semperis

WELCOME

Semperis Overview

Sean Deuby

PRINCIPAL TECHNOLOGIST, SEMPERIS

sean@semperis.com

CONTACT INFORMATION:

Jimmy McNary (VP Federal) jimmym@semperis.com

Sean Deuby (Principal Technologist) seand@semperis.com

Chris Ingle (Senior Solutions Architect) chrisi@semperis.com

Anne Morgan (Federal Sales) annem@semperis.com

KKR

INSIGHT PARTNERS

Microsoft Partner

Enterprise Cloud Alliance
Microsoft Accelerator Alumni
Microsoft Co-Sell
Microsoft Intelligence Security Association (MISA)

Inc. 5000 America's Fastest-Growing Private Companies

TOP 5 FASTEST-GROWING CYBERSECURITY COMPANIES

500™ Technology Fast 500 2024 NORTH AMERICA

5 YEARS IN A ROW OF DOUBLE-DIGIT GROWTH

FORTUNE CYBER 60

NAMED TO FORTUNE'S CYBER 60 2024 LIST

Inc. Best Workplaces 2024

3 CONSECUTIVE YEARS ON THE LIST

dun's 100

#14 ON DUN'S 100 2022 RANKING OF BEST STARTUPS

MVP

150+ COMBINED YEARS OF MICROSOFT MVP EXPERIENCE

EY Entrepreneur Of The Year®
2023 Award Winner

EY HONORS SEMPERIS CEO MICKEY BRESMAN

Inc. 5000 Vet100 2022 IVMF America's Fastest-Growing Veteran-Owned Businesses

TOP 10 OF US 100 FASTEST-GROWING VETERAN-OWNED BUSINESSES

semperis

Agenda

- About Semperis
- Security, Identity, and Active Directory
- Active Directory Attack and Recovery Risks
- Protecting Hybrid Identity Before, During, and After an Attack

semperis

ABOUT SEMPERIS

Foundational identity security

Identity-driven cyber resilience and threat mitigation for hybrid and multi-cloud environments

Gartner peerinsights™

5.0 ★★★★★

The world's biggest brands trust Semperis

100+ million

Identities protected by Semperis (and counting)

#1 health system in the US, **top 5** in the world

2/3 top consulting firms in the world

2/3 top airlines in the world

#1 and **#5** big box retailer in the world

#1 bank in Europe. **#2** bank in the U.S.

Top 5 property insurer in the U.S. **#2** auto insurer

Federal Zero Trust Strategy

- Validated user identity and access management
- Real-time device inspection and patching
- Secure application and workload development
- Network environment isolation
- End-to-end data encryption and protection
- Improved detection and response times
- Automation and orchestration

- **Zero Trust Secure Network & Data Access: Continuous Monitoring of User Identities**
- **Application Security Stack: Proven Hardened platform**
- **Visibility and Analytics: Behavioral Analytics and in-stream monitoring**

WhoAmI /career

Sean Deuby

Principal Technologist
Americas

MVP Microsoft Most Valuable Professional

2004-2019

When	*Where*	*What*
1982-1997	TEXAS INSTRUMENTS	WINDOWS NT SERVER Version 3.51 BETA
1997-2008	intel	Windows Server Active Directory
2010-2014	Windows IT Pro	Azure Active Directory
2014-2019	edgile	Enterprise Mobility + Security
2019-Present	semperis HYBRID IDENTITY PROTECTION EST. 2020 THE PODCAST	+ Microsoft Active Directory

Active Directory at the Core

Active Directory is **fundamental** to an organization’s security

It is almost **universally targeted** in cyberattacks

It is **highly vulnerable** in ways you know...

…and in ways **you haven’t prepared for**

It must be protected by **purpose-built solutions**

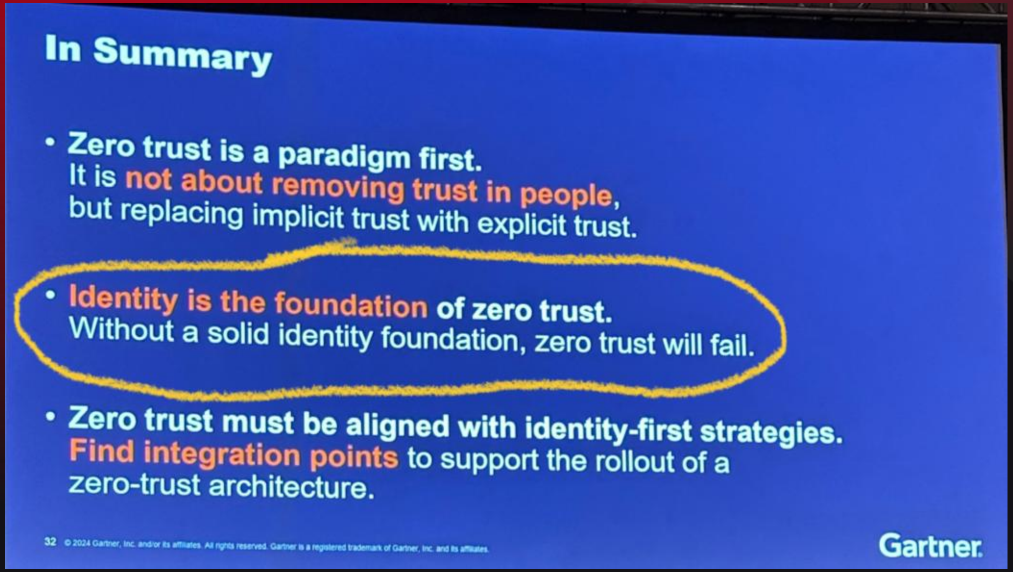
semperis

> "Identity isn't *a* security problem.
> Identity is *the* security problem."

Jen Easterly | former CISA Director

semperis

“Identity is the foundation of zero trust. Without a solid identity foundation, zero trust will fail.”
- John Watts, “Demystifying Zero Trust in an Identity First Strategy”

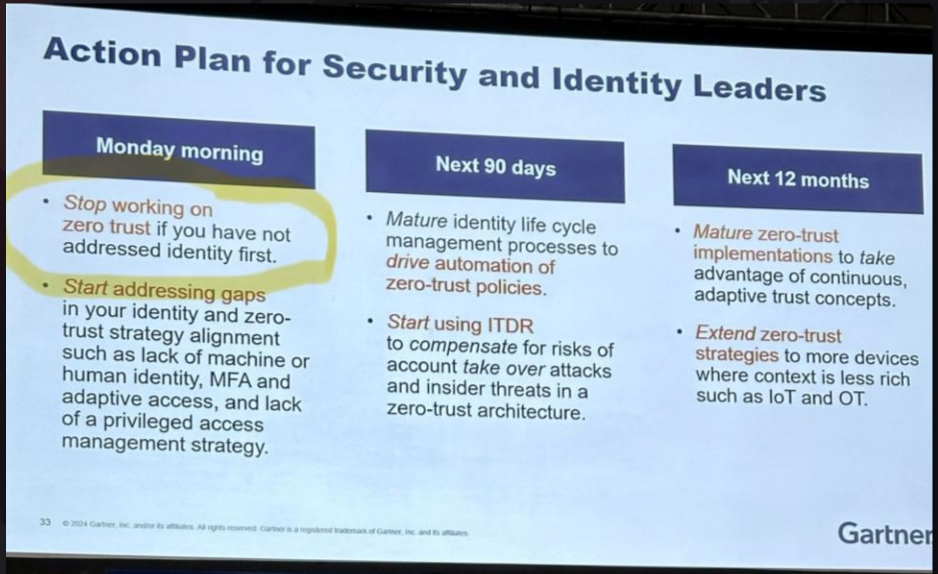


In Summary

- **Zero trust is a paradigm first.** It is not about removing trust in people, but replacing implicit trust with explicit trust.
- **Identity is the foundation of zero trust.** Without a solid identity foundation, zero trust will fail.
- **Zero trust must be aligned with identity-first strategies.** Find integration points to support the rollout of a zero-trust architecture.

32 © 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Gartner



Action Plan for Security and Identity Leaders

Monday morning

- *Stop* working on zero trust if you have not addressed identity first.
- *Start* addressing gaps in your identity and zero-trust strategy alignment such as lack of machine or human identity, MFA and adaptive access, and lack of a privileged access management strategy.

Next 90 days

- *Mature* identity life cycle management processes to *drive* automation of zero-trust policies.
- *Start* using ITDR to *compensate* for risks of account *take over* attacks and insider threats in a zero-trust architecture.

Next 12 months

- *Mature* zero-trust implementations to *take* advantage of continuous, adaptive trust concepts.
- *Extend* zero-trust strategies to more devices where context is less rich such as IoT and OT.

33 © 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Gartner

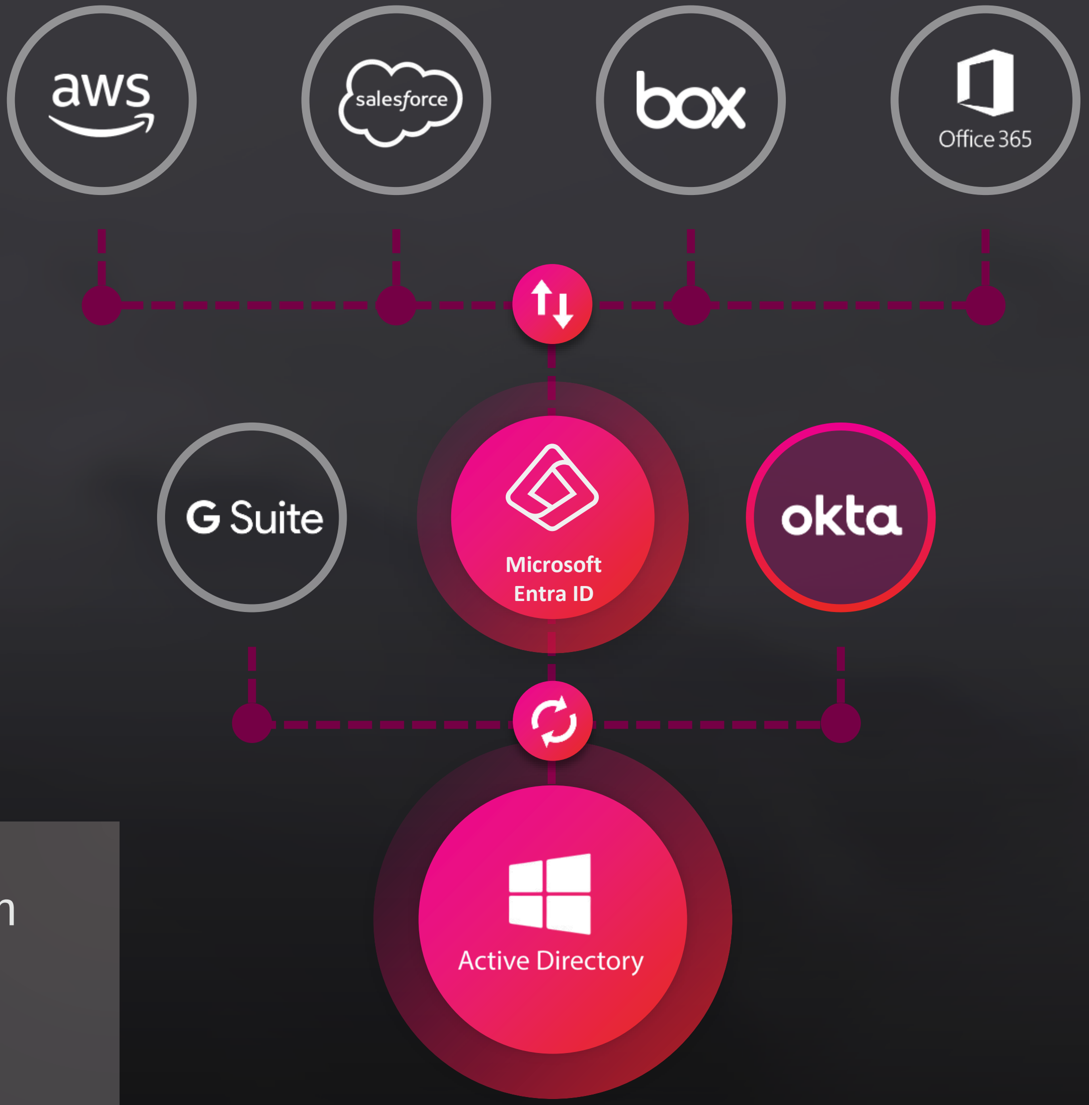
“*Stop* working on zero trust if you haven’t addressed identity first.”

Gartner IAM Summit 2024

KEYS TO THE KINGDOM

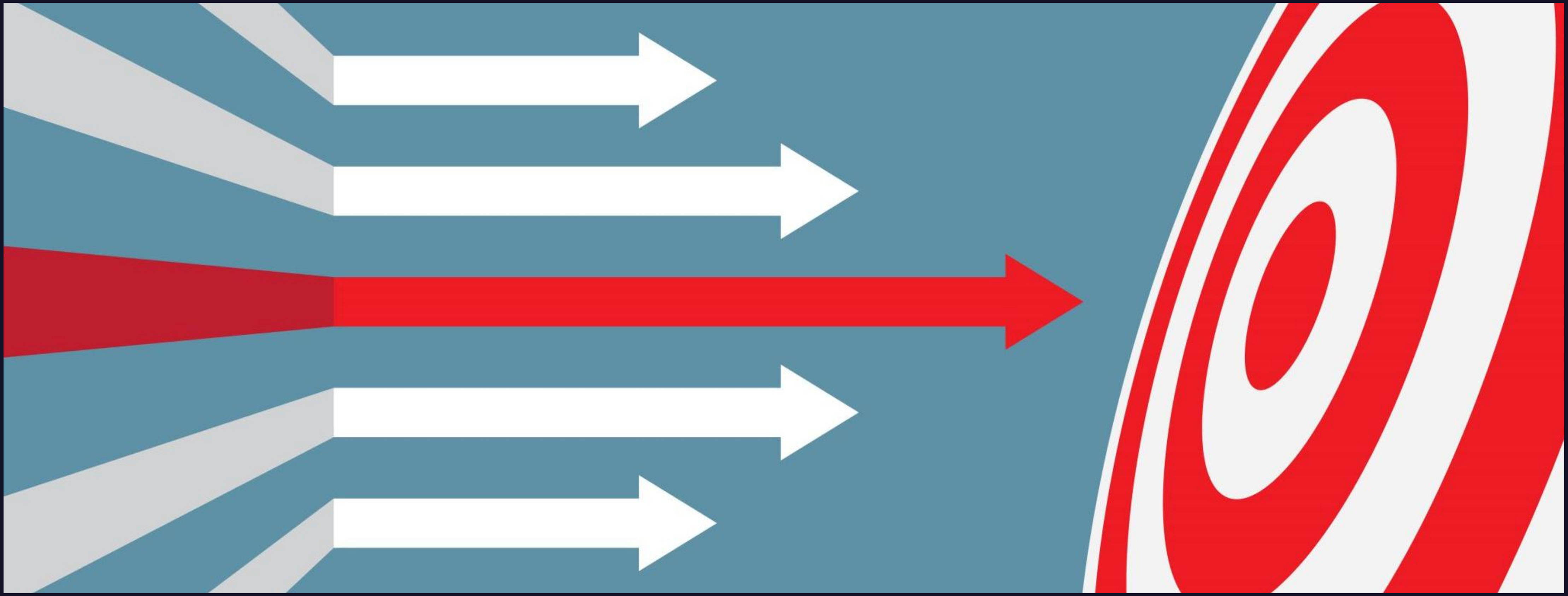
If Active Directory isn't secure, nothing is

- AD is the **de facto identity system** in almost all medium and large organizations
- **Hybrid Identity**: AD integrated with cloud identity services to provide single sign on to cloud applications
- **Zero trust model** assumes hybrid AD integrity



For 90% of organizations, security starts with AD

Active Directory as a Target



semperis

#1 TARGET

*When Microsoft Incident Response is engaged during an incident…**in most engagements, threat actors have taken full control of Active Directory** –i.e., total domain compromise.*

Microsoft

***90% of attacks investigated involve AD in some form**, whether it is the initial attack vector or targeted to achieve persistence or privileges.*

MANDIANT

The Five Eyes' urgent guidance on AD security threats

- Cybersecurity agencies from the **Five Eyes intelligence 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 over 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.

