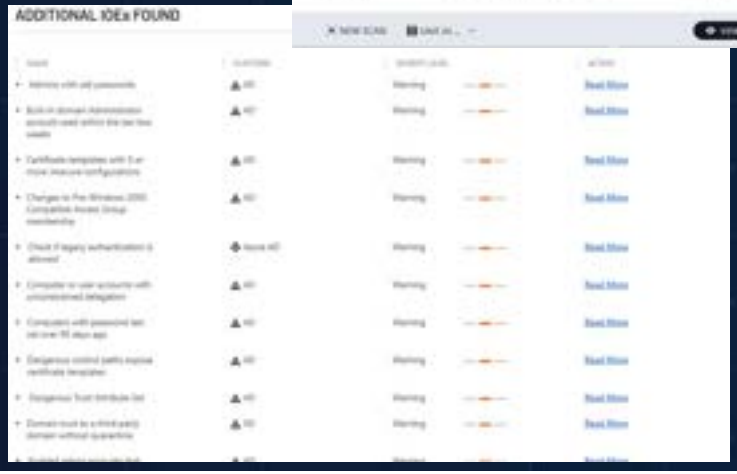
semperis

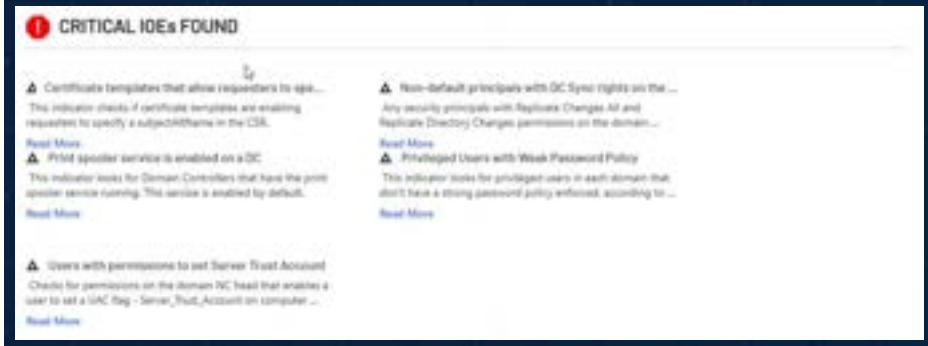
➢How? - You ask? – Threat Detection Response (TDR) Tools!

PURPLE KNIGHT

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







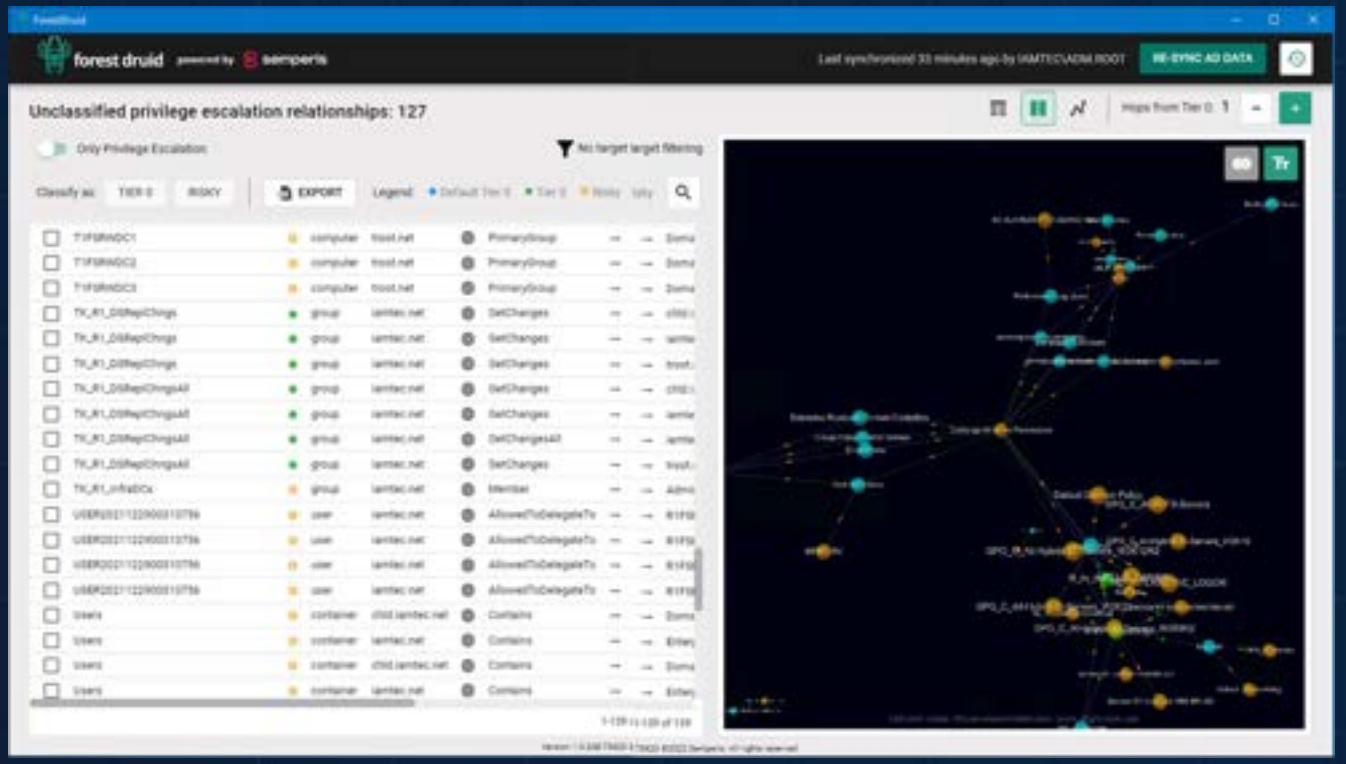
Securing And Protecting AD

semperis

➢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!**)



