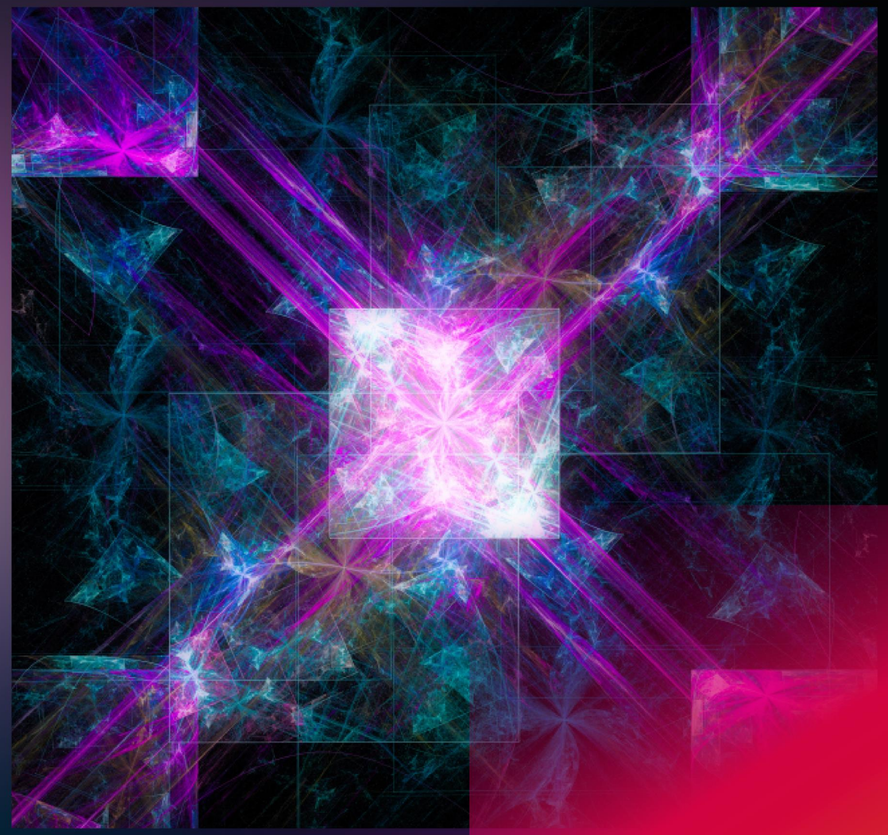
semperis

"Back from hell“
Das Identity Immunsystem



Severin Kopinski
Enterprise Sales Director

semperis

Stephane Nappo

"Anstatt Cyberangriffe zu fürchten oder zu ignorieren, sollten Sie dafür sorgen, dass Sie gegen sie gewappnet sind."

semperis


RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
CYBERSECURITY
FRAMEWORK
VERSION 1.1

semperis

10 000 000 000 000

semperis

10 000 000 000 000 $

semperis

> ***Nine days for an Active Directory recovery isn't good enough, you should aspire to 24 hours; if you can't, then you can't repair anything else.***

ANDY POWELL, MAERSK CISO

semperis

Was sagen die Nachrichten?

Survey Finds Active Directory Outages on the Rise

- Redmond 02/2024

Japan's Space Program at Risk After Microsoft Active Directory Breach

- Dark Reading 12/2023

The Change Healthcare attack: Explaining how it happened

- Tech Target 03/2024

AD-Instanz von NRWs Schulministerium ungesichert im Netz

- Golem 04/2023

semperis

Warum wird das AD angegriffen?