- Semperis' Purple Knight free AD security assessment utility recommended

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Detecting and Mitigating Active Directory Compromises

First published: September 2024

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

CISA
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

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

https://cisa.gov/resources-tools/resources/detecting-and-mitigating-active-directory-compromises

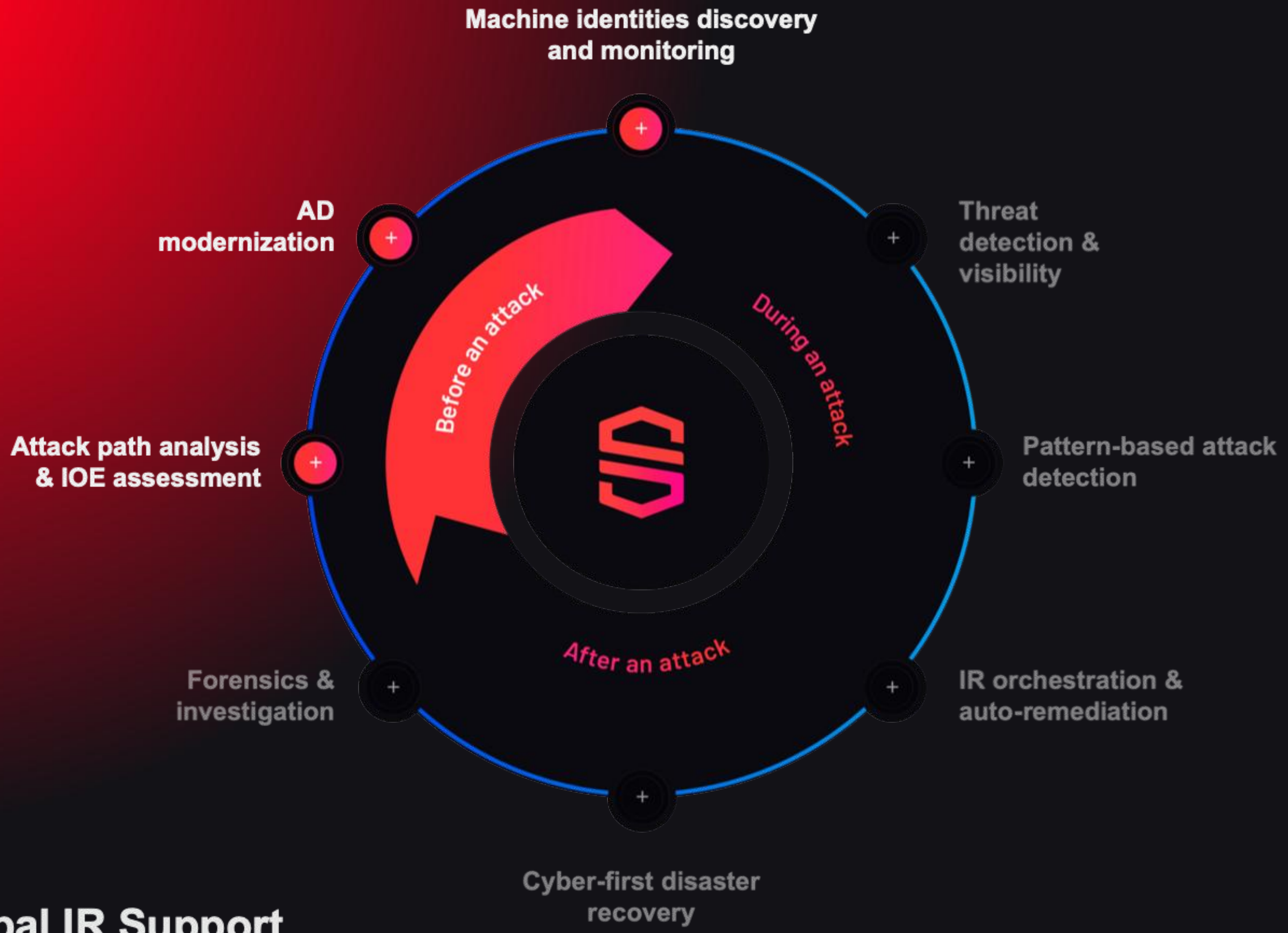
FOUNDATIONAL IDENTITY SECURITY

So, what does it take to protect hybrid AD?

(AD and Entra ID)

semperis

PRE-attack

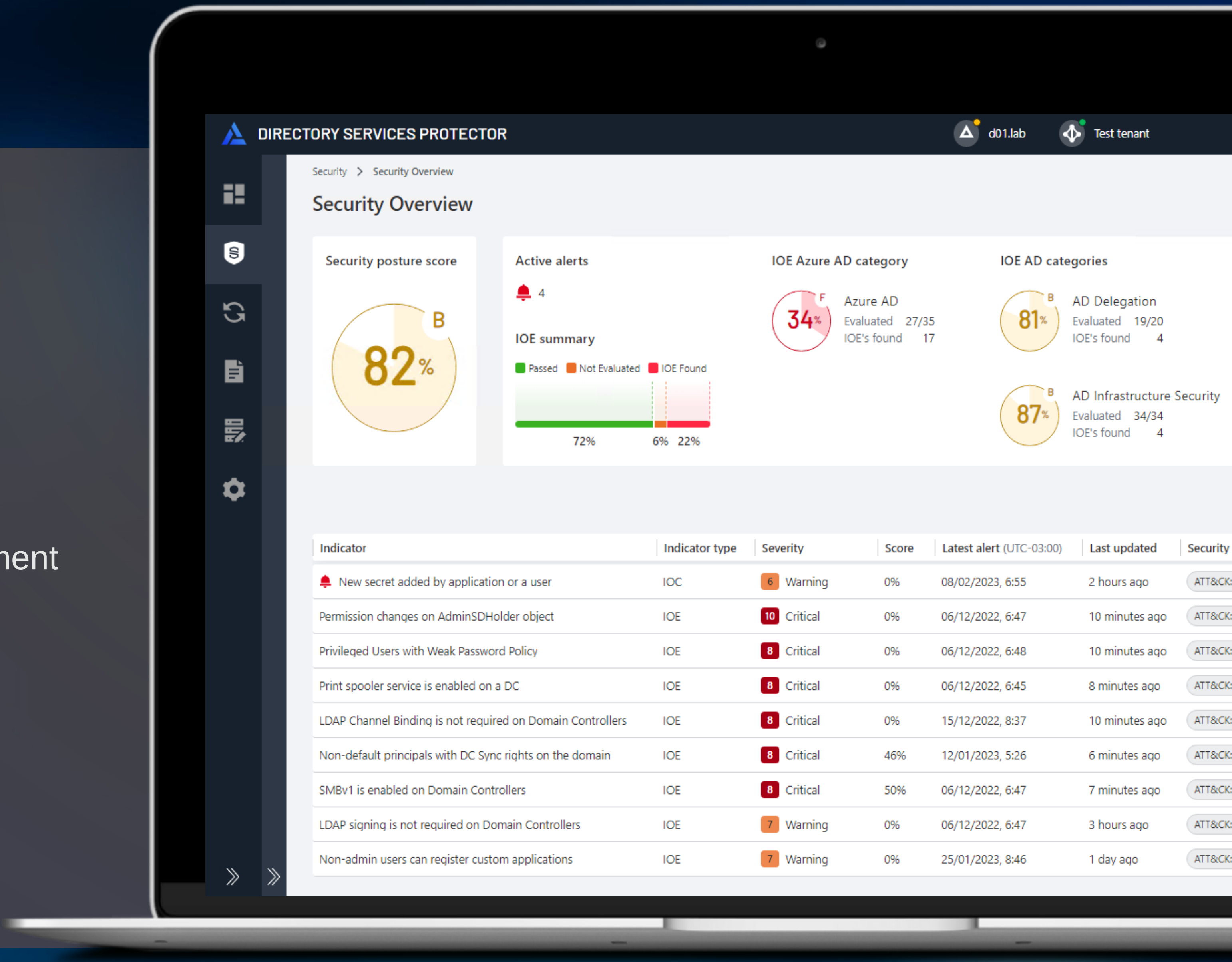

Machine identities discovery and monitoring
Threat detection & visibility
Pattern-based attack detection
IR orchestration & auto-remediation
Cyber-first disaster recovery
Forensics & investigation
Attack path analysis & IOE assessment
AD modernization
Before an attack
During an attack
After an attack

24/7 Global IR Support

DIRECTORY SERVICES PROTECTOR

Prevent

- Continuous vulnerability assessment
- Compliance reporting



DIRECTORY SERVICES PROTECTOR   d01.lab   Test tenant

Security > Security Overview

Security Overview

Security posture score

B 82%

Active alerts

4

IOE summary

🟩 Passed 🟧 Not Evaluated 🟥 IOE Found

72% 6% 22%

IOE Azure AD category

F 34% Azure AD
Evaluated 27/35
IOE's found 17

IOE AD categories

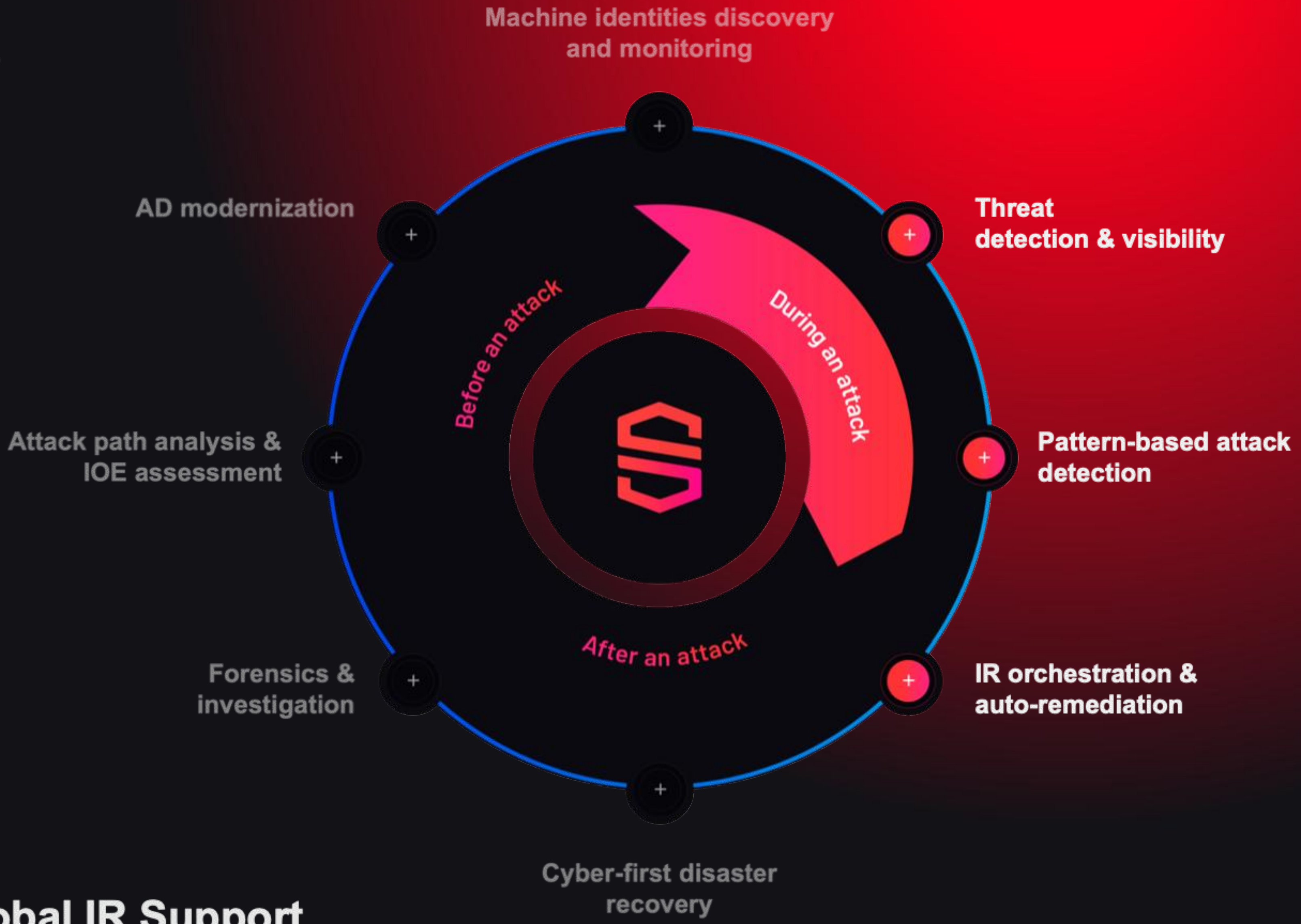
B 81% AD Delegation
Evaluated 19/20
IOE's found 4