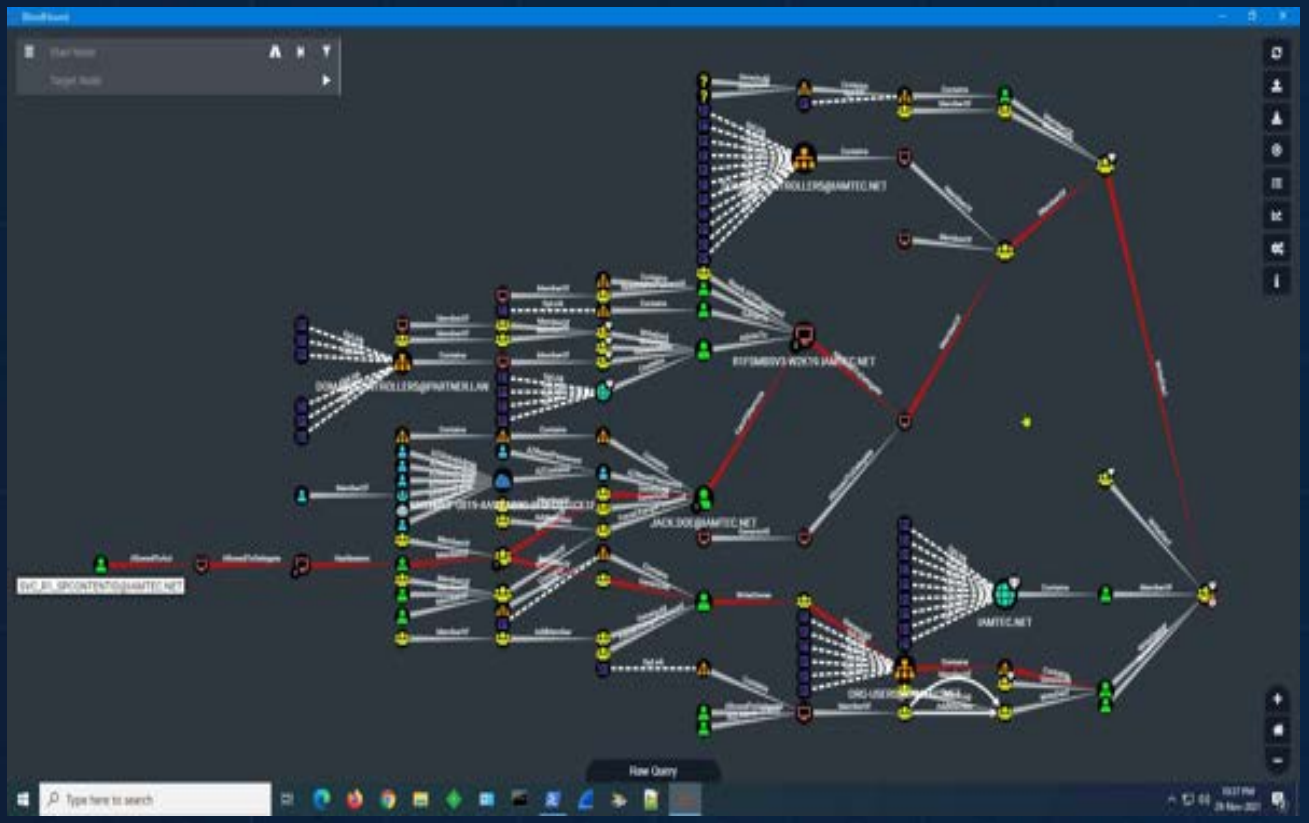
Securing And Protecting AD

semperis

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

BLOODHOUND

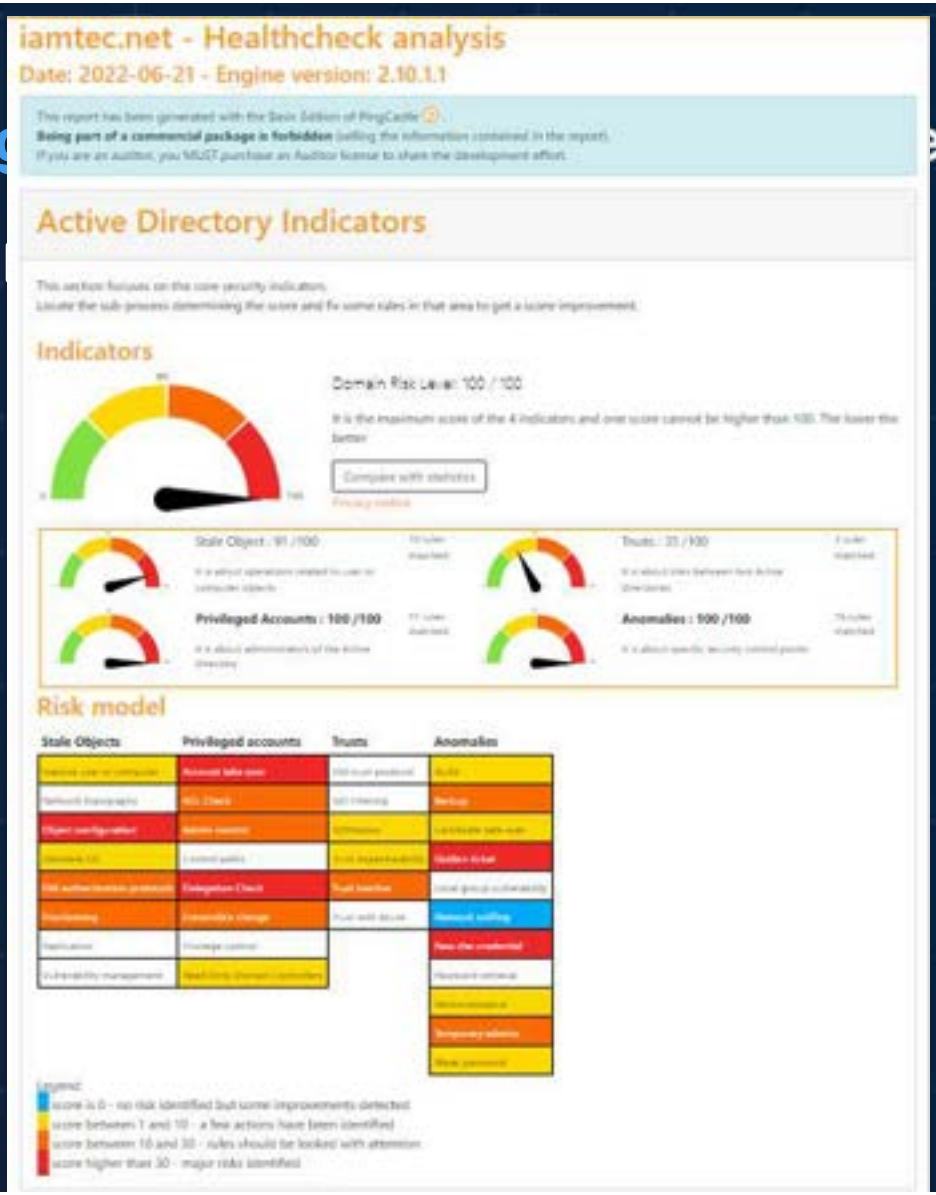
- Extraction of AD data through “SharpHound” command-line tool
- Imported/Processed by BloodHound UI-tool to visualize attack-path(s) (**OUTSIDE-IN**)



Securing And Protecting

emperis

➢How? - You ask? – Threat



PING CASTLE

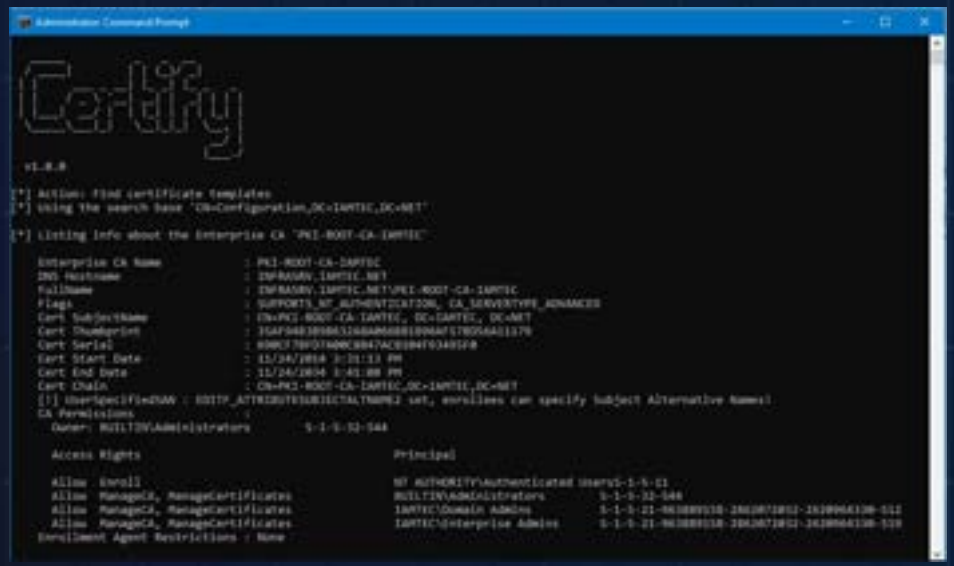
- Command-Line tool for evaluation security posture of an AD domain