1) **Ziel für Angreifer:** Active Directory (AD) enthält wichtige Informationen und ist ein zentrales Ziel für Angriffe.
2) **Schwere Folgen:** AD-Kompromittierung kann zu Datenverlust, Ransomware, Privilegieneskalation und dauerhaften Bedrohungen führen.
3) **Angriffsmethoden und -tools:** Häufige Angriffe sind Phishing, Brute-Force und Passwort-Spraying; genutzte Tools sind Mimikatz, BloodHound, PowerShell Empire, Cobalt Strike und andere.
4) **Schwachstellen:** Schwache Passwörter, komplexe Infrastruktur, mangelnde Überwachung und veraltete Benutzerkonten machen AD anfällig.
5) **Passwortsicherheit:** Schwache und wiederverwendete Passwörter sind leicht angreifbar.
6) **Unzureichende Überwachung:** Fehlende Überwachungswerkzeuge und schlecht verwaltete Benutzerkonten erhöhen das Risiko.

semperis

WIE SCHNELL BRINGEN SIE AD ZURÜCK?

- Nur 37 % der Unternehmen sind sich der Komplexität der Wiederherstellung von Forests bewusst

- Mehr als 50 % der Befragten haben ihren AD-Wiederherstellungsprozess noch nie getestet –

  oder haben nicht einmal einen ausgearbeitet

semperis

What does it take to manually perform an Active Directory forest recovery?

Days to weeks…

1. Pull the network cables from all DCs or otherwise disable network

2. Connect DCs to be restored to a private network (*Oh yes - establish a global private VLAN*)

For each domain:

3. Nonauthoritative restore of first writeable DC
4. Auth restore of SYSVOL on that DC
5. Remediate malware
6. Reset all admin account passwords
7. Seize FSMOs
8. Metadata cleanup of all writeable DCs except for targeted seed forest DCs
9. Configure DNS on the forest root DC
10. Remove the global catalog from each DC.

(Wait for global catalog to be removed)

11. Delete DNS NS records of DCs that no longer exist

12. Delete DNS SRV records of DCs that no longer exist

13. Raise the value of available RID pools by 100K

14. Invalidate the current RID pool for every DC

15. Reset the computer account of the root DC twice

16. Reset krbtgt account twice *(You have a seed forest at this point)*

17. Configure Windows Time

18. Verify replication between seed DCs

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

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

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

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

For each DC to be repromoted into the seed forest:

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

(Days pass while you clean and rebuild DCs)

(Now you have a large enough forest to support basic operations)

27. Verify health of the full forest

28. Move restored forest to the corporate network

29. Reboot all servers and clients to force communications with the new forest

Semperis' five-click automated AD recovery:

1. Login to console
2. Click **Forest Recovery**
3. Choose backup set to recover from
4. Click **Analyze**
5. Click **Recover**

Compare to:

Semperis' AD Forest Recovery

Minutes to hours…

Semperis orchestrates a fully automated forest recovery process—avoiding human errors, reducing downtime by 90%, and eliminating the risk of malware reinfection.

Important considerations

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

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

Required staff for manual AD forest recovery:
Core AD team, operators at every datacenter, plus other external support (Estimated 10-15 IT support staffers in average enterprise)

Required staff for Semperis' ADFR:
Only 1-2 AD admins

Finden Sie Schwachstellen in Ihrem Active Directory und Entra ID bevor es Angreifer tun!

Sichern Sie sich die Nummer 1 unter den AD-Sicherheitstools.
Laden Sie Purple Knight kostenlos herunter.

- Über **23.000** Downloads weltweit
- Mehr als **150** Sicherheitsindikatoren
- Zeigt offene Schwachstellen im AD auf
- Komplett kostenfrei und offli e nutzbar

semperis.com/de/purple-knight

KOSTENLOSEN DOWNLOAD ANFORDERN

SECURITY POSTURE OVERVIEW

This report summarizes the security assessment results performed in your hybrid identity environment on 09/08/22 by Semperis' Active Directory security assessment tool, Purple Knight. Depending on the environments selected for evaluation, the report includes the assessment results for an Active Directory forest, an Azure AD tenant, or both.
Active Directory forest: Purple Knight queried the Active Directory environment and ran a series of security indicator scripts against domains within the selected forest (see Appendix 1 – Domains list for a full list of the domains included in the assessment).