B 87% AD Infrastructure Security
Evaluated 34/34
IOE's found 4

Indicator	Indicator type	Severity	Score	Latest alert (UTC-03:00)	Last updated	Security
New secret added by application or a user	IOC	6 Warning	0%	08/02/2023, 6:55	2 hours ago	ATT&CK
Permission changes on AdminSDHolder object	IOE	10 Critical	0%	06/12/2022, 6:47	10 minutes ago	ATT&CK
Privileged Users with Weak Password Policy	IOE	8 Critical	0%	06/12/2022, 6:48	10 minutes ago	ATT&CK
Print spooler service is enabled on a DC	IOE	8 Critical	0%	06/12/2022, 6:45	8 minutes ago	ATT&CK
LDAP Channel Binding is not required on Domain Controllers	IOE	8 Critical	0%	15/12/2022, 8:37	10 minutes ago	ATT&CK
Non-default principals with DC Sync rights on the domain	IOE	8 Critical	46%	12/01/2023, 5:26	6 minutes ago	ATT&CK
SMBv1 is enabled on Domain Controllers	IOE	8 Critical	50%	06/12/2022, 6:47	7 minutes ago	ATT&CK
LDAP signing is not required on Domain Controllers	IOE	7 Warning	0%	06/12/2022, 6:47	3 hours ago	ATT&CK
Non-admin users can register custom applications	IOE	7 Warning	0%	25/01/2023, 8:46	1 day ago	ATT&CK

semperis

DURING attack

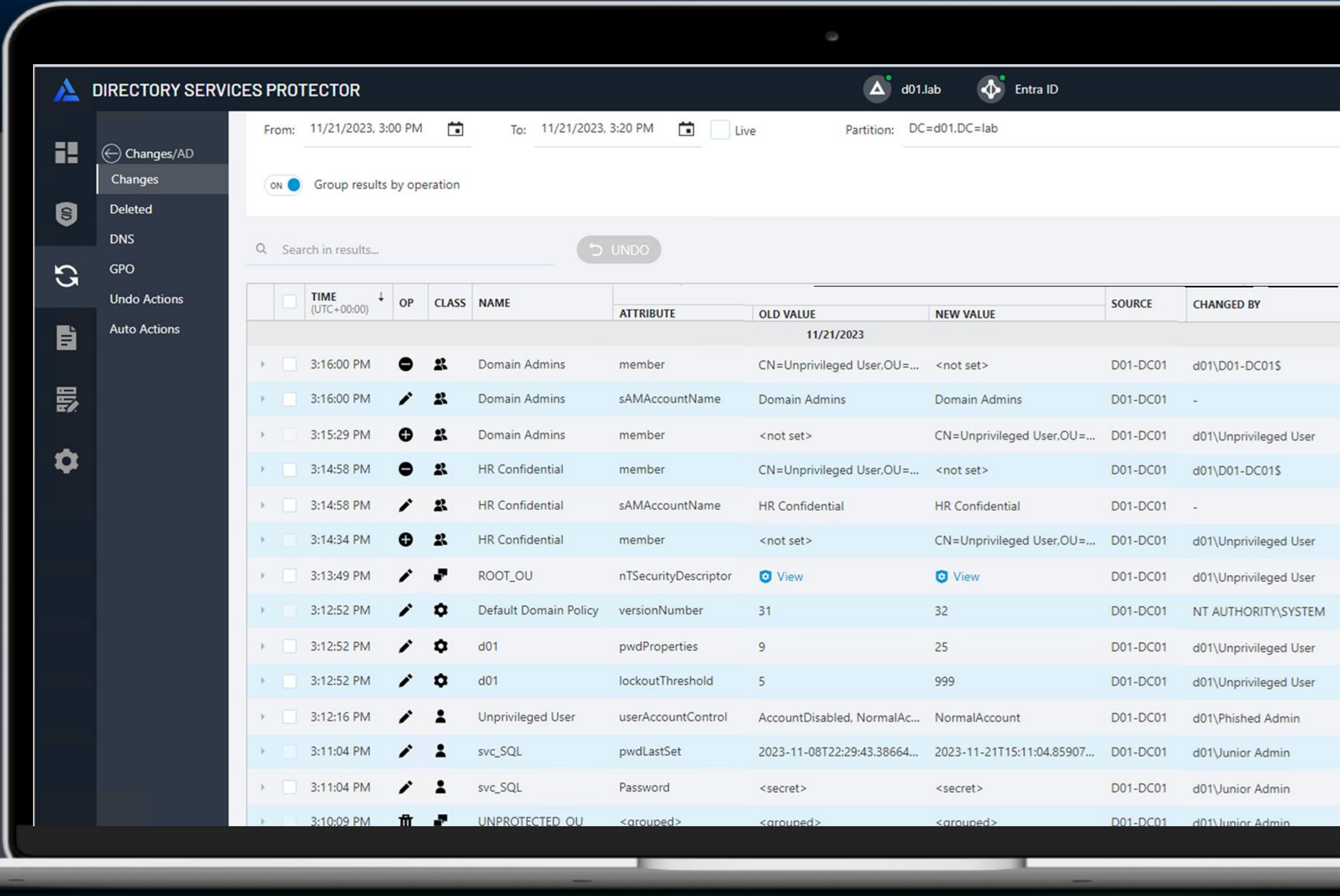

Machine identities discovery and monitoring
AD modernization
Threat detection & visibility
Before an attack
During an attack
Attack path analysis & IOE assessment
Pattern-based attack detection
After an attack
Forensics & investigation
IR orchestration & auto-remediation
Cyber-first disaster recovery

24/7 Global IR Support

DIRECTORY SERVICES PROTECTOR

Detect & Respond

- ✓ Tamperproof tracking
- ✓ Real-time security alerts
- ✓ Auto-remediation (malicious change rollback)



From: 11/21/2023, 3:00 PM To: 11/21/2023, 3:20 PM □ Live Partition: DC=d01,DC=lab

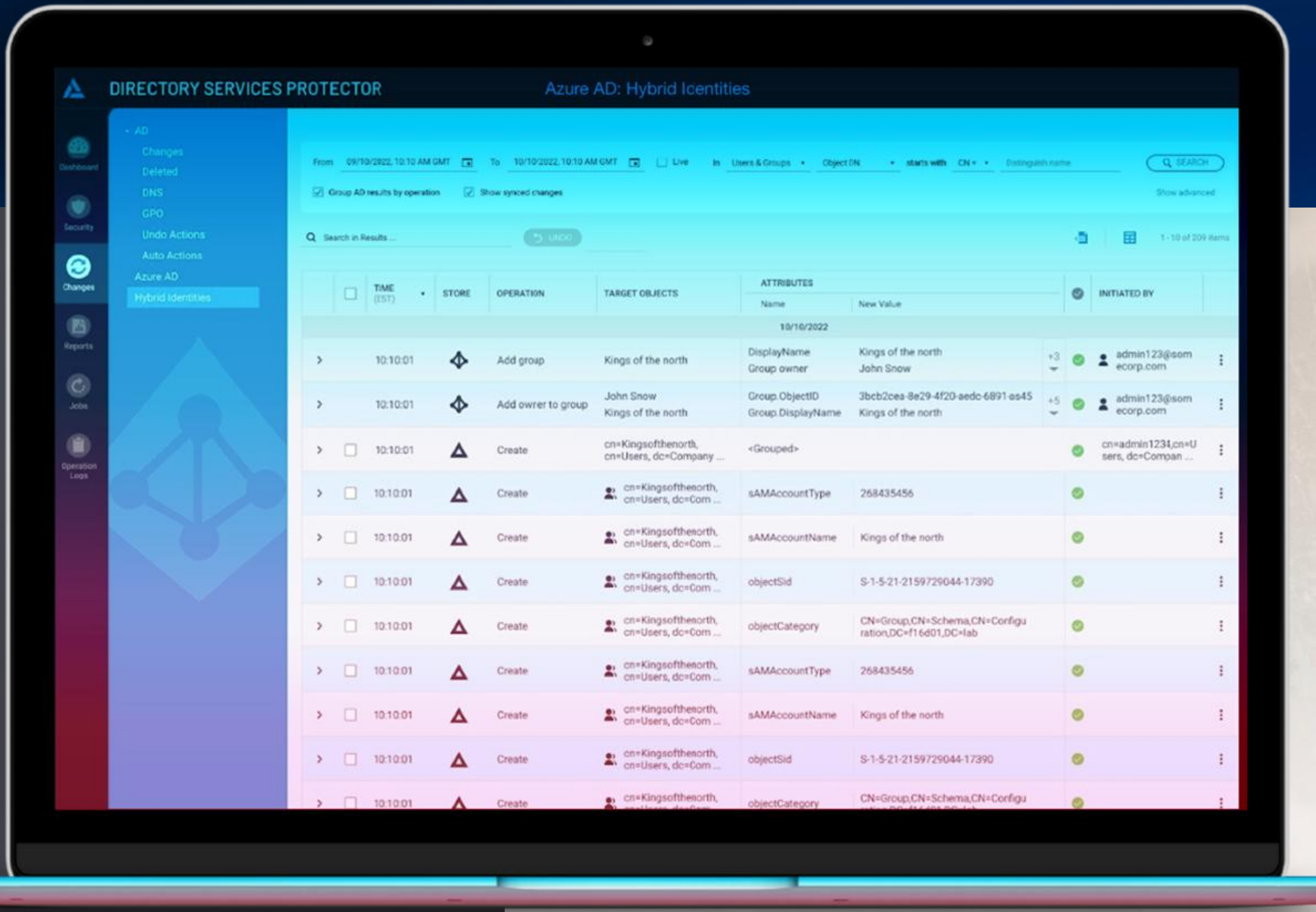
ON ● Group results by operation

□	TIME (UTC+00:00)	OP	CLASS	NAME	ATTRIBUTE	OLD VALUE	NEW VALUE	SOURCE	CHANGED BY
						11/21/2023			
□	3:16:00 PM	⊖	👥	Domain Admins	member	CN=Unprivileged User,OU=...	<not set>	D01-DC01	d01\D01-DC01$
□	3:16:00 PM	✎	👥	Domain Admins	sAMAccountName	Domain Admins	Domain Admins	D01-DC01	-
□	3:15:29 PM	⊕	👥	Domain Admins	member	<not set>	CN=Unprivileged User,OU=...	D01-DC01	d01\Unprivileged User
□	3:14:58 PM	⊖	👥	HR Confidential	member	CN=Unprivileged User,OU=...	<not set>	D01-DC01	d01\D01-DC01$
□	3:14:58 PM	✎	👥	HR Confidential	sAMAccountName	HR Confidential	HR Confidential	D01-DC01	-
□	3:14:34 PM	⊕	👥	HR Confidential	member	<not set>	CN=Unprivileged User,OU=...	D01-DC01	d01\Unprivileged User
□	3:13:49 PM	✎	▨	ROOT_OU	nTSecurityDescriptor	View	View	D01-DC01	d01\Unprivileged User
□	3:12:52 PM	✎	⚙	Default Domain Policy	versionNumber	31	32	D01-DC01	NT AUTHORITY\SYSTEM
□	3:12:52 PM	✎	⚙	d01	pwdProperties	9	25	D01-DC01	d01\Unprivileged User
□	3:12:52 PM	✎	⚙	d01	lockoutThreshold	5	999	D01-DC01	d01\Unprivileged User
□	3:12:16 PM	✎	👤	Unprivileged User	userAccountControl	AccountDisabled, NormalAc...	NormalAccount	D01-DC01	d01\Phished Admin
□	3:11:04 PM	✎	👤	svc_SQL	pwdLastSet	2023-11-08T22:29:43.38664...	2023-11-21T15:11:04.85907...	D01-DC01	d01\Junior Admin
□	3:11:04 PM	✎	👤	svc_SQL	Password	<secret>	<secret>	D01-DC01	d01\Junior Admin
□	3:10:09 PM	🗑	▨	UNPROTECTED_OU	<grouped>	<grouped>	<grouped>	D01-DC01	d01\Junior Admin

DIRECTORY SERVICES PROTECTOR

Extend identity protection to Entra ID

Without seeing the complete picture, hybrid AD attacks fly under the radar. You need visibility into threats across AD and Entra ID.



From 09/10/2022, 10:10 AM GMT To 10/10/2022, 10:10 AM GMT □ Live In Users & Groups Object DN starts with CN Distinguish name

☑ Group AD results by operation ☑ Show synced changes

Search in Results ...

1 - 10 of 209 items

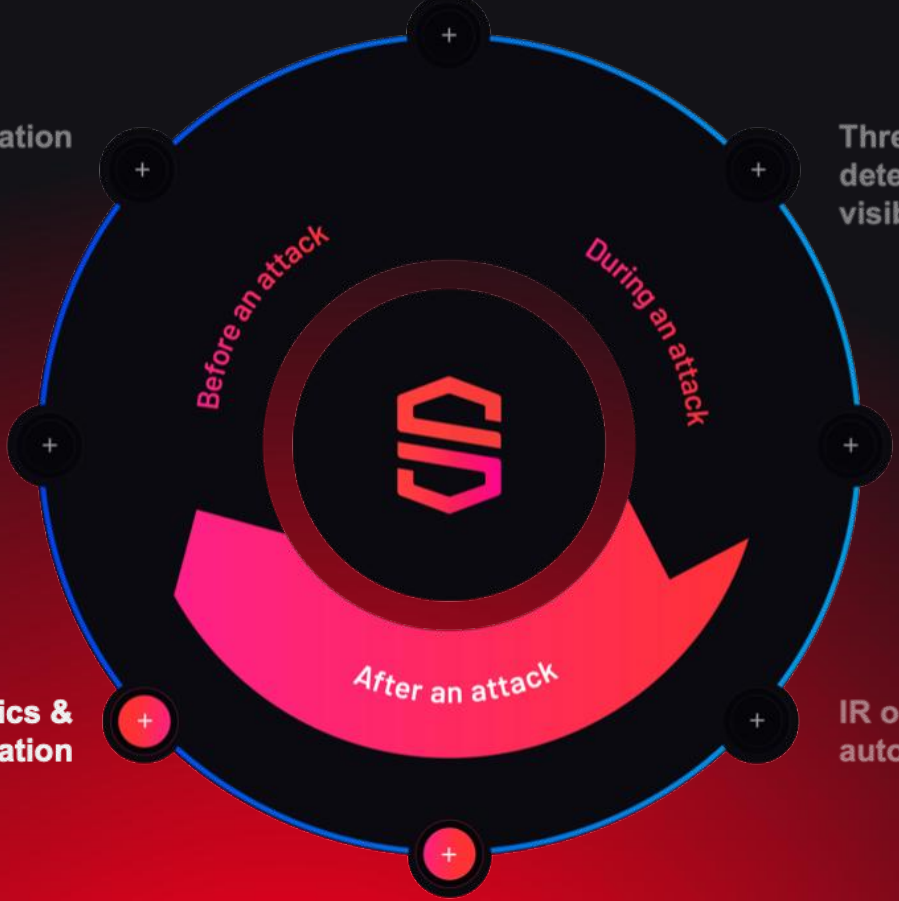
	□	TIME (EST)	STORE	OPERATION	TARGET OBJECTS	ATTRIBUTES			✓	INITIATED BY
						Name	New Value			
						10/10/2022				
›		10:10:01		Add group	Kings of the north	DisplayName Group owner	Kings of the north John Snow	+3	✓	admin123@somecorp.com
›		10:10:01		Add owrer to group	John Snow Kings of the north	Group.ObjectID Group.DisplayName	3bcb2cea-8e29-4f20-aedc-6891-as45 Kings of the north	+5	✓	admin123@somecorp.com
›	□	10:10:01		Create	cn=Kingsofthenorth, cn=Users, dc=Company ...	<Grouped>			✓	cn=admin1234,cn=Users, dc=Compan ...
›	□	10:10:01		Create	cn=Kingsofthenorth, cn=Users, dc=Com ...	sAMAccountType	268435456		✓	
›	□	10:10:01		Create	cn=Kingsofthenorth, cn=Users, dc=Com ...	sAMAccountName	Kings of the north		✓	
›	□	10:10:01		Create	cn=Kingsofthenorth, cn=Users, dc=Com ...	objectSid	S-1-5-21-2159729044-17390		✓	
›	□	10:10:01		Create	cn=Kingsofthenorth, cn=Users, dc=Com ...	objectCategory	CN=Group,CN=Schema,CN=Configuration,DC=f16d01,DC=lab		✓	
›	□	10:10:01		Create	cn=Kingsofthenorth, cn=Users, dc=Com ...	sAMAccountType	268435456		✓	
›	□	10:10:01		Create	cn=Kingsofthenorth, cn=Users, dc=Com ...	sAMAccountName	Kings of the north		✓	
›	□	10:10:01		Create	cn=Kingsofthenorth, cn=Users, dc=Com ...	objectSid	S-1-5-21-2159729044-17390		✓	
›	□	10:10:01		Create	cn=Kingsofthenorth,	objectCategory	CN=Group,CN=Schema,CN=Configu		✓	

- Entra ID security indicators
- Entra ID change tracking and rollback
- Hybrid view of AD and Entra ID

Prevention, detection, and response all in one console.

semperis

POST-attack



Machine identities discovery and monitoring

AD modernization

Threat detection & visibility

Attack path analysis & IOE assessment

Pattern-based attack detection

Forensics & investigation

IR orchestration & auto-remediation

Cyber-first disaster recovery

24/7 Global IR Support

semperis

Case Study: When Nation States Attack Active Directory

semperis

IDENTITY UNDER ATTACK:

Blue vs. Red

Blue

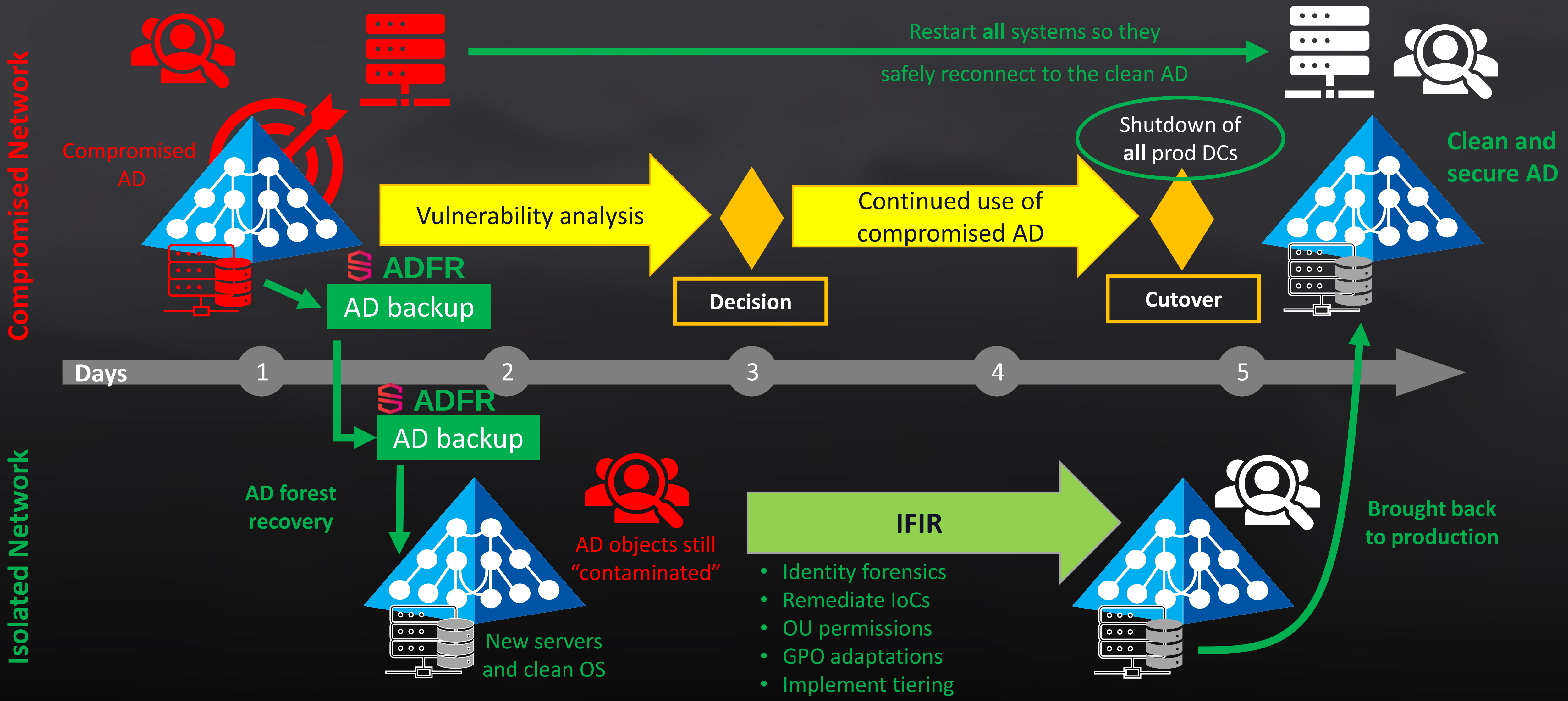
- Offshore telecom and microbanking organization
- Critical infrastructure for its country
- Basic Defender endpoint security

Red

- At least **three** different nation state actors
  - MuddyWater (Iran)
  - GALLIUM (China)
  - Cozy Bear / APT29 (Russia)

semperis

AD Cyber Recovery Timeline



Compromised Network

Isolated Network

Compromised AD

ADFR

AD backup

Restart **all** systems so they safely reconnect to the clean AD

Vulnerability analysis

Decision

Continued use of compromised AD

Shutdown of **all** prod DCs

Cutover

Clean and secure AD

Days 1 2 3 4 5

ADFR

AD backup

AD forest recovery

AD objects still "contaminated"

New servers and clean OS

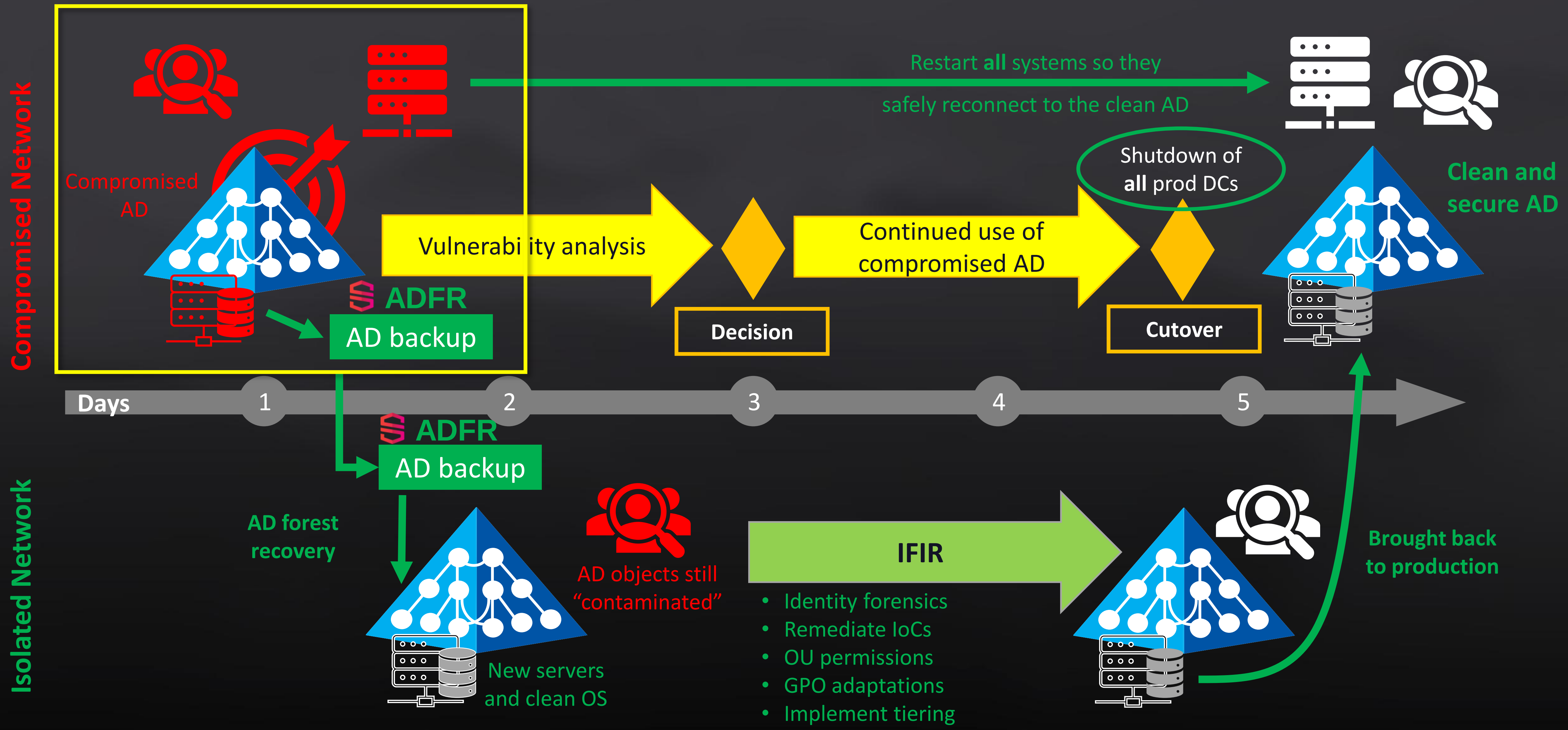
IFIR

- Identity forensics
- Remediate IoCs
- OU permissions
- GPO adaptations
- Implement tiering

Brought back to production

semperis

AD Cyber Recovery Timeline



Compromised Network

Compromised AD

ADFR

AD backup

Restart **all** systems so they safely reconnect to the clean AD

Vulnerability analysis

Decision

Continued use of compromised AD

Shutdown of **all** prod DCs

Cutover

Clean and secure AD

Days 1 2 3 4 5

Isolated Network

ADFR

AD backup

AD forest recovery

AD objects still “contaminated”

New servers and clean OS

IFIR

- Identity forensics
- Remediate IoCs
- OU permissions
- GPO adaptations
- Implement tiering

Brought back to production

semperis

IDENTITY UNDER ATTACK:

Untrustworthy Forest

Fallout

Obvious Effects

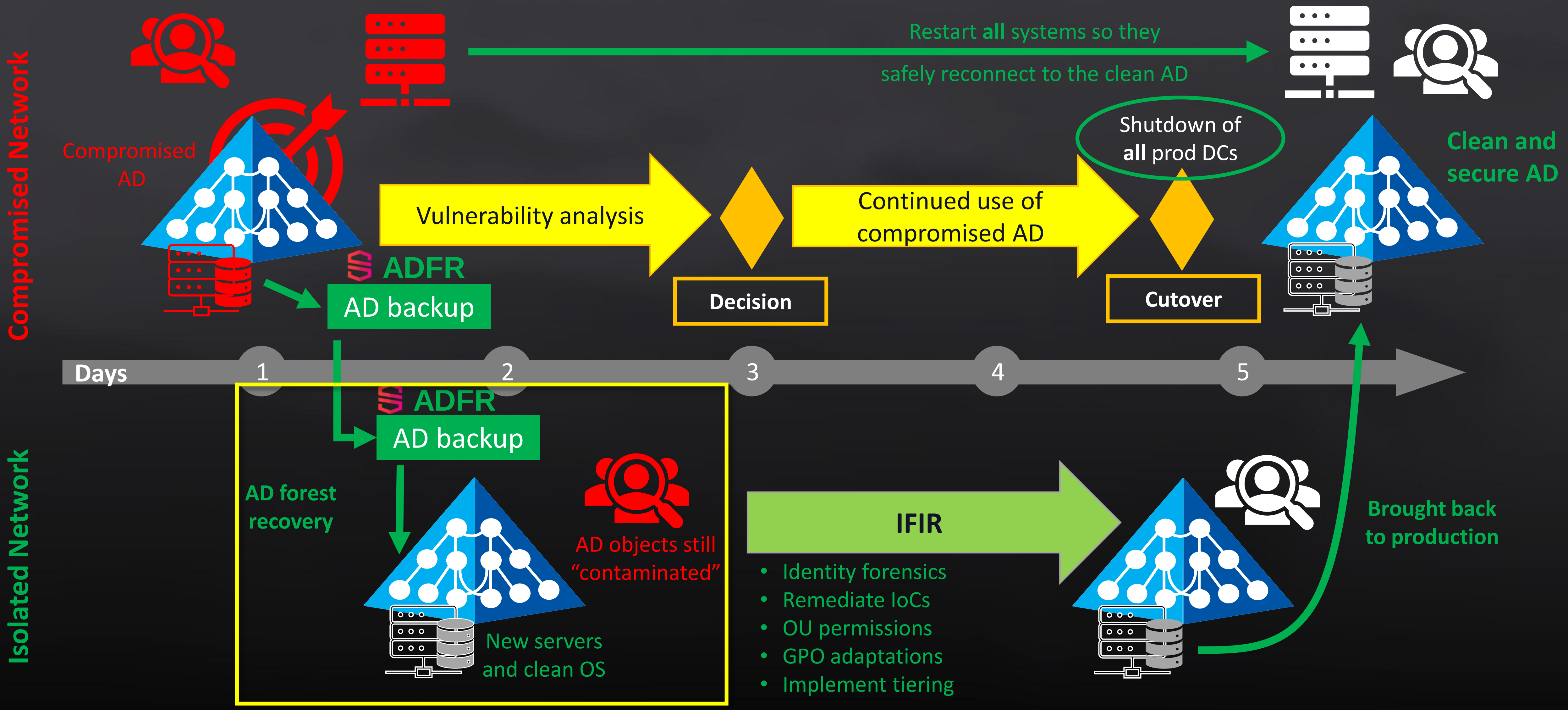
- All DCs have malware on them (OS, SYSVOL)
- Some DCs are not functional

Not So Obvious Effects

- Threat actor changes in the service to provide control or persistence
    - Privileged group membership changed
    - Permissions changed (e.g. AdminSDHolder)
    - Group Policy objects (GPOs) changed
    - Hidden objects (Deny Read ACE)
    - Back doors inserted (Mimikatz DCSHADOW)

semperis

AD Cyber Recovery Timeline



semperis

IDENTITY UNDER ATTACK:

Recover the Compromised Forest to an Isolated Recovery Environment (IRE)

Active Directory Forest Recovery (ADFR)

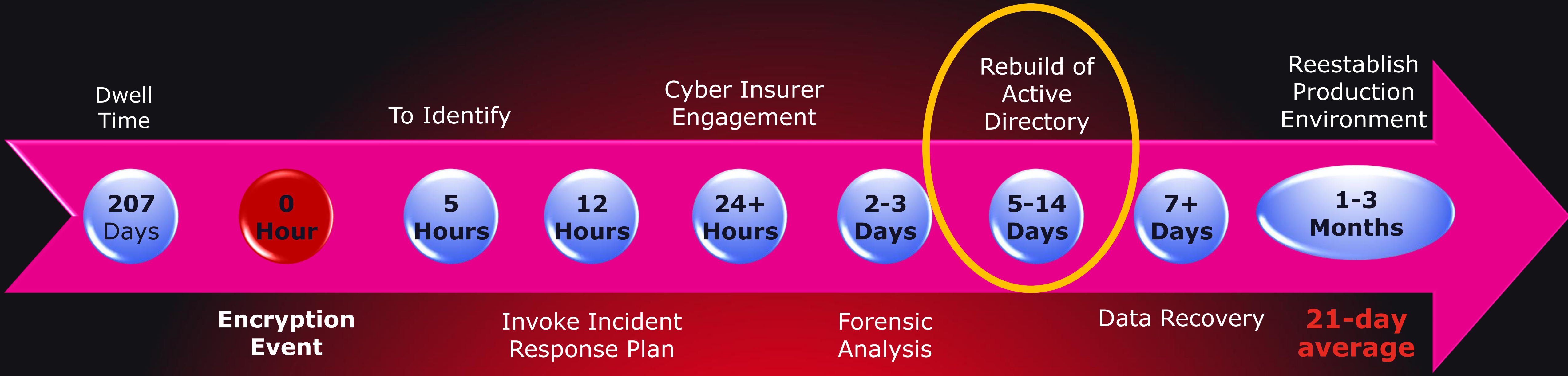
ADFR backs up AD components **but not the domain controller's OS**

- ➢Leaves malware behind
- ➢Much smaller, faster backups
- ➢Removes hardware recovery dependencies
    - ➢E.g. VMware → Azure VM

1. Create an isolated network and provision fresh (=malware free) VMs

2. Perform an automated, high-speed **AD forest recovery** using ADFR to the new, malware-free servers in the isolated network