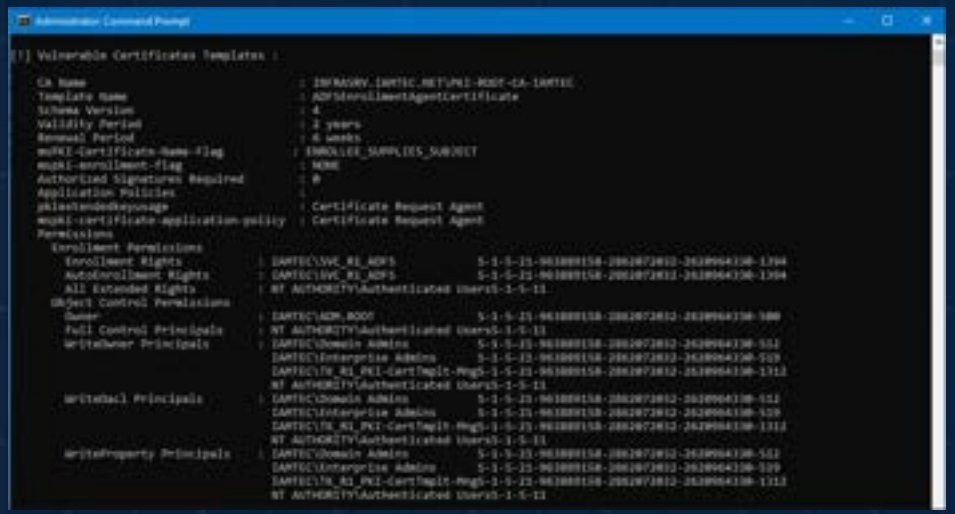
Securing And Protecting AD

semperis

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

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



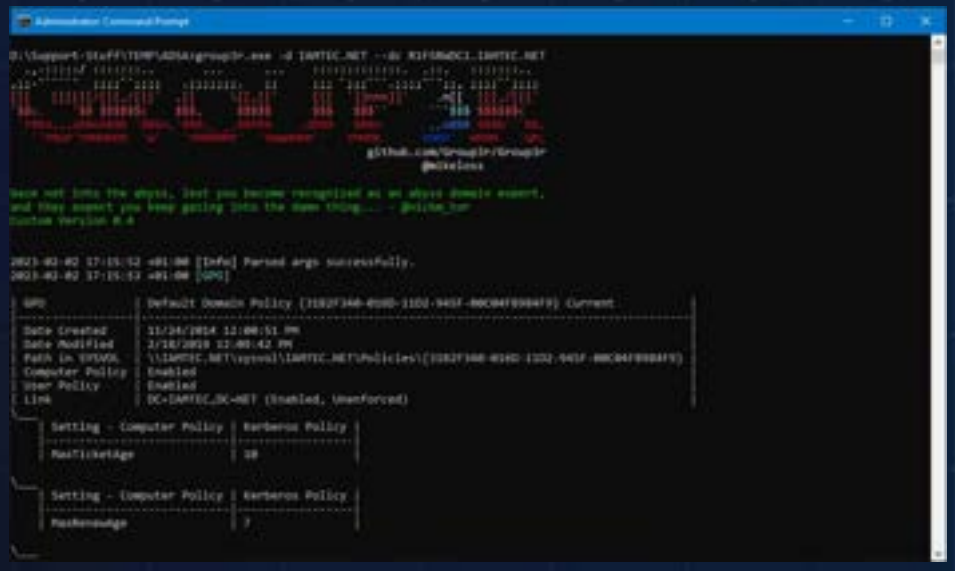


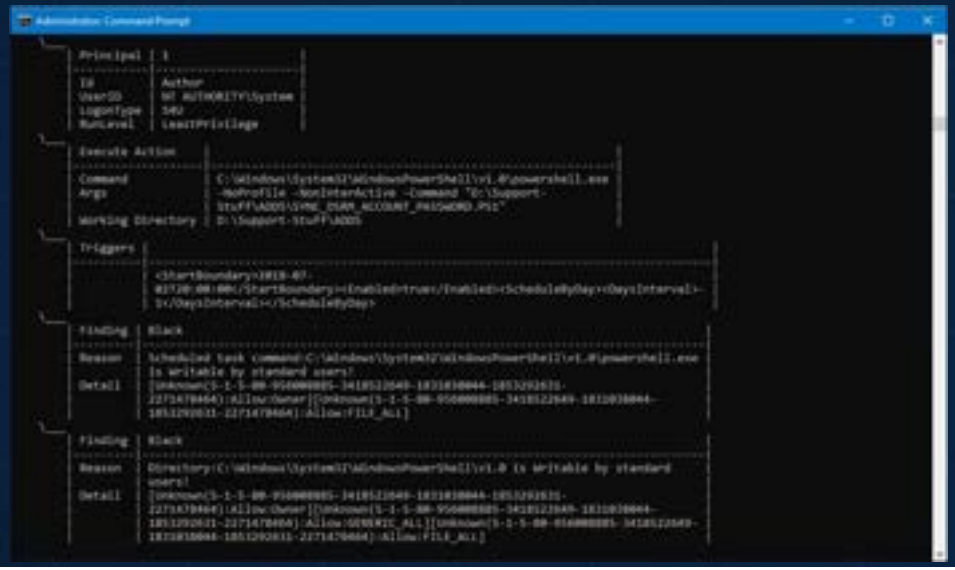
Securing And Protecting AD

semperis

➢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?

semperis

- 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

SEMPERIS.COM

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

AD DR Plan - Why?

- Business Reasoning

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

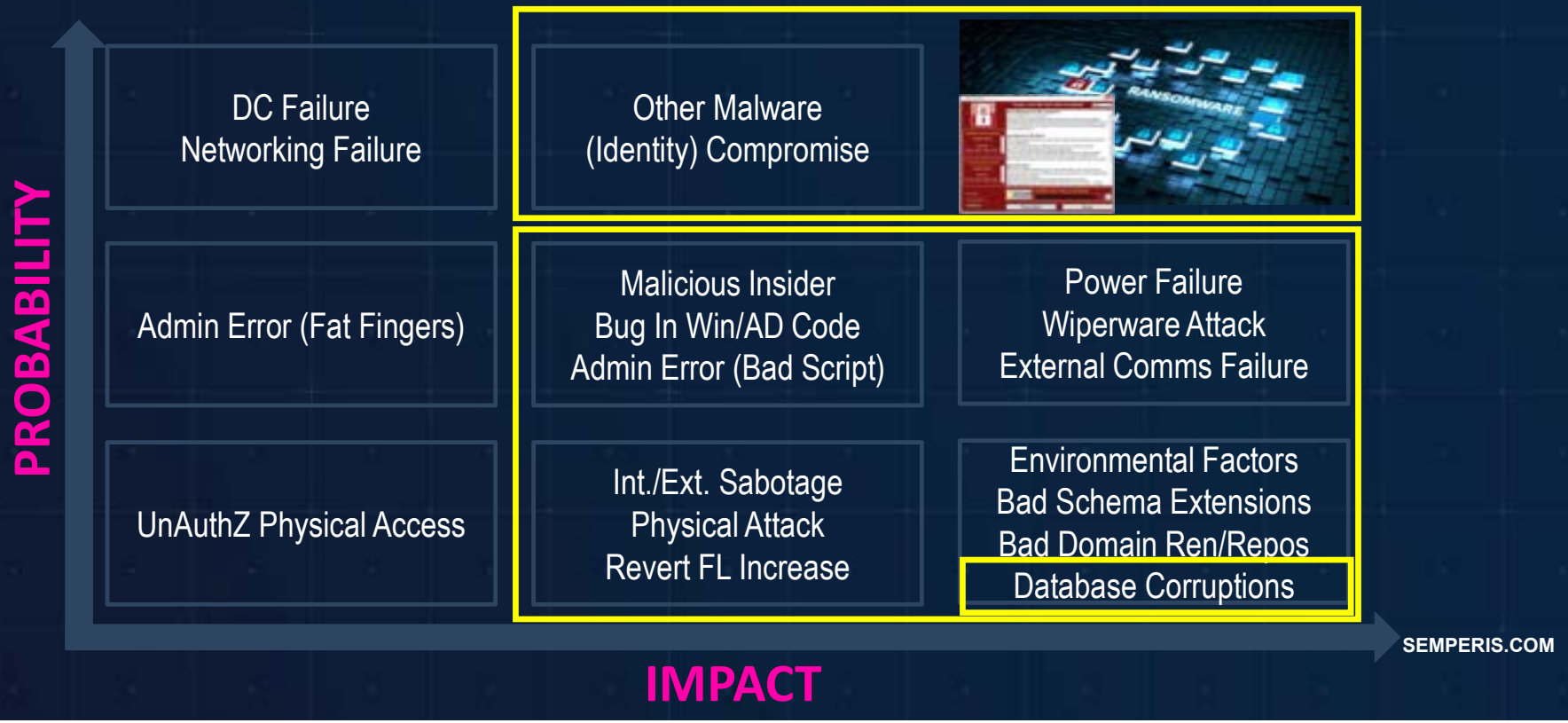
  - Complexity:
    - May look simple, difficult in practice!
    - Reinstalling/recovering 1 DC is easy! Recovering many, in distributed environment? What about outsourcing?

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

AD DR Plan - Why?

semperis

- Business Reasoning
  - Probability/Impact of Scenarios



semperis

AD DR Plan - Options

AD DR Plan - Options

semperis

	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 =-
Focus	Core only, no dependencies	Comms, logistics, pre/post, core, dependencies	
Text/Tools	High/None	Medium/E.g. PowerShell	Low/Commercial tool (AD focused, ADFR)
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 (No AD Integration/Dependency!)
Backup Type (Size)	WSB (Large) + Custom (Large) (AD Integrated?! -> ☹)		Propriety (Small) + Non-AD-I

AD DR Plan - Options

semperis

	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 =-
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)			

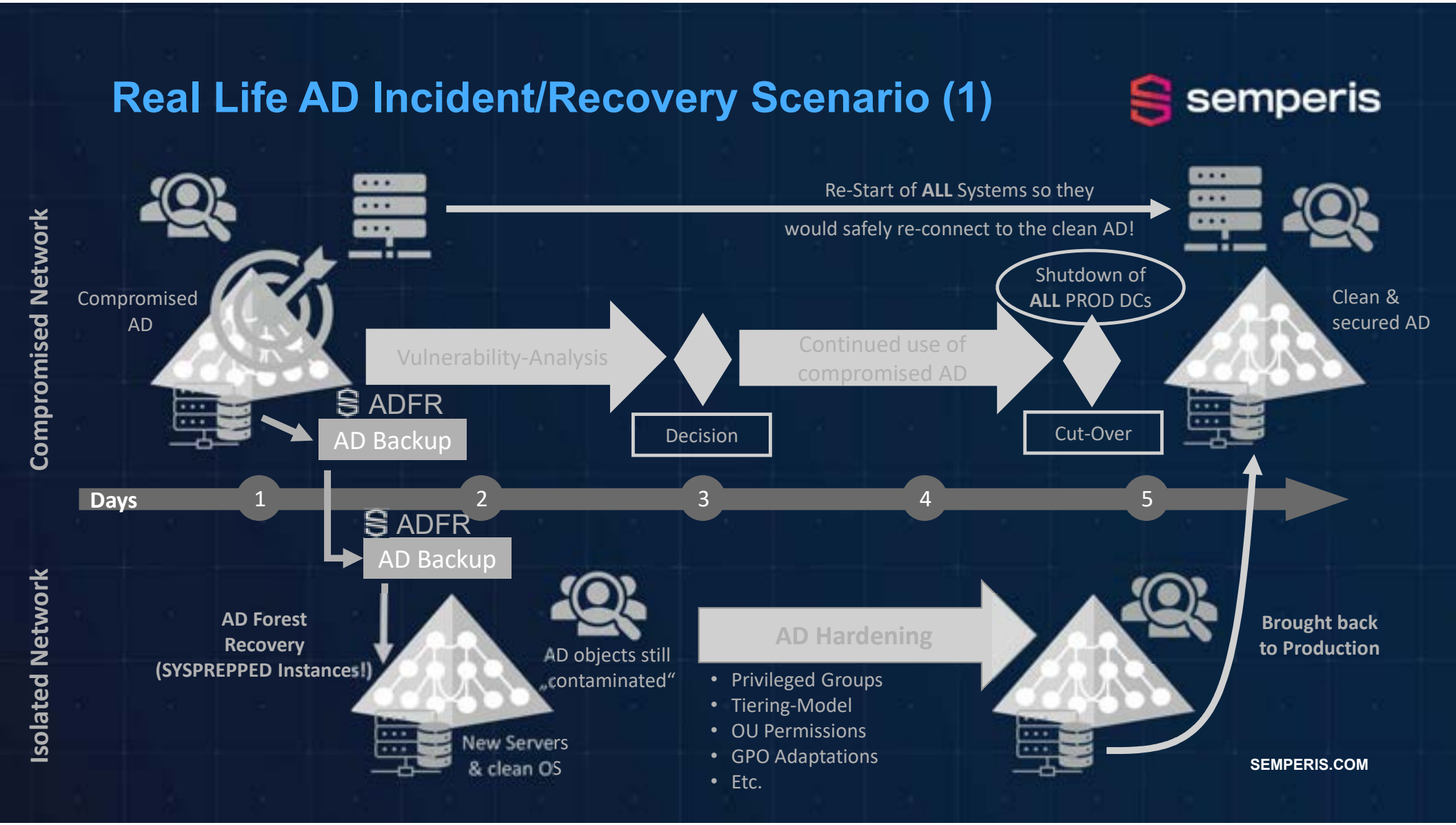
- Have you also thought about:
  - Where to store your plan/code/tools?
  - Credentials required during recovery?
  - Dependency on AD, RE: authentication and authorization?
  - Impact of recovery on Sync with AAD – Connect Sync or Cloud Sync
  - Impact of recovery on AuthN method for AAD – Fed, PTA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

...AND So Much More!!!

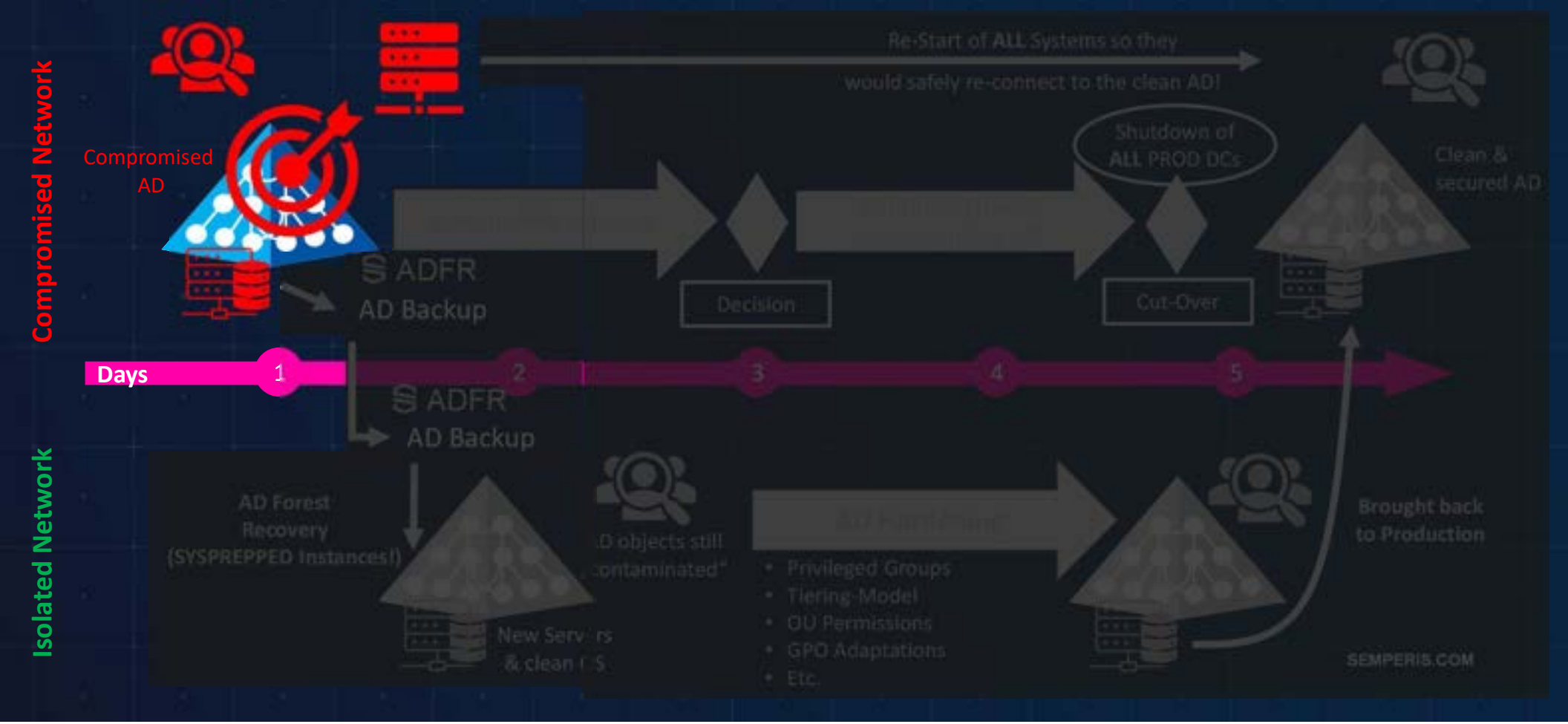
Real Life AD Incident/Recovery Scenario

Real Life AD Incident/Recovery Scenario (1)