Cyberattack Recovery Timeline



Dwell Time

207 Days

0 Hour

Encryption Event

To Identify

5 Hours

12 Hours

Invoke Incident Response Plan

Cyber Insurer Engagement

24+ Hours

2-3 Days

Forensic Analysis

Rebuild of Active Directory

5-14 Days

7+ Days

Data Recovery

Reestablish Production Environment

1-3 Months

21-day average

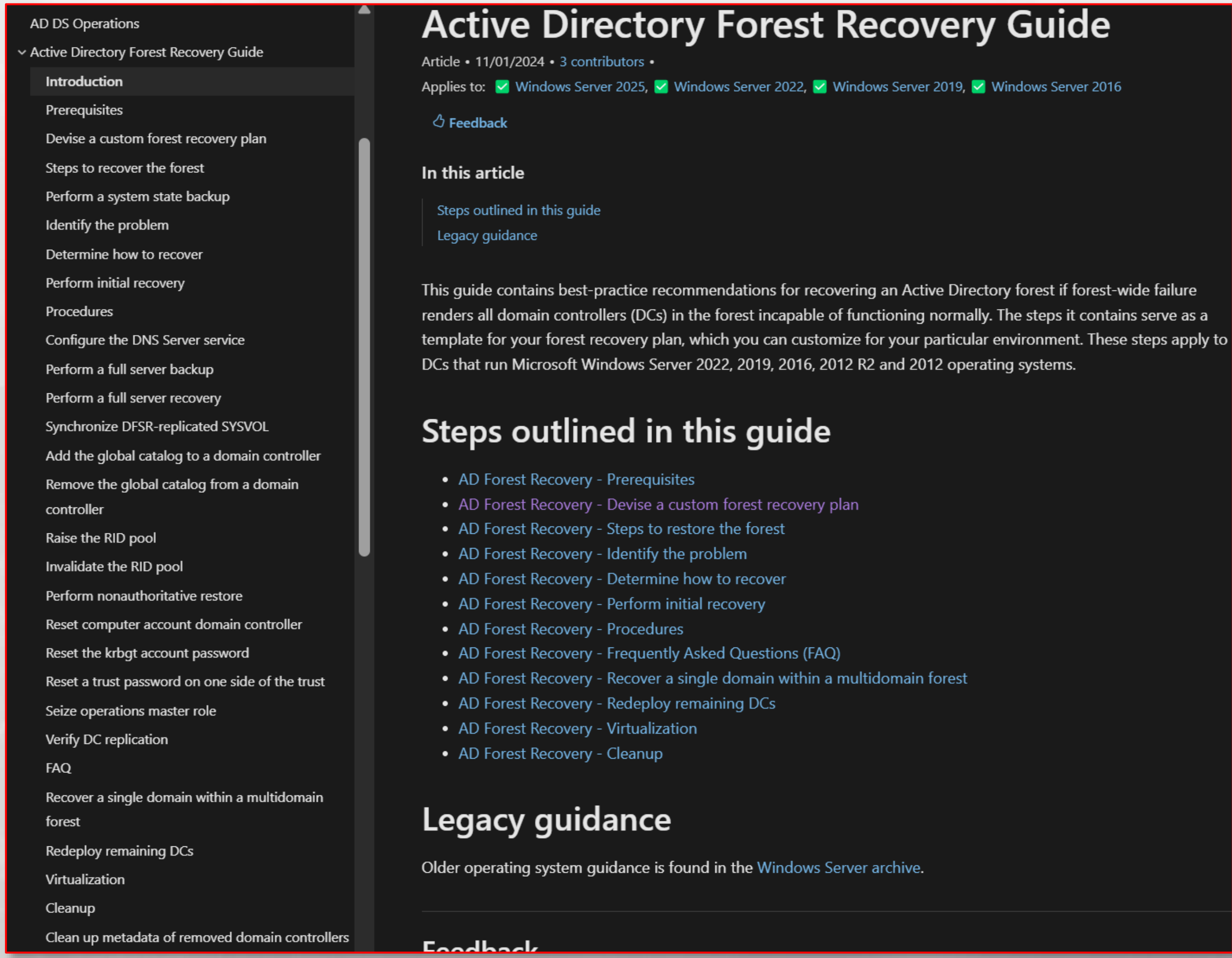
Source: CDW Data Protection Information Management (DPIM) Team

semperis

What is Active Directory Forest Recovery?

- 29+ step process of
  - Restoring, tearing down, resetting, and rebuilding your Active Directory forest

- Equivalent to **149-page procedure**
  - **40 pages** of core procedure
  - **109 pages** of supplementary procedures
- Generic; you must customize it
- *Not designed for cyber*
- Manual
- Painstakingly complex – to be executed during a company-wide outage



AD DS Operations

Active Directory Forest Recovery Guide

- Introduction
- Prerequisites
- Devise a custom forest recovery plan
- Steps to recover the forest
- Perform a system state backup
- Identify the problem
- Determine how to recover
- Perform initial recovery
- Procedures
- Configure the DNS Server service
- Perform a full server backup
- Perform a full server recovery
- Synchronize DFSR-replicated SYSVOL
- Add the global catalog to a domain controller
- Remove the global catalog from a domain controller
- Raise the RID pool
- Invalidate the RID pool
- Perform nonauthoritative restore
- Reset computer account domain controller
- Reset the krbgt account password
- Reset a trust password on one side of the trust
- Seize operations master role
- Verify DC replication
- FAQ
- Recover a single domain within a multidomain forest
- Redeploy remaining DCs
- Virtualization
- Cleanup
- Clean up metadata of removed domain controllers

Active Directory Forest Recovery Guide

Article • 11/01/2024 • 3 contributors •

Applies to: ☑ Windows Server 2025, ☑ Windows Server 2022, ☑ Windows Server 2019, ☑ Windows Server 2016

Feedback

In this article

Steps outlined in this guide

Legacy guidance

This guide contains best-practice recommendations for recovering an Active Directory forest if forest-wide failure renders all domain controllers (DCs) in the forest incapable of functioning normally. The steps it contains serve as a template for your forest recovery plan, which you can customize for your particular environment. These steps apply to DCs that run Microsoft Windows Server 2022, 2019, 2016, 2012 R2 and 2012 operating systems.

Steps outlined in this guide

- AD Forest Recovery - Prerequisites
- AD Forest Recovery - Devise a custom forest recovery plan
- AD Forest Recovery - Steps to restore the forest
- AD Forest Recovery - Identify the problem
- AD Forest Recovery - Determine how to recover
- AD Forest Recovery - Perform initial recovery
- AD Forest Recovery - Procedures
- AD Forest Recovery - Frequently Asked Questions (FAQ)
- AD Forest Recovery - Recover a single domain within a multidomain forest
- AD Forest Recovery - Redeploy remaining DCs
- AD Forest Recovery - Virtualization
- AD Forest Recovery - Cleanup

Legacy guidance

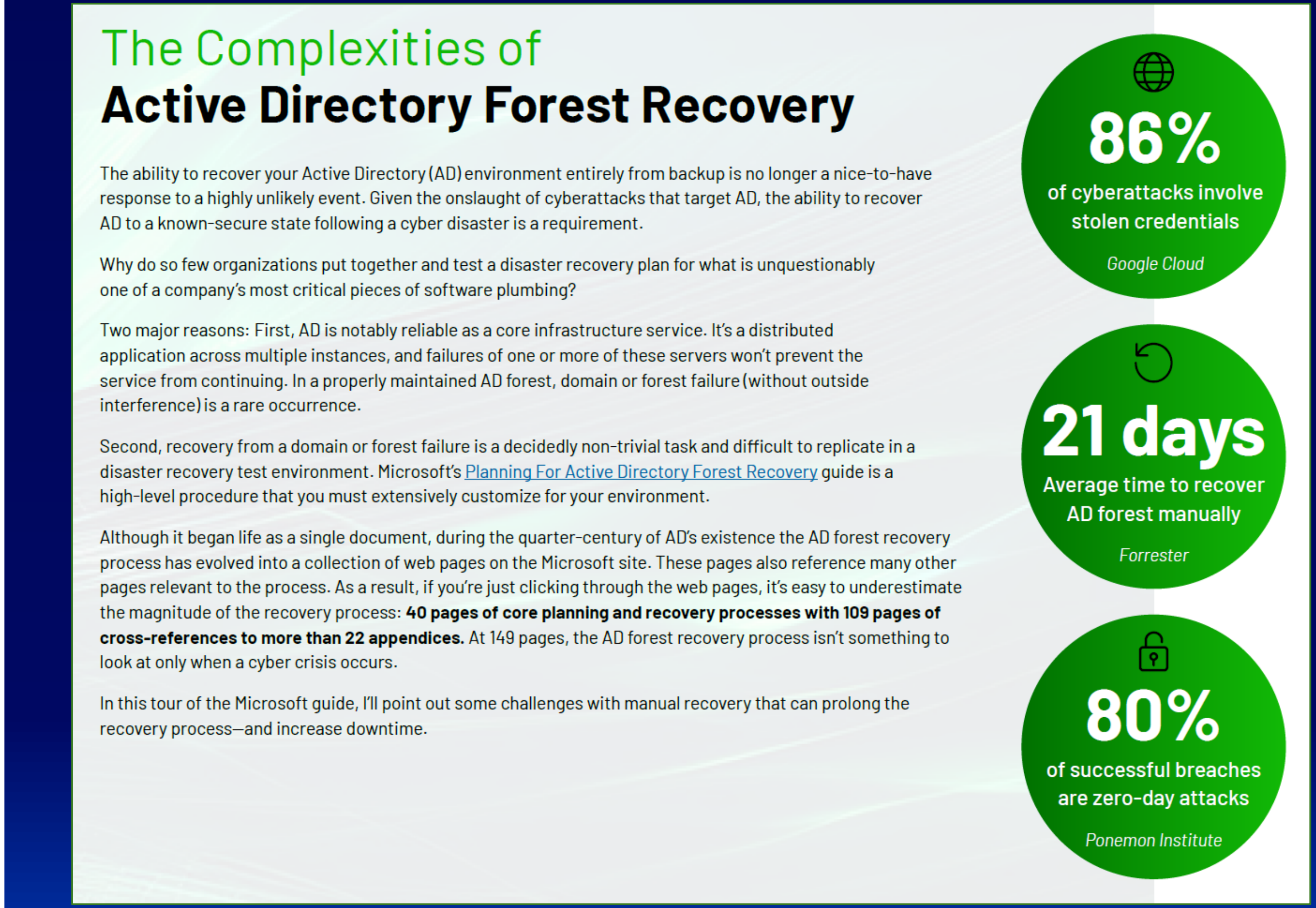
Older operating system guidance is found in the Windows Server archive.

Feedback

→ If you haven’t studied, customized, and tested your own version you’re in for a very rough time.

The “Guide to the Guide”

- Do you really need a guide for a long-established process like Active Directory forest recovery?
- **Yes.**
- My document provides real-world guidance on the recovery process
  - 14 pages
  - 28 different points to consider *before* you execute a forest recovery



The Complexities of Active Directory Forest Recovery

The ability to recover your Active Directory (AD) environment entirely from backup is no longer a nice-to-have response to a highly unlikely event. Given the onslaught of cyberattacks that target AD, the ability to recover AD to a known-secure state following a cyber disaster is a requirement.

Why do so few organizations put together and test a disaster recovery plan for what is unquestionably one of a company's most critical pieces of software plumbing?

Two major reasons: First, AD is notably reliable as a core infrastructure service. It's a distributed application across multiple instances, and failures of one or more of these servers won't prevent the service from continuing. In a properly maintained AD forest, domain or forest failure (without outside interference) is a rare occurrence.

Second, recovery from a domain or forest failure is a decidedly non-trivial task and difficult to replicate in a disaster recovery test environment. Microsoft's Planning For Active Directory Forest Recovery guide is a high-level procedure that you must extensively customize for your environment.

Although it began life as a single document, during the quarter-century of AD's existence the AD forest recovery process has evolved into a collection of web pages on the Microsoft site. These pages also reference many other pages relevant to the process. As a result, if you're just clicking through the web pages, it's easy to underestimate the magnitude of the recovery process: **40 pages of core planning and recovery processes with 109 pages of cross-references to more than 22 appendices.** At 149 pages, the AD forest recovery process isn't something to look at only when a cyber crisis occurs.

In this tour of the Microsoft guide, I'll point out some challenges with manual recovery that can prolong the recovery process—and increase downtime.

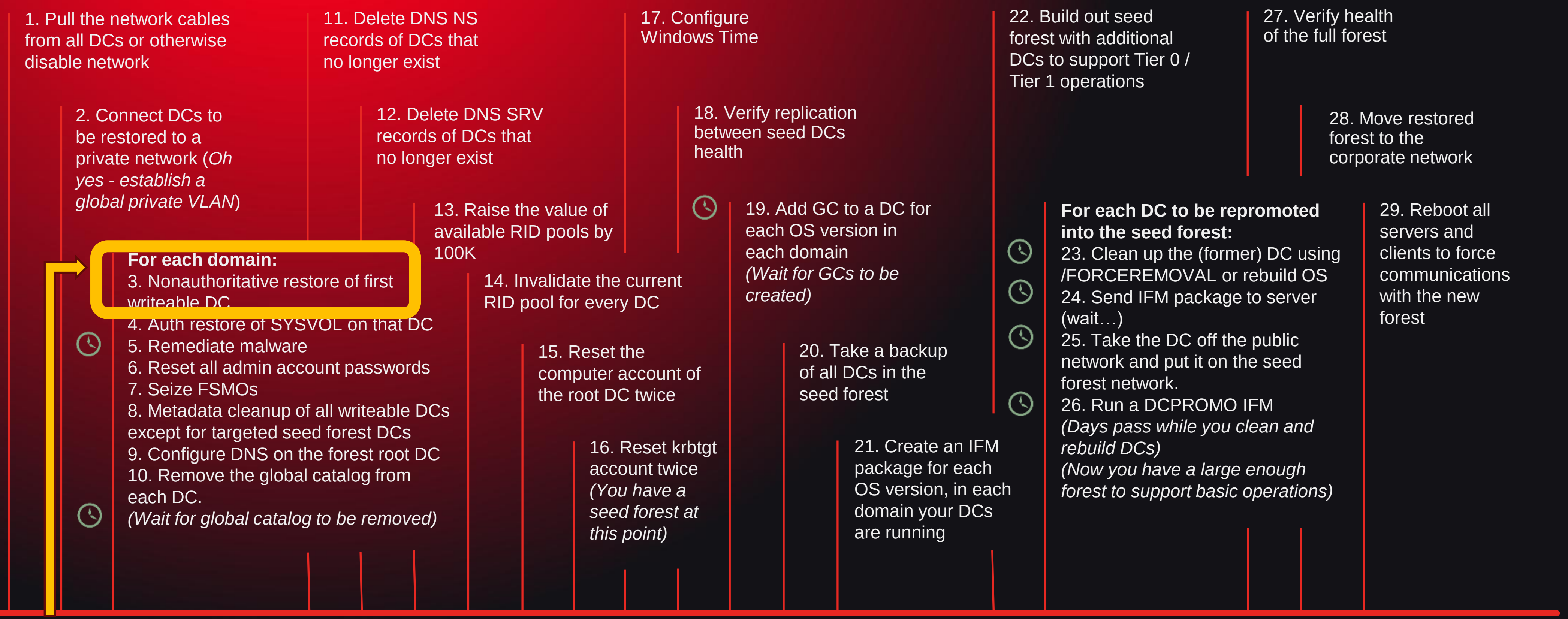
86%
of cyberattacks involve stolen credentials
Google Cloud

21 days
Average time to recover AD forest manually
Forrester

80%
of successful breaches are zero-day attacks
Ponemon Institute

https://www.semperis.com/blog/manual-ad-forest-recovery-problems/

What is Active Directory Forest Recovery?