semperis

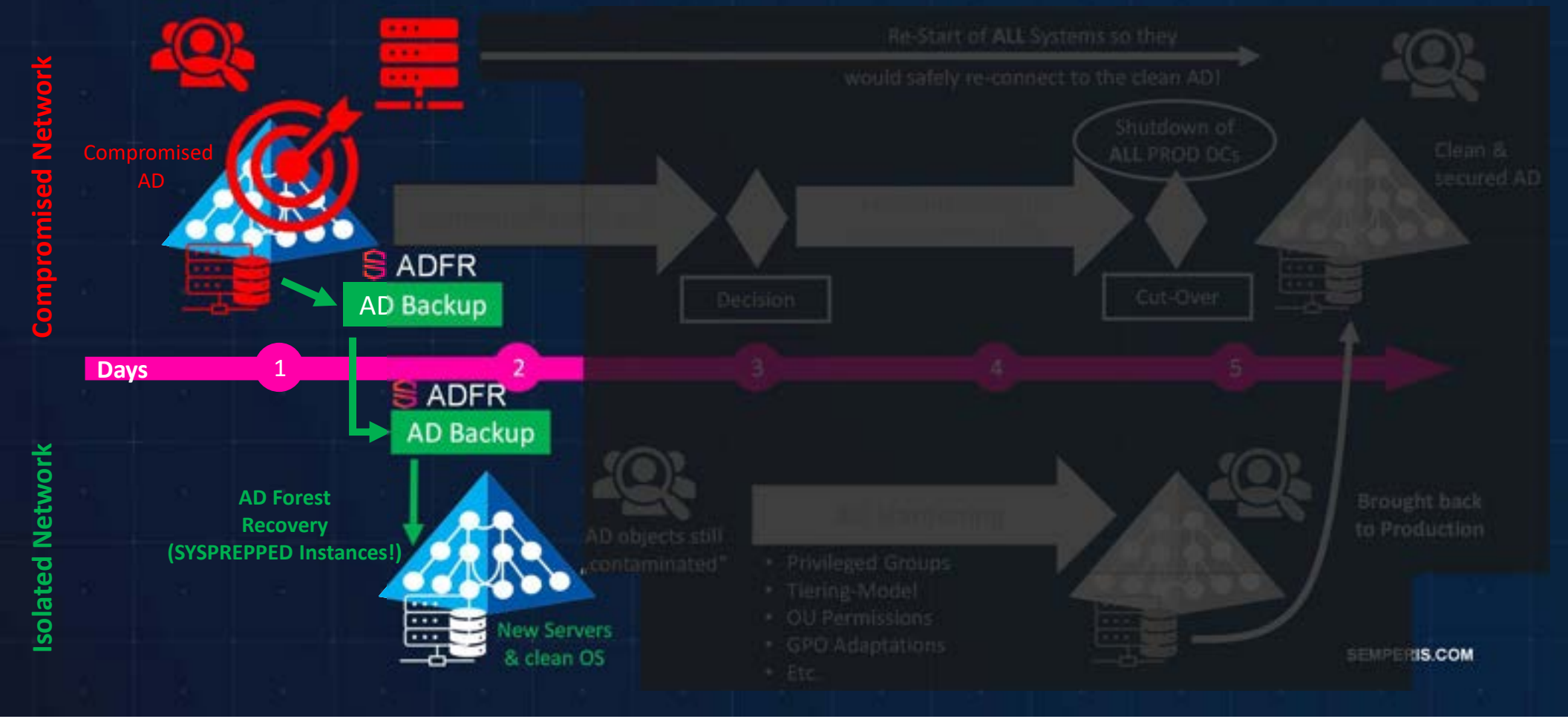


Real Life AD Incident/Recovery Scenario (1)
> *Oops, You've Been BREACHED !!!*

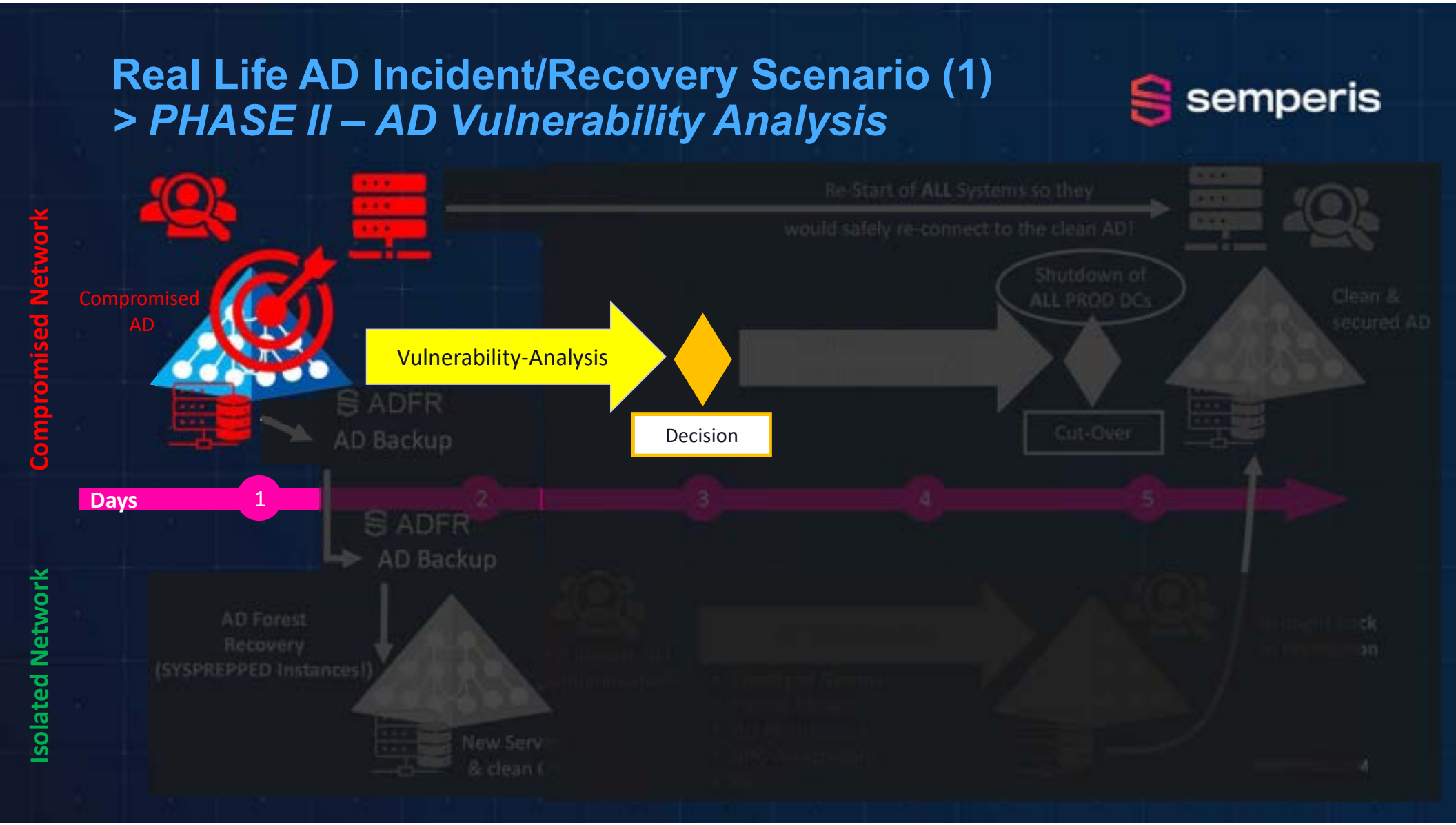


Real Life AD Incident/Recovery Scenario (1)
> *PHASE I - SAFETY NET For AD*

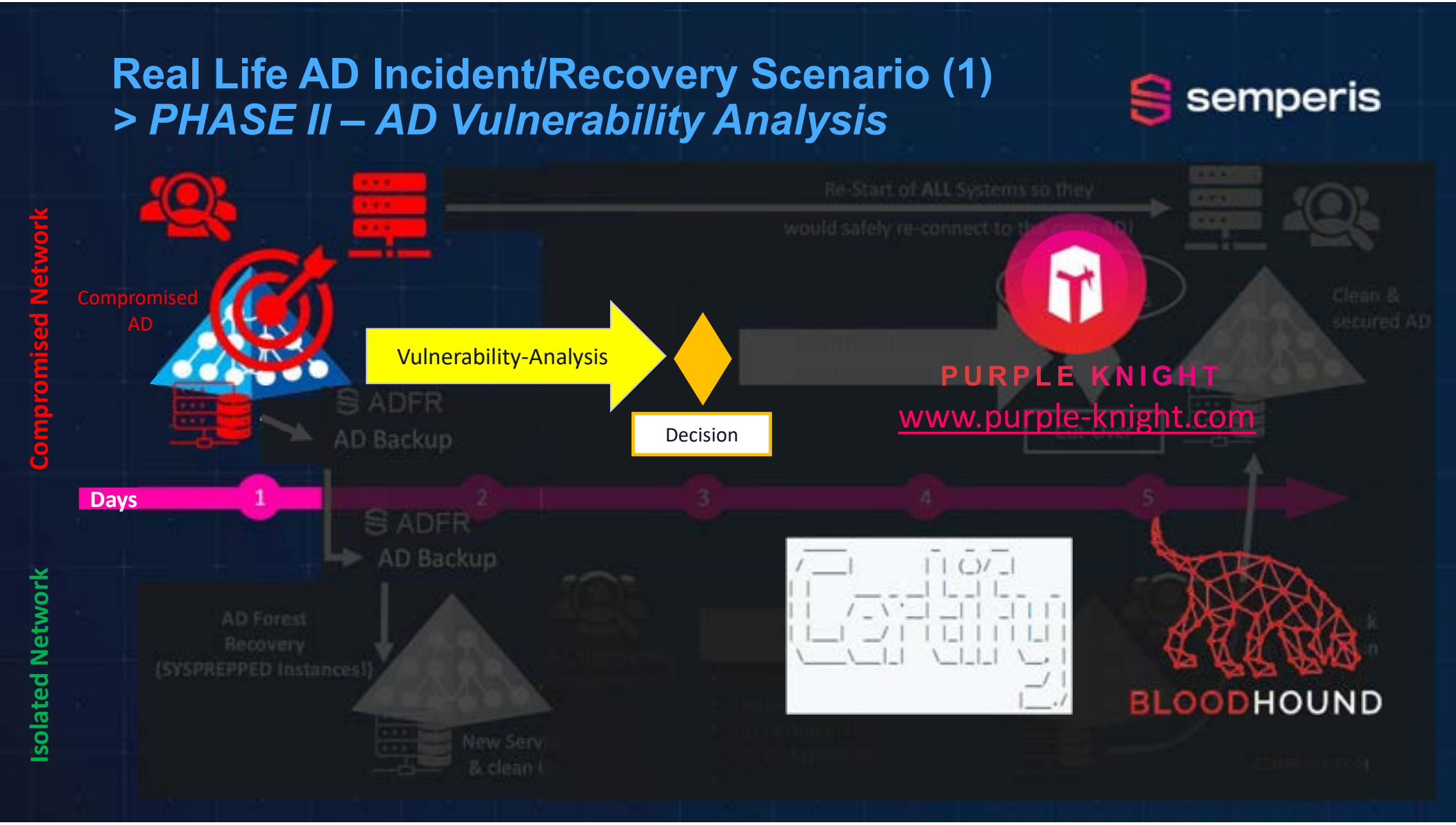
semperis



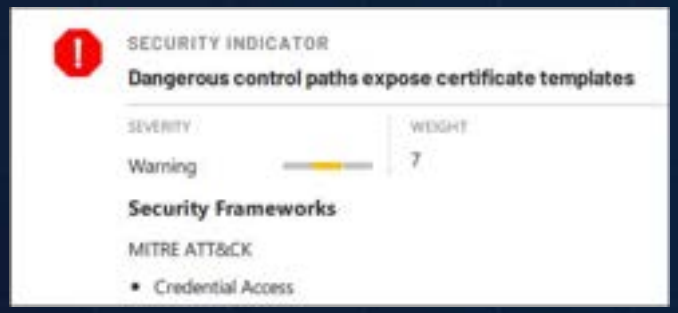
Real Life AD Incident/Recovery Scenario (1)
> *PHASE II – AD Vulnerability Analysis*

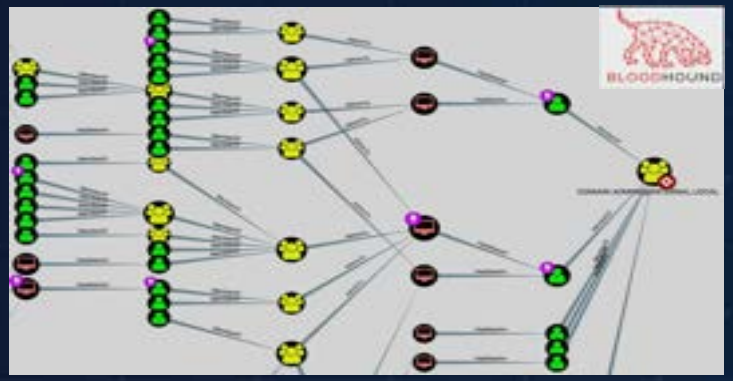


Real Life AD Incident/Recovery Scenario (1)
> *PHASE II – AD Vulnerability Analysis*



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





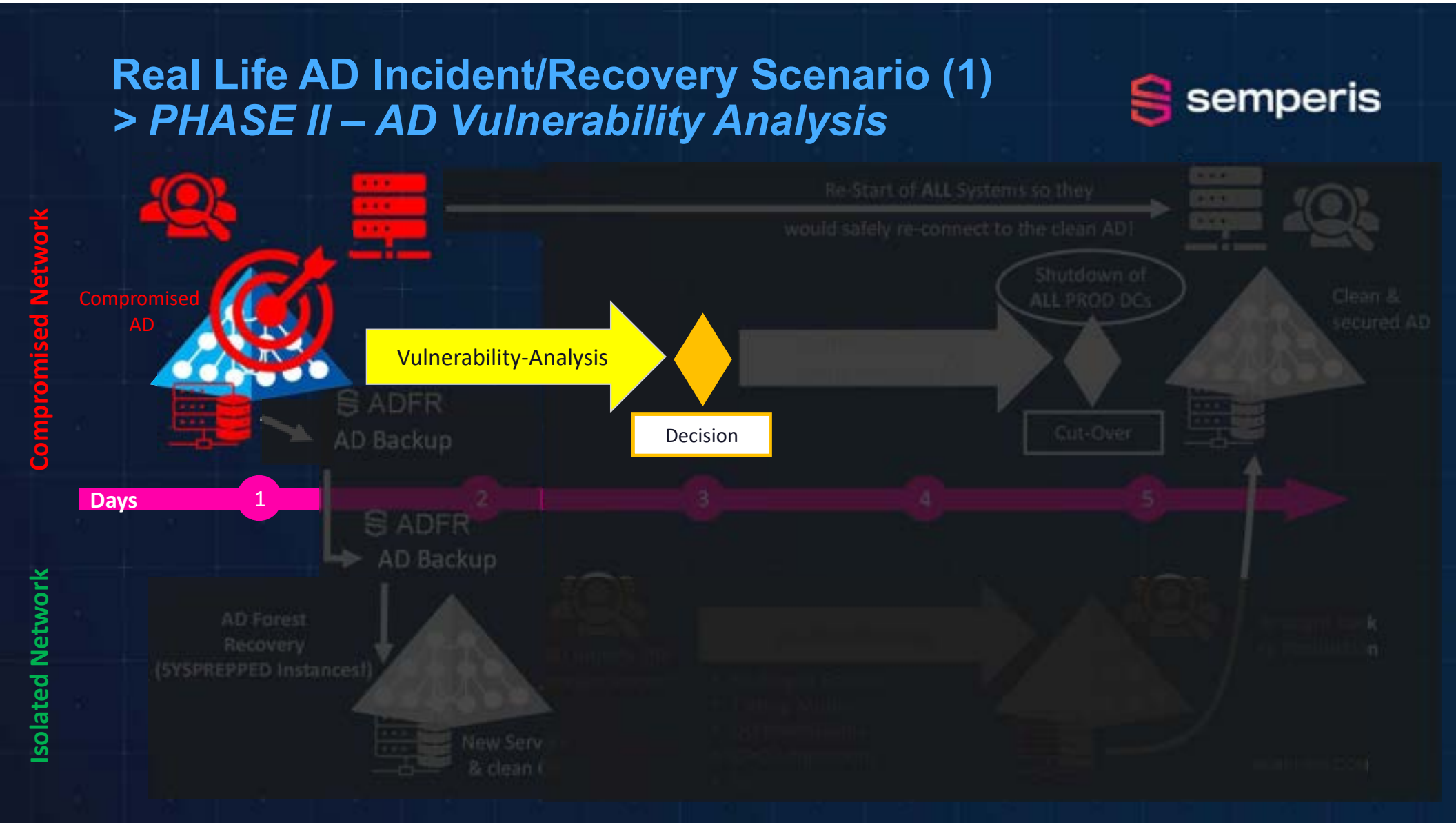
Domain Computers were allowed to change certificate templates – which allows intruders to create their own authentication certificates for any user!

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

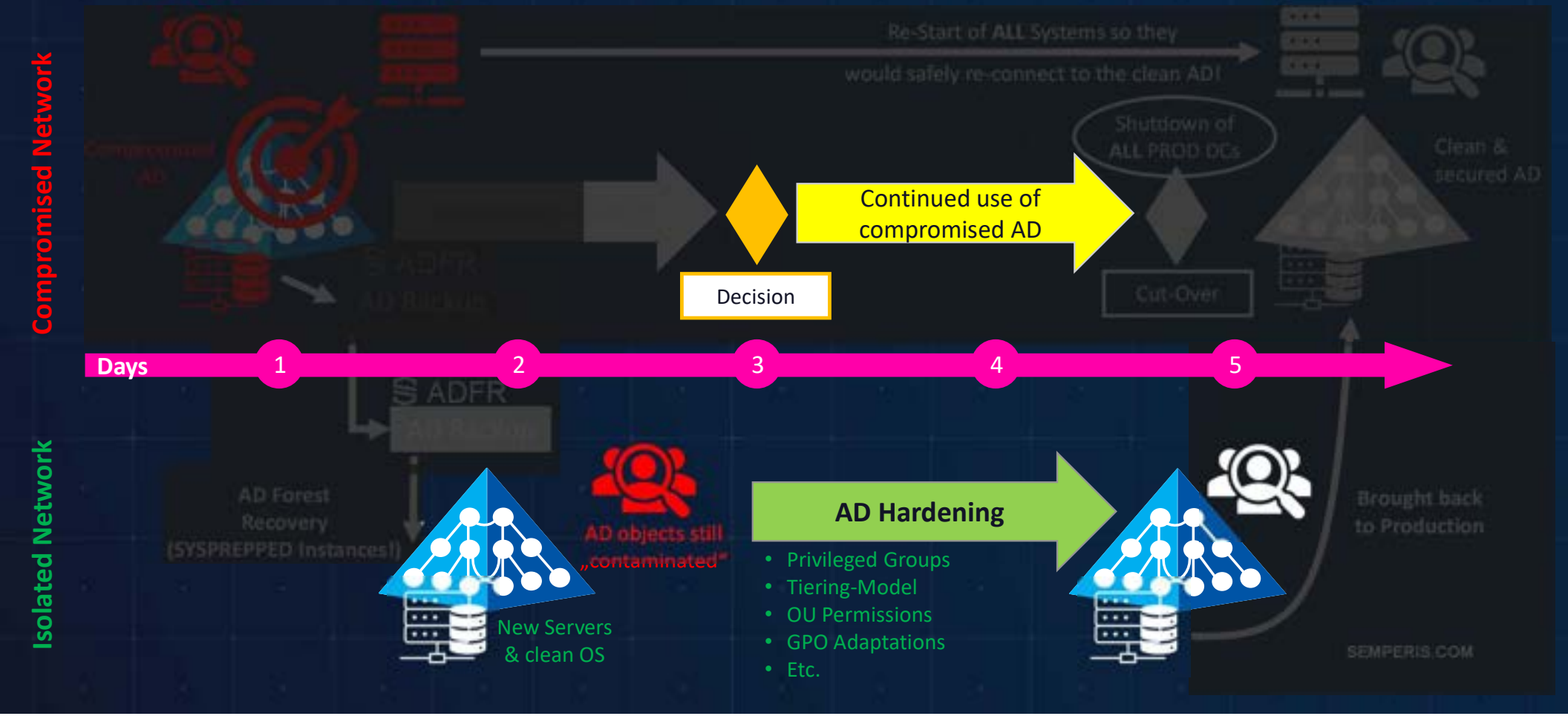
And **EVERYONE** was permissioned to reset the password of the helpdesk account!