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 health

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

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

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

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

For each DC to be repromoted into the seed forest:
23. Clean up the (former) DC using /FORCEREMOVAL or rebuild OS
24. Send IFM package to server (wait…)
25. Take the DC off the public network and put it on the seed forest network.
26. Run a DCPROMO IFM
(Days pass 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

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

Important considerations

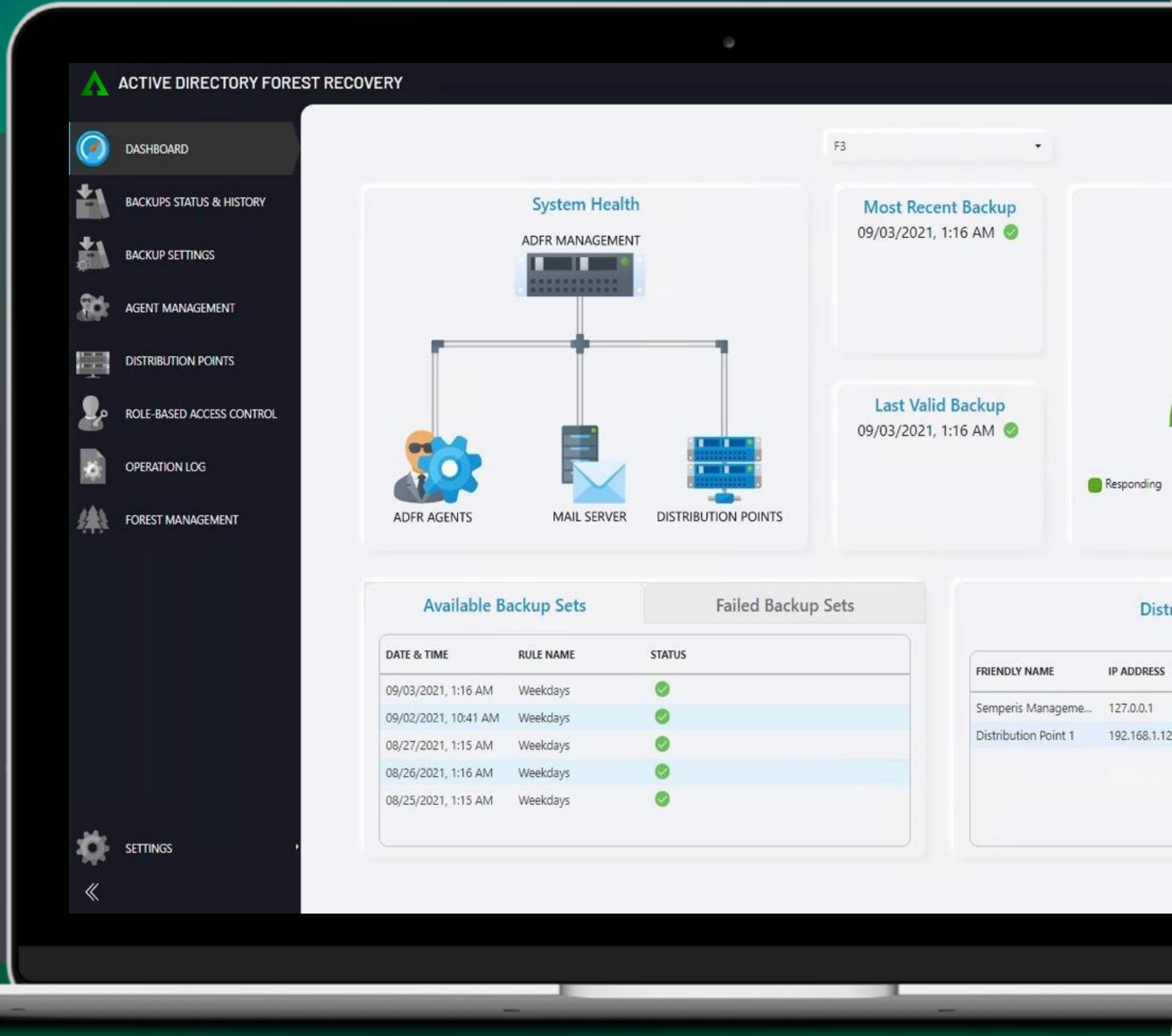
Manual recovery is error-prone and often requires additional cycles to correct missteps, extending the timeline even further

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)

AD FOREST RECOVERY

Shorten forest recovery by 90%

- ✓ Rapid, malware-free recovery
- ✓ Advanced recovery automation
- ✓ Automated Azure Cloud Backup
- ✓ Flexible provisioning for disaster scenarios
- ✓ Post-attack forensics



Most Recent Backup
09/03/2021, 1:16 AM ✓

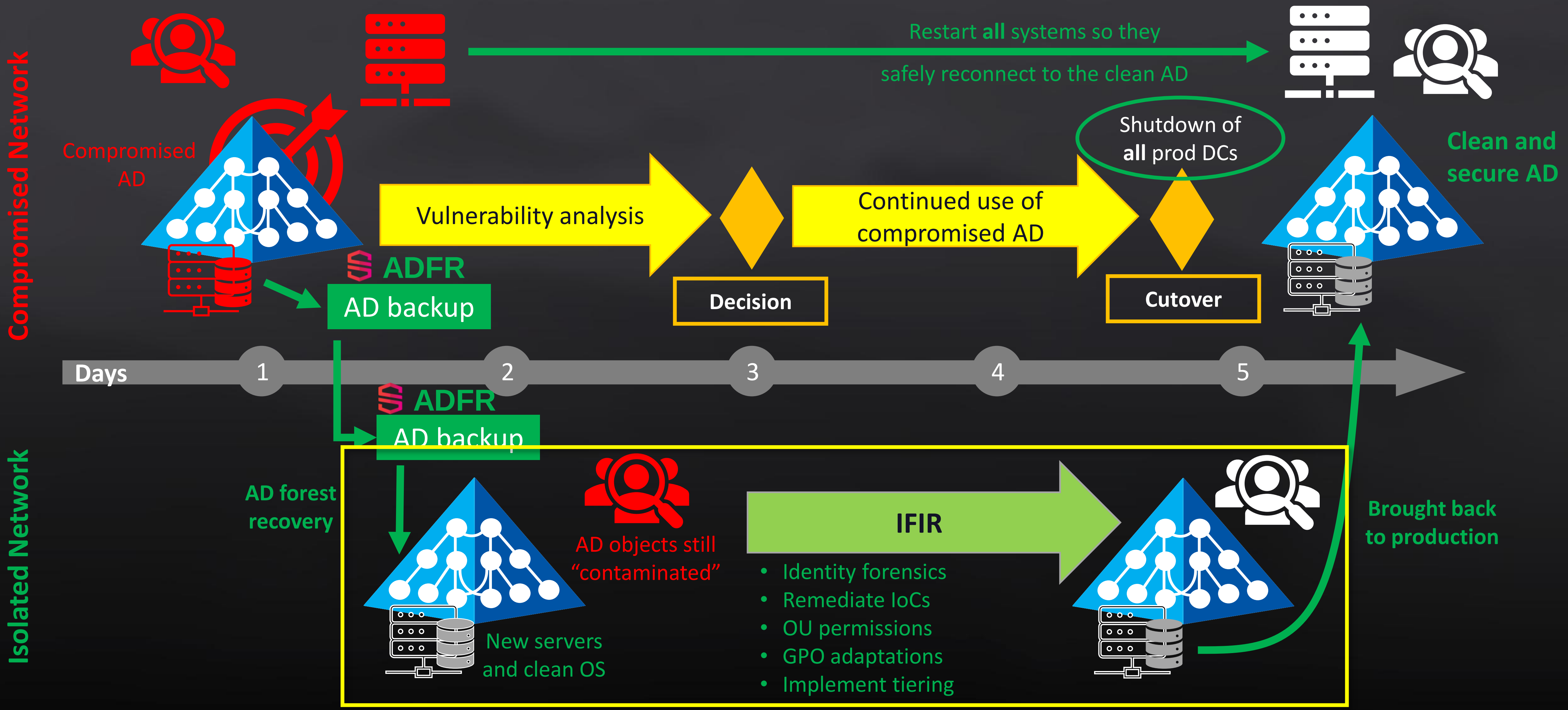
Last Valid Backup
09/03/2021, 1:16 AM ✓

DATE & TIME	RULE NAME	STATUS
09/03/2021, 1:16 AM	Weekdays	✓
09/02/2021, 10:41 AM	Weekdays	✓
08/27/2021, 1:15 AM	Weekdays	✓
08/26/2021, 1:16 AM	Weekdays	✓
08/25/2021, 1:15 AM	Weekdays	✓

FRIENDLY NAME	IP ADDRESS
Semperis Manageme...	127.0.0.1
Distribution Point 1	192.168.1.12

semperis

AD Cyber Recovery Timeline



- Identity forensics
- Remediate IoCs
- OU permissions
- GPO adaptations
- Implement tiering

semperis

IDENTITY UNDER ATTACK:

Cleaning the Recovery Forest

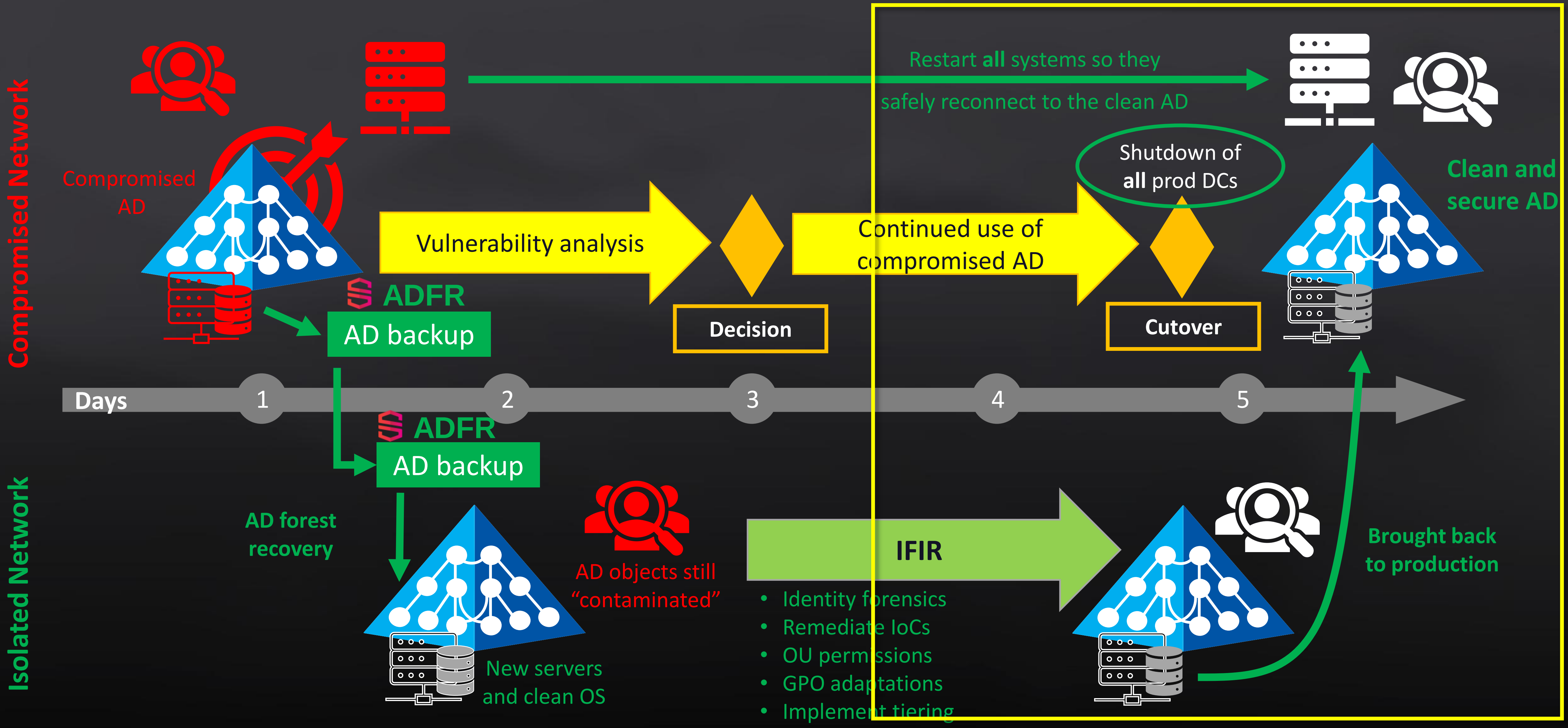
IFIR (Identity Forensics and Incident Response)

You have a recovery forest with clean DCs - *but the service is still untrustworthy*

- Identify and assess persistence mechanisms (backdoors) and hidden threats with Semperis tools and experts
- Remediate threat actor changes, focusing on probable threat actor penetration techniques
- If time, apply security practices such as admin tiering

semperis

AD Cyber Recovery Timeline



Compromised Network

Compromised AD

ADFR

AD backup

Vulnerability analysis

Decision

Continued use of compromised AD

Shutdown of **all** prod DCs

Cutover

Restart **all** systems so they safely reconnect to the clean AD

Clean and secure AD

Days 1 2 3 4 5

Isolated Network

ADFR

AD backup

AD forest recovery

New servers and clean OS

AD objects still “contaminated”

IFIR

- Identity forensics
- Remediate IoCs
- OU permissions
- GPO adaptations
- Implement tiering

Brought back to production

semperis

IDENTITY UNDER ATTACK:

Cutover

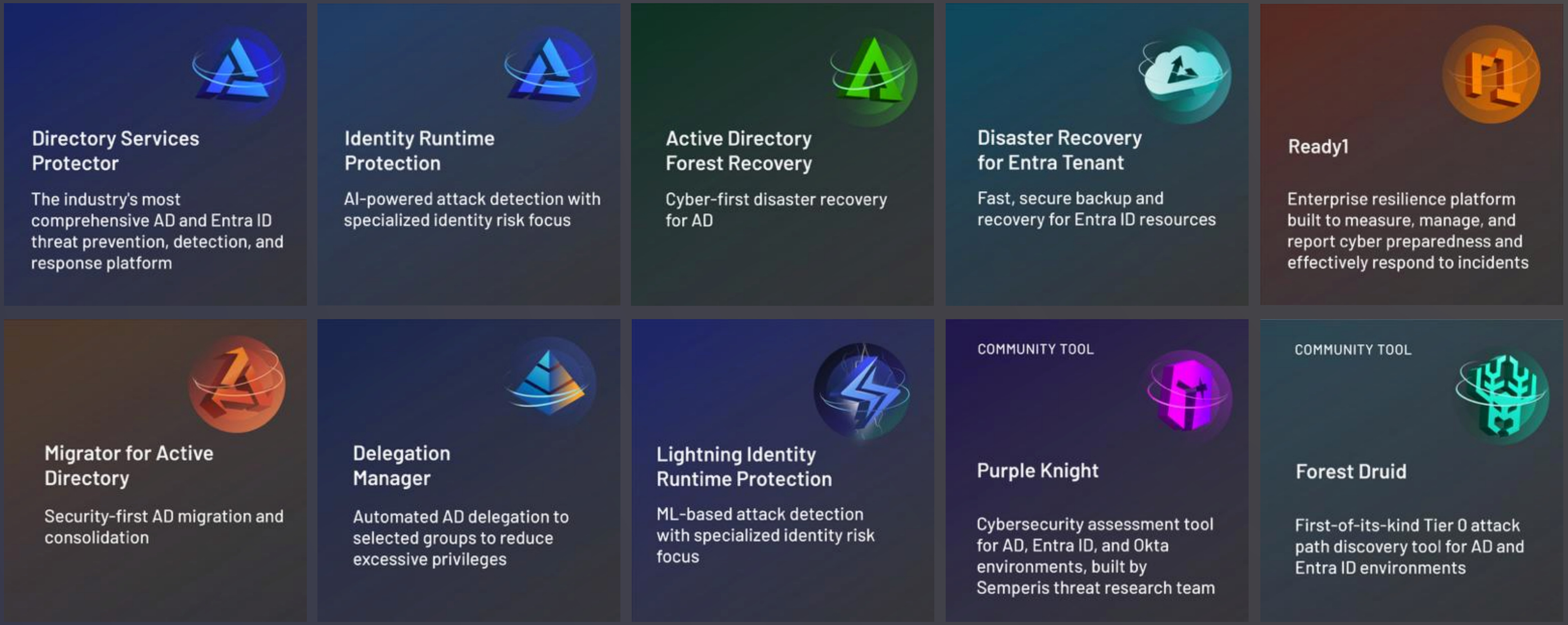
Using the New Forest

1. Shut down existing production forest (!)
2. Update recovery forest DNS to production
3. Open isolated network to production network
4. Register recovery forest DCs in DNS
5. Reboot all domain joined servers and PCs

= Clean Active Directory forest!

semperis

Our Products



Directory Services Protector

The industry's most comprehensive AD and Entra ID threat prevention, detection, and response platform

Identity Runtime Protection

AI-powered attack detection with specialized identity risk focus

Active Directory Forest Recovery

Cyber-first disaster recovery for AD

Disaster Recovery for Entra Tenant

Fast, secure backup and recovery for Entra ID resources

Ready1

Enterprise resilience platform built to measure, manage, and report cyber preparedness and effectively respond to incidents

Migrator for Active Directory

Security-first AD migration and consolidation

Delegation Manager

Automated AD delegation to selected groups to reduce excessive privileges

Lightning Identity Runtime Protection

ML-based attack detection with specialized identity risk focus

COMMUNITY TOOL

Purple Knight

Cybersecurity assessment tool for AD, Entra ID, and Okta environments, built by Semperis threat research team

COMMUNITY TOOL

Forest Druid

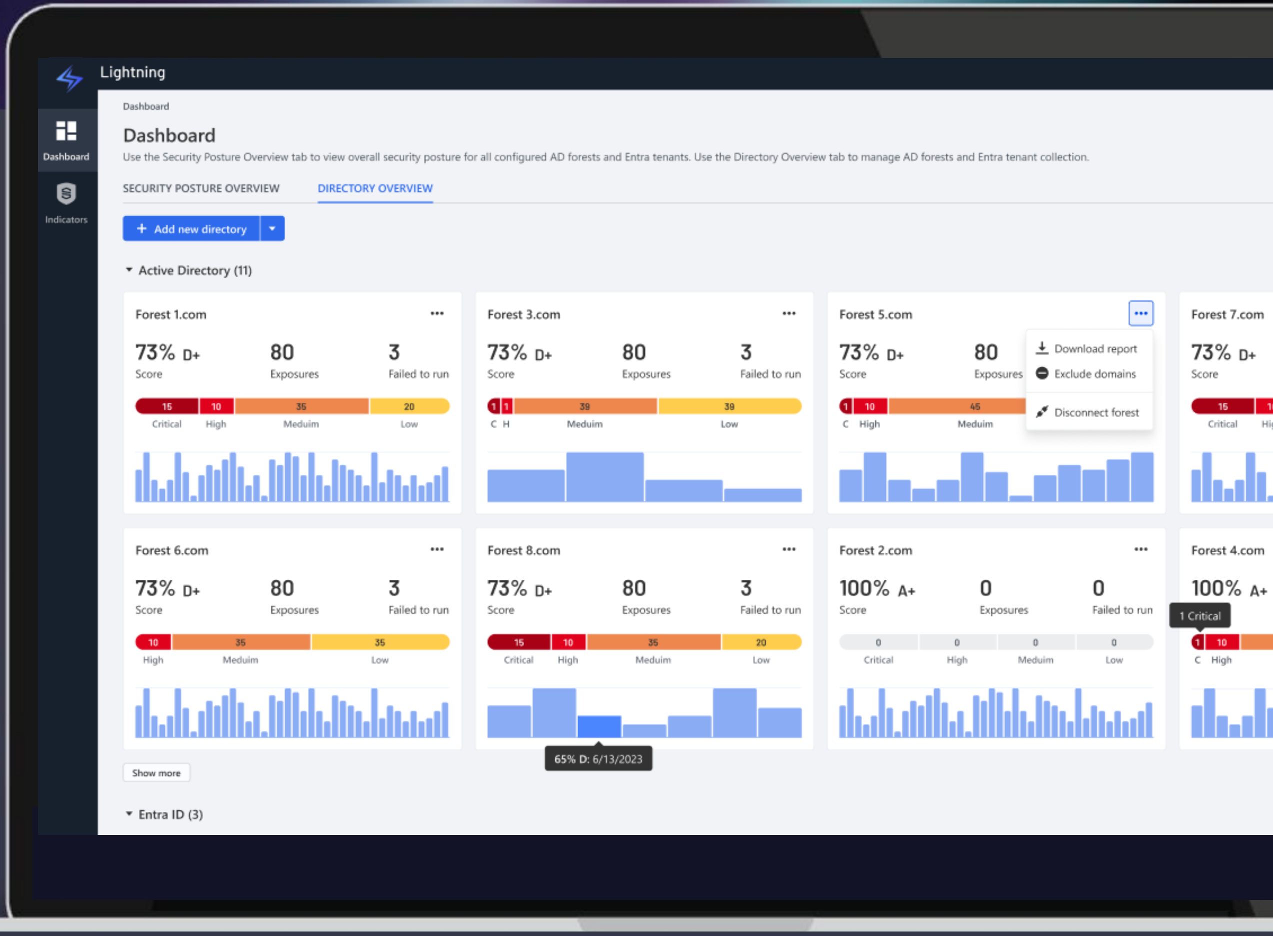
First-of-its-kind Tier 0 attack path discovery tool for AD and Entra ID environments

LIGHTNING INTELLIGENCE

Simple, powerful security posture monitoring

Lack of visibility into security indicators of exposure (IOEs) across hybrid identity environments increases cybersecurity risk for organizations of all sizes.

Lightning Intelligence provides clear security posture insights across hybrid AD and Entra ID environments in an easily deployed SaaS solution to simplify security posture assessments.



Dashboard

Dashboard

Use the Security Posture Overview tab to view overall security posture for all configured AD forests and Entra tenants. Use the Directory Overview tab to manage AD forests and Entra tenant collection.

Active Directory (11)

Forest	Score	Exposures	Failed to run	Critical	High	Meduim	Low
Forest 1.com	73% D+	80	3	15	10	35	20
Forest 3.com	73% D+	80	3	1	1	39	39
Forest 5.com	73% D+	80		1	10	45	
Forest 7.com	73% D+			15			
Forest 6.com	73% D+	80	3		10	35	35
Forest 8.com	73% D+	80	3	15	10	35	20
Forest 2.com	100% A+	0	0	0	0	0	0
Forest 4.com	100% A+			1	10		

Entra ID (3)

- Conduct scheduled and on-demand IOE scanning
- See AD and Entra ID security posture trends and insights in a single dashboard view
- Generate on-demand security posture assessment reports
- Accelerate deployment with no DC agent installation required

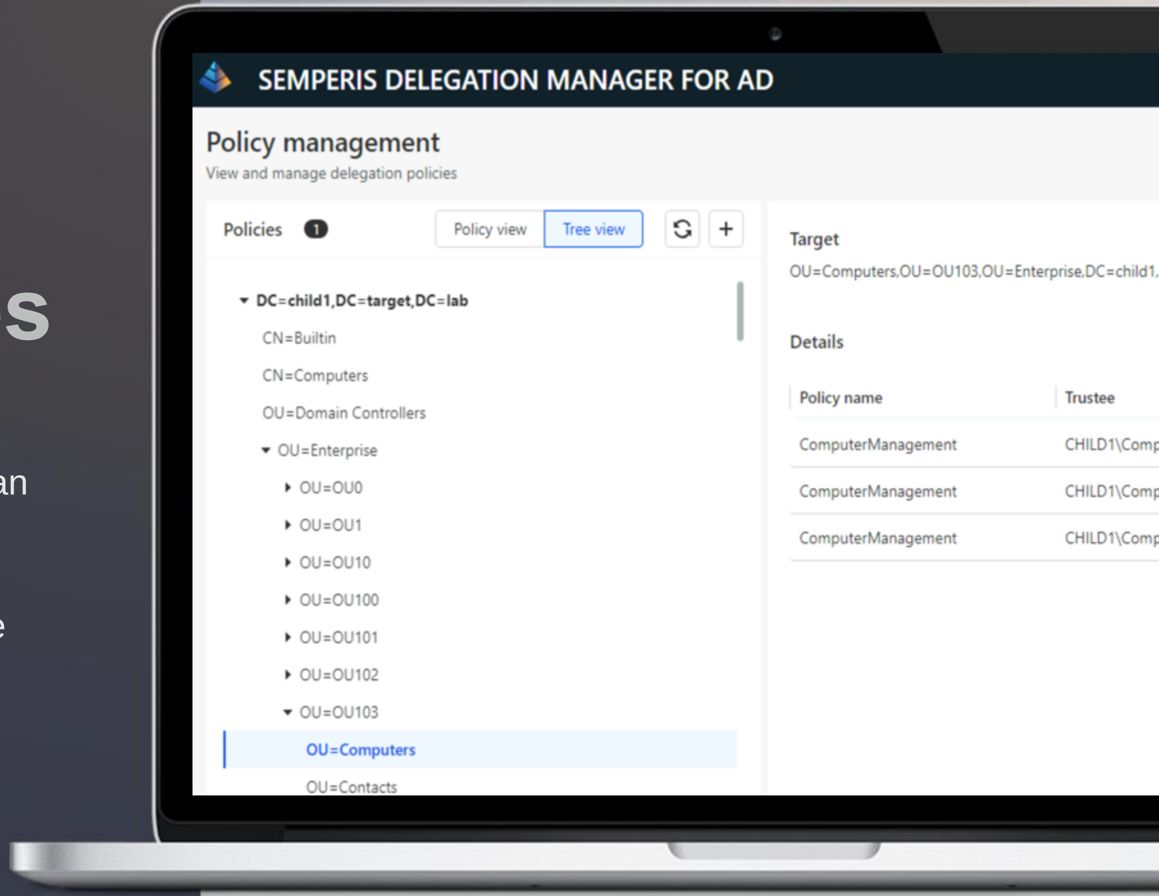
DELEGATION MANAGER FOR AD

Simplify AD delegation to reduce excessive privileges

Cyber attackers routinely exploit AD security vulnerabilities related to over-privileged accounts—and remediating these misconfigurations can be time-consuming and error-prone.

Delegation Manager helps IT teams easily enforce a security-first delegation model to reduce excessive rights while improving response time to user needs.

- Securely delegate administrative privileges
- Seamlessly reinforce policy compliance
- Control access rights with a built-in policy wizard
- See permissions across the directory in a visual dashboard to accelerate remediation



Policy management

View and manage delegation policies

- DC=child1,DC=target,DC=lab
  - CN=Builtin
  - CN=Computers
  - OU=Domain Controllers
  - OU=Enterprise
    - OU=OU0
    - OU=OU1
    - OU=OU10
    - OU=OU100
    - OU=OU101
    - OU=OU102
    - OU=OU103
      - OU=Computers
      - OU=Contacts

Target

OU=Computers,OU=OU103,OU=Enterprise,DC=child1,

Details

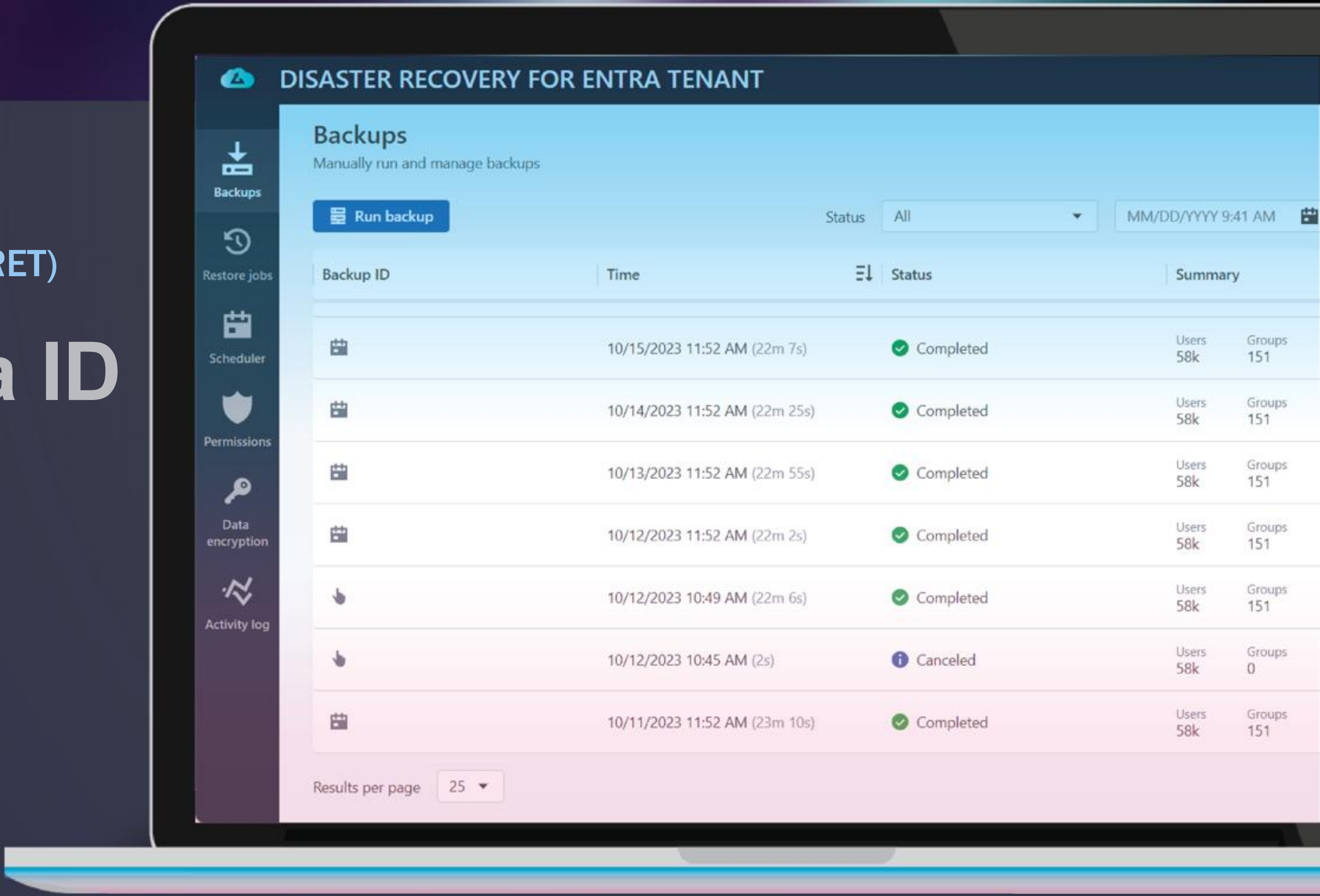
Policy name	Trustee
ComputerManagement	CHILD1\Comp
ComputerManagement	CHILD1\Comp
ComputerManagement	CHILD1\Comp

DISASTER RECOVERY FOR ENTRA TENANT (DRET)

Protect critical Entra ID resources from cyberattacks

Entra ID is home to critical resources that provide authentication and access to cloud-based apps and services.