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*



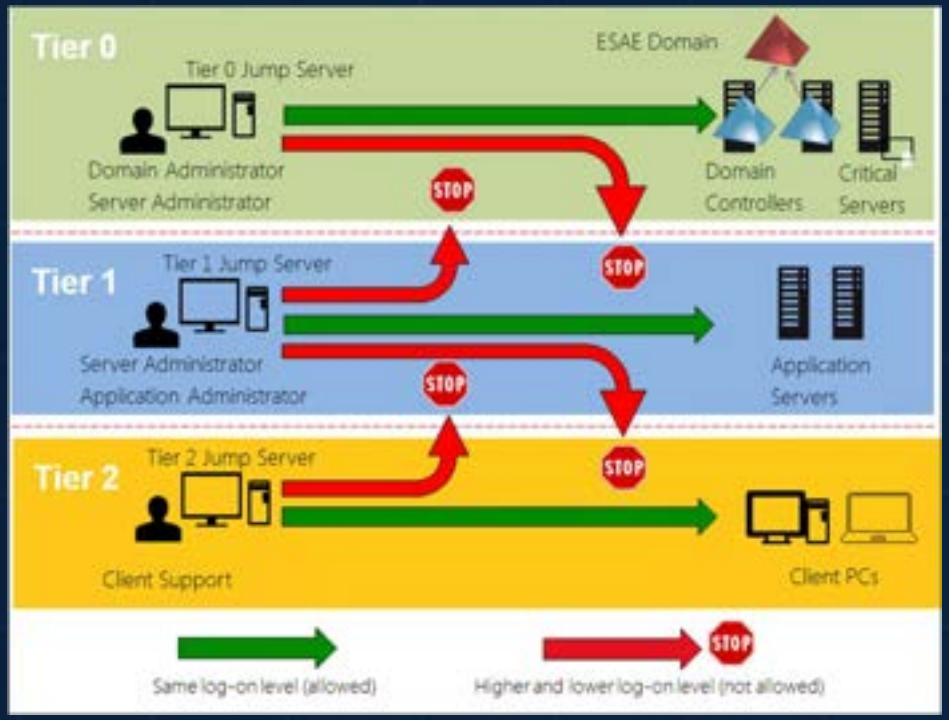
Real Life AD Incident/Recovery Scenario (1)
> *PHASE III - Divide And Conquer!*



Real Life AD Incident/Recovery Scenario (1)
> AD Hardening Speedway…

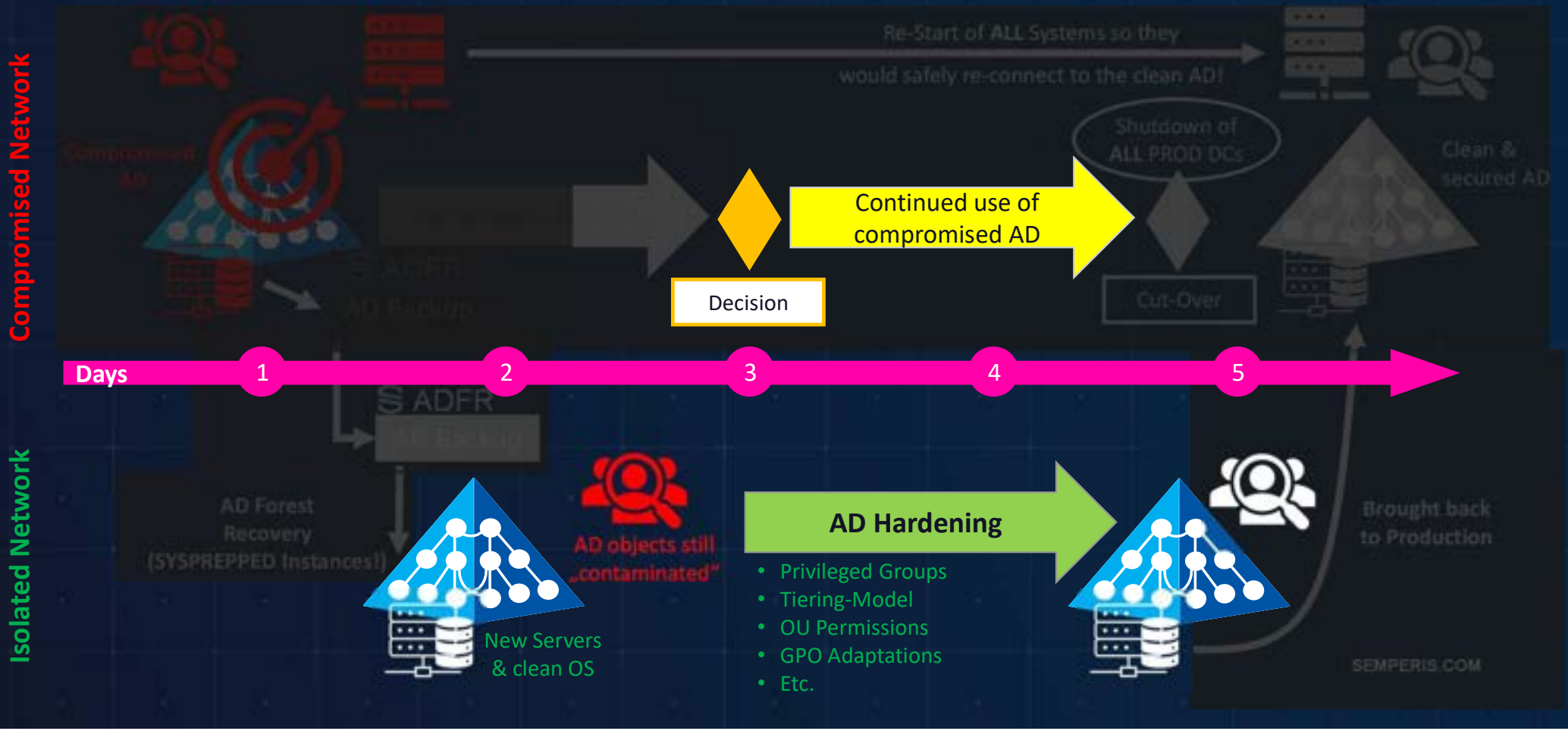
semperis

- 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
  - …



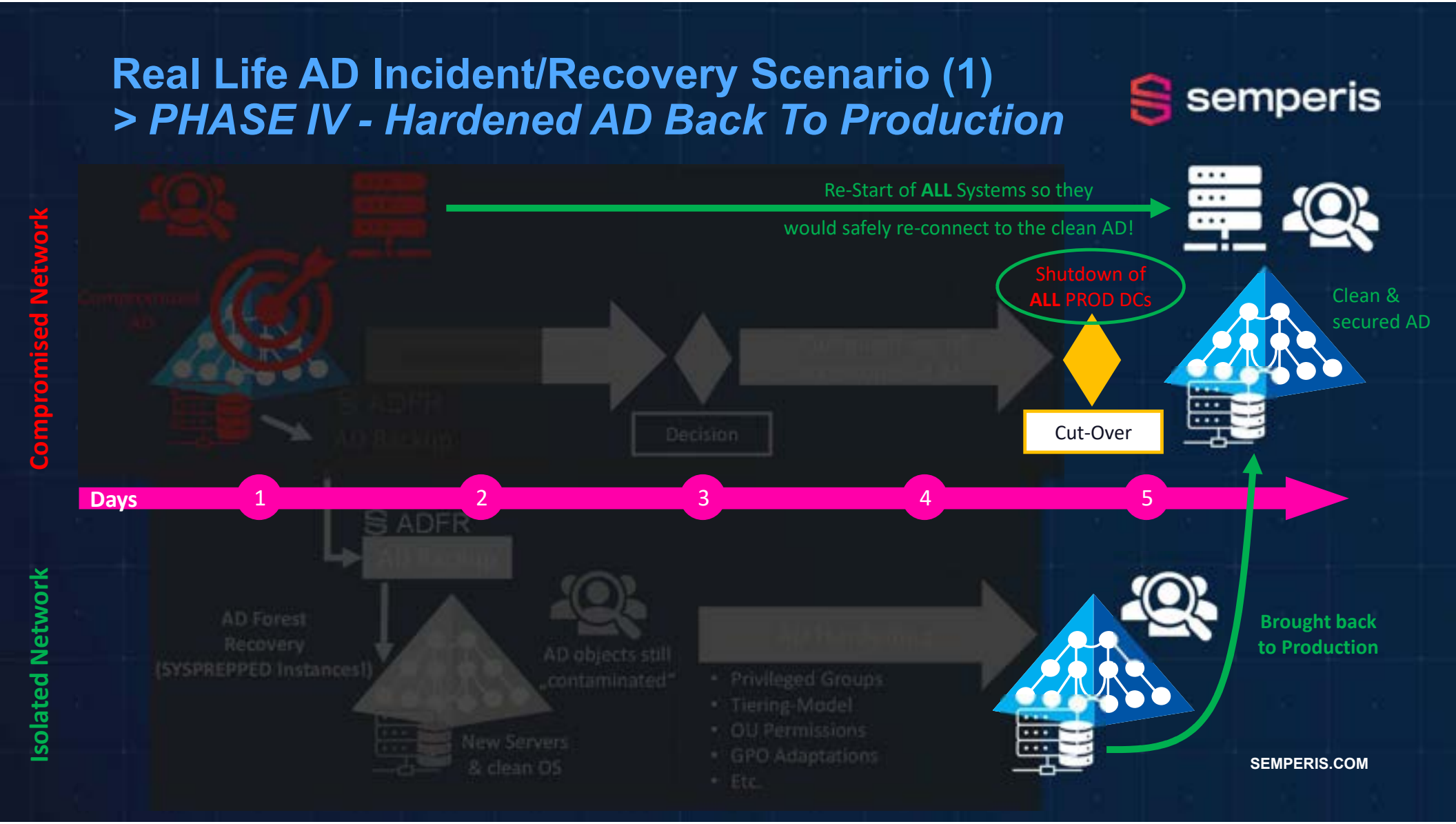
Real Life AD Incident/Recovery Scenario (1)
> *PHASE III - Divide And Conquer!*