An unintended change—such as a soft or hard deletion or misconfiguration of Entra ID objects—could cause days or weeks of business disruptions.



Backups

Manually run and manage backups

Backup ID	Time	Status	Summary
	10/15/2023 11:52 AM (22m 7s)	Completed	Users 58k Groups 151
	10/14/2023 11:52 AM (22m 25s)	Completed	Users 58k Groups 151
	10/13/2023 11:52 AM (22m 55s)	Completed	Users 58k Groups 151
	10/12/2023 11:52 AM (22m 2s)	Completed	Users 58k Groups 151
	10/12/2023 10:49 AM (22m 6s)	Completed	Users 58k Groups 151
	10/12/2023 10:45 AM (2s)	Canceled	Users 58k Groups 0
	10/11/2023 11:52 AM (23m 10s)	Completed	Users 58k Groups 151

- Cut downtime by recovering objects the Entra ID Recycle Bin leaves behind
- Recover hard-deleted user objects, security groups, and conditional access policies
- Restore individual objects, bulk restore multiple objects, and compare backups
- Protect Entra ID data with Semperis secure storage (SOC 2, Type II) and encryption options

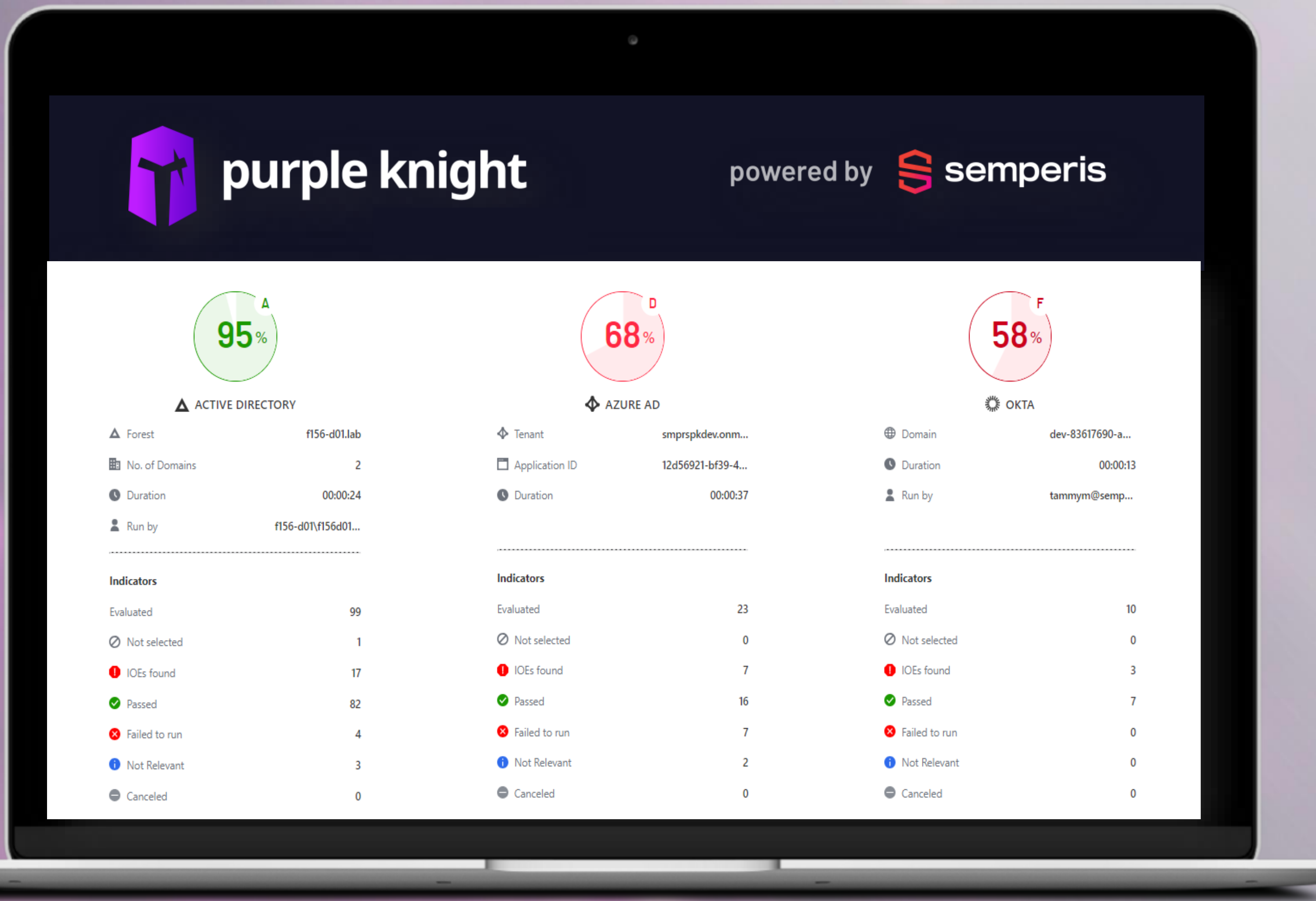
semperis

MEET PURPLE KNIGHT

Spot weaknesses before attackers do

Get the #1 community hybrid AD security assessment tool

- **37,000+** downloads
- **150+** security indicators
- **45%** attack surface reduction
- Recommended by NSA / Five Eyes Security Alliance



purple knight powered by semperis

A 95% ACTIVE DIRECTORY

Forest	f156-d01.lab
No. of Domains	2
Duration	00:00:24
Run by	f156-d01\f156d01...
Indicators	
Evaluated	99
Not selected	1
IOEs found	17
Passed	82
Failed to run	4
Not Relevant	3
Canceled	0

D 68% AZURE AD

Tenant	smprspkdev.onm...
Application ID	12d56921-bf39-4...
Duration	00:00:37
Indicators	
Evaluated	23
Not selected	0
IOEs found	7
Passed	16
Failed to run	7
Not Relevant	2
Canceled	0

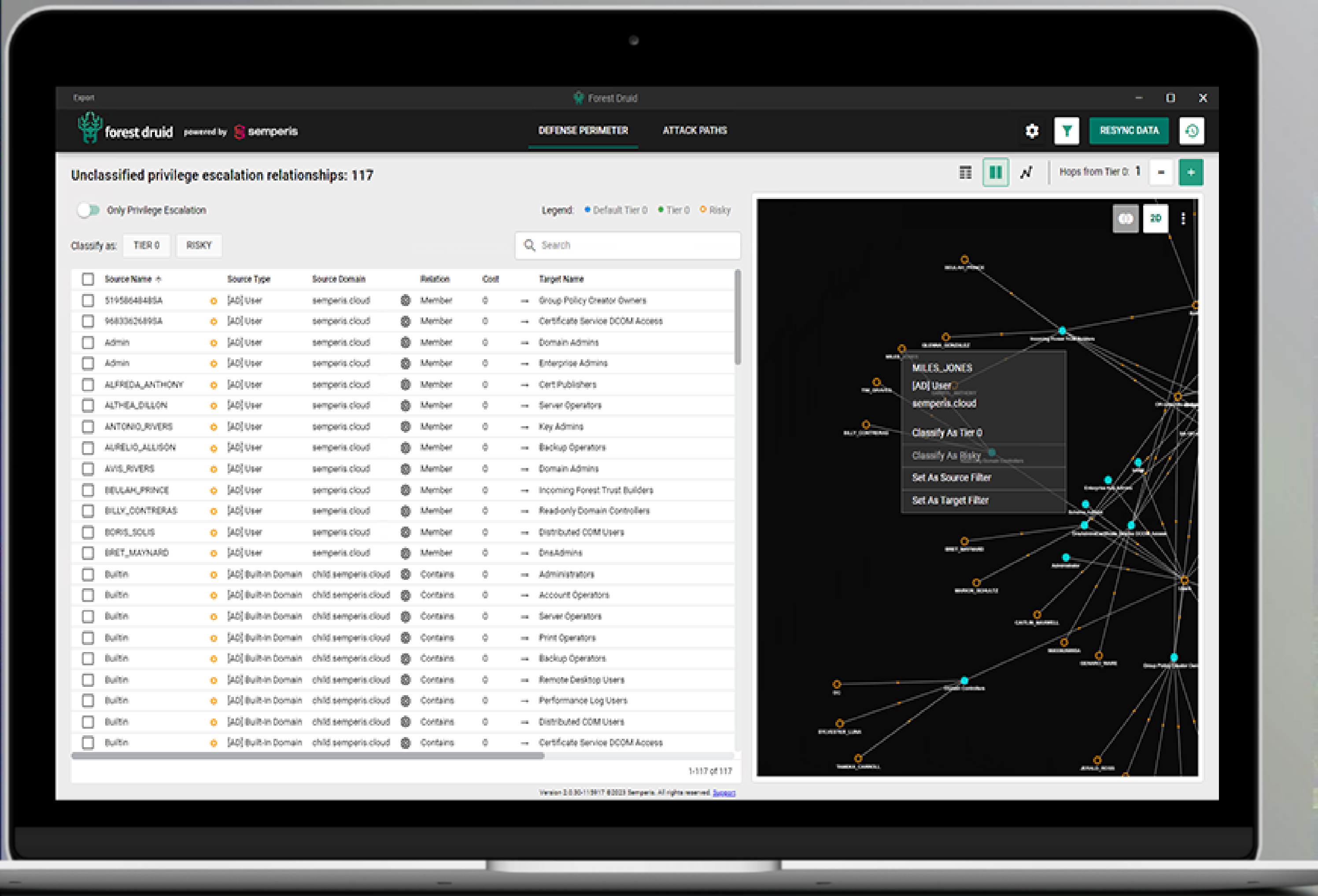
F 58% OKTA

Domain	dev-83617690-a...
Duration	00:00:13
Run by	tammym@semp...
Indicators	
Evaluated	10
Not selected	0
IOEs found	3
Passed	7
Failed to run	0
Not Relevant	0
Canceled	0

MEET FOREST DRUID

Close the paths attackers use to target Tier 0 assets

- Uncover vulnerable Tier 0 assets before it's too late
- Lock down excessive privileges, which create 99% of attack paths into Tier 0 assets
- Discover the most dangerous attack paths—not just the most common ones



Unclassified privilege escalation relationships: 117

Only Privilege Escalation

Legend: ● Default Tier 0 ● Tier 0 ○ Risky

Classify as: TIER 0 RISKY

Search

☐	Source Name	Source Type	Source Domain	Relation	Cost	Target Name
☐	5195864848SA	[AD] User	semperis.cloud	Member	0	Group Policy Creator Owners
☐	9683362689SA	[AD] User	semperis.cloud	Member	0	Certificate Service DCOM Access
☐	Admin	[AD] User	semperis.cloud	Member	0	Domain Admins
☐	Admin	[AD] User	semperis.cloud	Member	0	Enterprise Admins
☐	ALFREDA_ANTHONY	[AD] User	semperis.cloud	Member	0	Cert Publishers
☐	ALTHEA_DILLON	[AD] User	semperis.cloud	Member	0	Server Operators
☐	ANTONIO_RIVERS	[AD] User	semperis.cloud	Member	0	Key Admins
☐	AURELIO_ALLISON	[AD] User	semperis.cloud	Member	0	Backup Operators
☐	AVIS_RIVERS	[AD] User	semperis.cloud	Member	0	Domain Admins
☐	BEULAH_PRINCE	[AD] User	semperis.cloud	Member	0	Incoming Forest Trust Builders
☐	BILLY_CONTRERAS	[AD] User	semperis.cloud	Member	0	Read-only Domain Controllers
☐	BORIS_SOLIS	[AD] User	semperis.cloud	Member	0	Distributed COM Users
☐	BRET_MAYNARD	[AD] User	semperis.cloud	Member	0	DnsAdmins
☐	Builtin	[AD] Built-in Domain	child.semperis.cloud	Contains	0	Administrators
☐	Builtin	[AD] Built-in Domain	child.semperis.cloud	Contains	0	Account Operators
☐	Builtin	[AD] Built-in Domain	child.semperis.cloud	Contains	0	Server Operators
☐	Builtin	[AD] Built-in Domain	child.semperis.cloud	Contains	0	Print Operators
☐	Builtin	[AD] Built-in Domain	child.semperis.cloud	Contains	0	Backup Operators
☐	Builtin	[AD] Built-in Domain	child.semperis.cloud	Contains	0	Remote Desktop Users
☐	Builtin	[AD] Built-in Domain	child.semperis.cloud	Contains	0	Performance Log Users
☐	Builtin	[AD] Built-in Domain	child.semperis.cloud	Contains	0	Distributed COM Users
☐	Builtin	[AD] Built-in Domain	child.semperis.cloud	Contains	0	Certificate Service DCOM Access

1-117 of 117

Version 2.0.30-113917 ©2023 Semperis. All rights reserved. Support

semperis

DOMAIN EXPERTISE

130+ years Microsoft MVP experience

260+ years Microsoft corporate support experience

800+ years identity-related experience

No vendor or services provider can outmatch Semperis' collective Microsoft MVP experience in **Directory Services and Group Policy**

The team behind Purple Knight

Purple Knight is a free AD cybersecurity assessment tool built and managed by Semperis' threat research team

The team behind Forest Druid

Forest Druid is a first-of-its-kind Tier 0 attack path discovery tool for Active Directory environments

Hybrid Identity thought leaders

Semperis hosts the award-winning Hybrid Identity Protection conference and podcast series

semperis

THANK YOU

Questions?

CONTACT INFORMATION:

Jimmy McNary (VP Federal) jimmym@semperis.com

Sean Deuby (Principal Technologist) seand@semperis.com

Chris Ingle (Senior Solutions Architect) chrisi@semperis.com

Anne Morgan (Federal Sales) annem@semperis.com

KKR

INSIGHT PARTNERS

Microsoft Partner

Enterprise Cloud Alliance
Microsoft Accelerator Alumni
Microsoft Co-Sell
Microsoft Intelligence Security Association (MISA)

Inc. 5000 America's Fastest-Growing Private Companies

TOP 5 FASTEST-GROWING CYBERSECURITY COMPANIES

500 Technology Fast 500 2023 NORTH AMERICA Deloitte.

4 YEARS IN A ROW OF DOUBLE-DIGIT GROWTH

FORTUNE CYBER 60

NAMED TO FORTUNE'S CYBER 60 2024 LIST

Inc. Best Workplaces 2024

3 CONSECUTIVE YEARS ON THE LIST

dun's 100

#14 ON DUN'S 100 2022 RANKING OF BEST STARTUPS

MVP

150+ COMBINED YEARS OF MICROSOFT MVP EXPERIENCE

EY Entrepreneur Of The Year 2023 Award Winner

EY HONORS SEMPERIS CEO MICKEY BRESMAN

Inc. 5000 Vet100 2022 IVMF

TOP 10 OF US 100 FASTEST-GROWING VETERAN-OWNED BUSINESSES