semperis



Real Life AD Incident/Recovery Scenario (1)
> *PHASE IV - Hardened AD Back To Production*

semperis



Real Life AD Incident/Recovery Scenario (1)
> *This Experience Felt Like…*

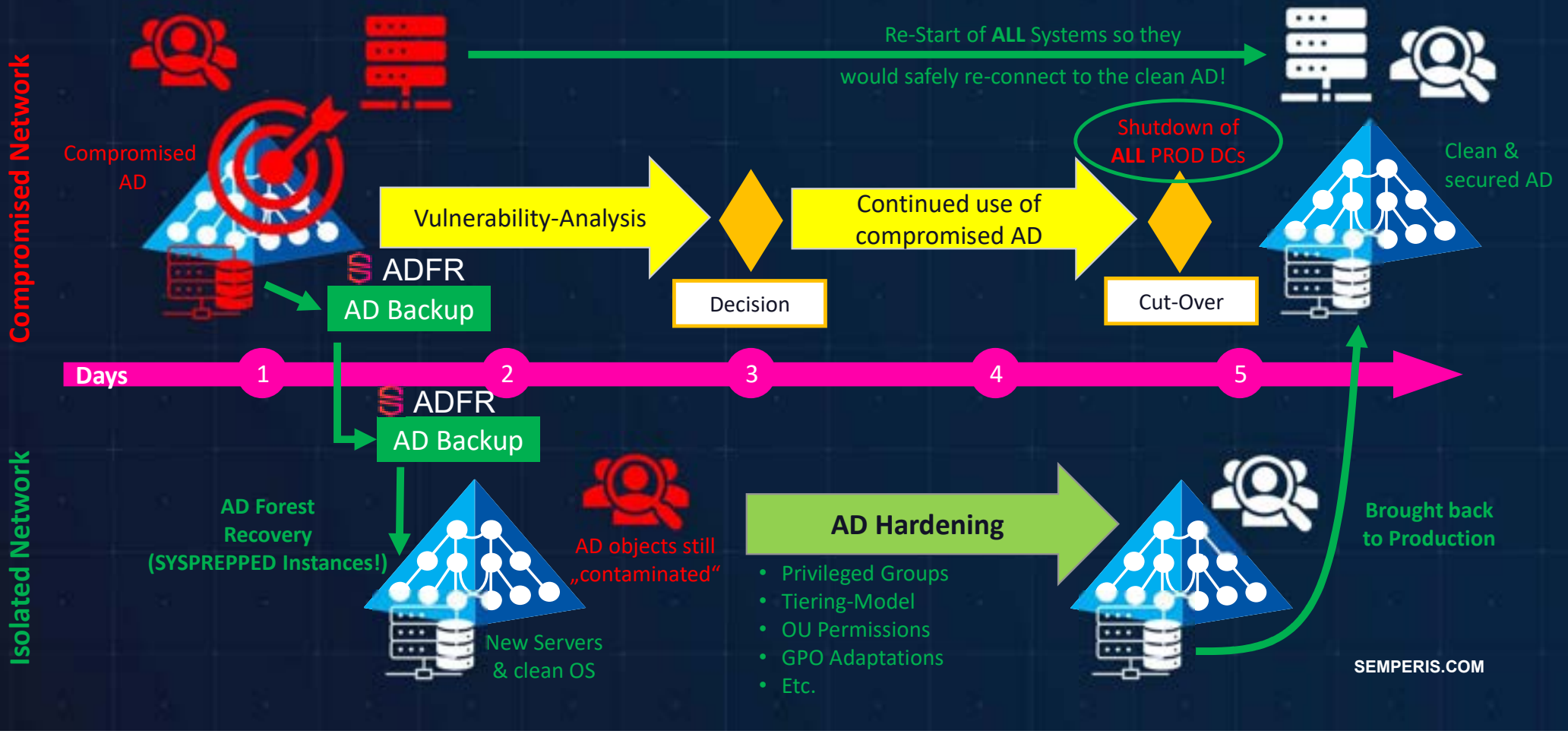
semperis

SEMPERIS.COM

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

Real Life AD Incident/Recovery Scenario (1)
> *In The End – They Survived!* ☺

semperis



Take Aways!

Take Aways!

semperis

- 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

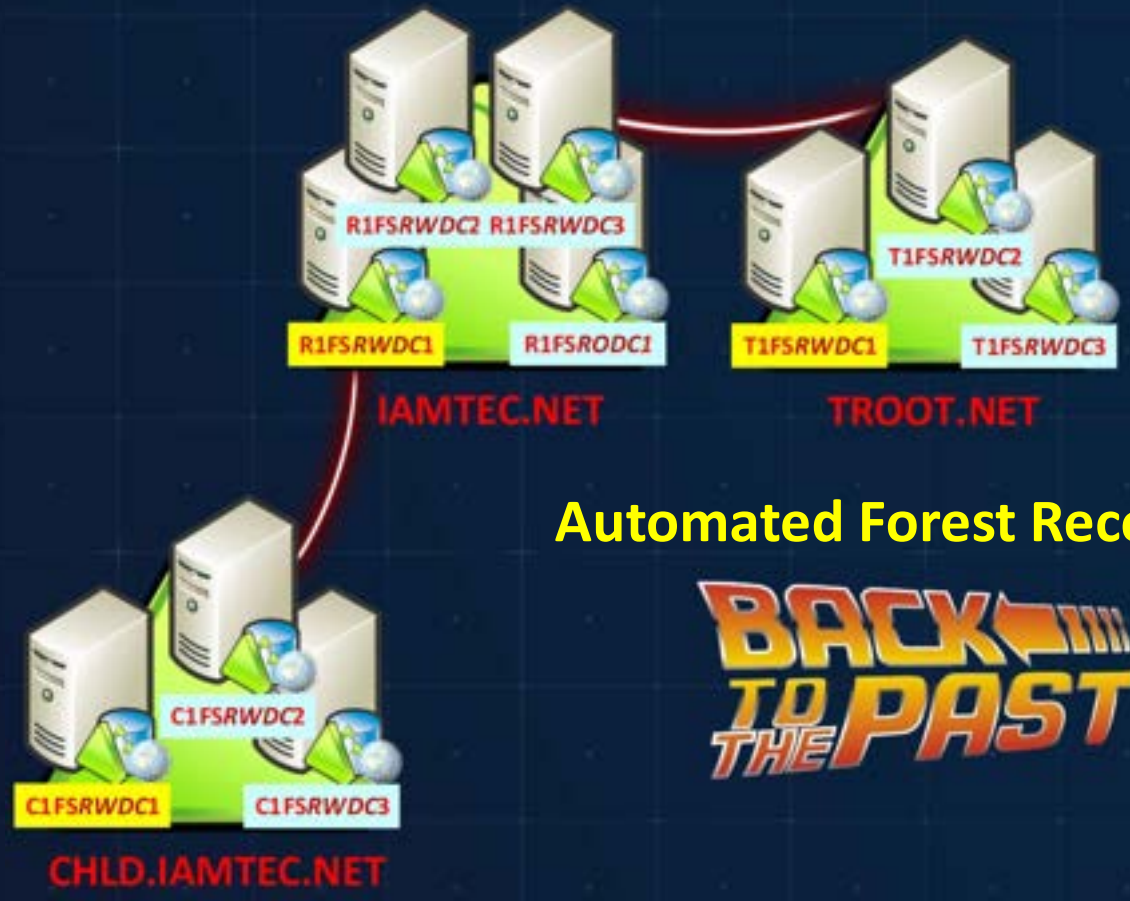
Take Aways!

semperis

- 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

semperis



Automated Forest Recovery

BACK TO THE PAST

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!