Azure AD tenant: Purple Knight queried the selected Azure AD tenant focusing on some of the most common attack vectors that threat actors use to gain access to the Azure AD environment.
The report provides an overall security risk score as well as detailed results about each Indicator of Exposure (IOE) found. By uncovering Active Directory and Azure AD security weaknesses, this assessment report provides valuable insight into the overall security posture across your hybrid identity environment and presents opportunities to minimize the attack surface and stay ahead of the ever-changing threat landscape.

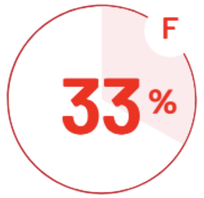
View Appendix 1 - Domains list

ACTIVE DIRECTORY

Forest	**dsplab.ca**
No. of Domains	**1**
Duration	**00:00:14.1839101**
Run by	**DSPLAB\administrator**

Indicators

Evaluated	**97**
Not selected	**1**



AZURE AD

Tenant	**dsplabca**
Application ID	**482596b2-6548-43c0-b8ba-3feb5eaa508b**
Duration	**00:00:05.6453624**
Run by	**DSPLAB\administrator**

Indicators

Evaluated	**11**
Not selected	**0**

CRITICAL IOEs FOUND

Evidence of Mimikatz DCShadow attack

DCShadow attacks enable attackers that have achieved privileg..

Read More...

Inheritance enabled on AdminSDHolder object

This indicator checks for inheritance being enabled on the Acce..

Read More...

krbtgt account with Resource-Based Constrained Delegation (RBCD) enabled

It is possible to create a Kerberos delegation on the krbtgt acco.

Read More...

Non-default principals with DC Sync rights on the domain

Any security principals with Replicate Changes All and Replicate..

Read More...

Permission changes on AdminSDHolder object

This indicator looks for Access Control List (ACL) changes on th..

Read More...

Print spooler service is enabled on a DC

This indicator scans Domain Controllers for a running print spo..

Read More...

Privileged Users with Weak Password Policy

This indicator looks for privileged users in each domain that do..

Read More...

ACTIVE DIRECTORY RESULTS

Categories

F
55%

ACCOUNT SECURITY

Account Security indicators pertain to security weaknesses on individual accounts--built-in or

Read More ...

F
58%

AD DELEGATION

AD delegation is a critical part of security and compliance. By delegating control over Active

Read More ...

C
75%

AD INFRASTRUCTURE SECURITY

AD Infrastructure Security indicators pertain to the security configuration of core parts of AD's

Read More ...

D
61%

GROUP POLICY SECURITY

Group Policy Security indicators pertain to the security configuration of GPOs and their

Read More ...

F
27%

KERBEROS SECURITY

Kerberos Security indicators pertain to the configuration of Kerberos capabilities on computer

Read More ...

SECURITY INDICATOR

Built-in domain Administrator account used within the last two weeks

IOE Found

F
0 %

SEVERITY
Warning

WEIGHT
5

Security Frameworks

MITRE ATT&CK

Credential Access

MITRE D3FEND

Detect - Credential Compromise Scope Analysis

Harden - Strong Password Policy

Description

The Domain Administrator account should only be used for initial build activities and, when necessary, disaster recovery. This indicator checks to see if the lastLogonTimestamp for the built-in Domain Administrator account has been updated within the last two weeks. If so, it could indicate that the user has been compromised.

Likelihood of Compromise

If best practices are followed and domain Admin is not used, this would indicate a compromise. Ensure any logins to the built-in Domain Administrator account are legitimate and accounted for. If not accounted for, a breach is likely and should be investigated.

Result

Found 1 domains in which the built-in administrator was used recently.

DistinguishedName	EventTimestamp
CN=Administrator,CN=Users,DC=dsplab,DC=ca	9/2/2022 9:07:41 PM

Showing 1 of 1

Remediation Steps

Ensure that the built-in domain Administrator account is not used regularly and has a complex password known only to highly privileged admins.

Stop chasing Active Directory attack paths.

Focus resources where it matters most: your Tier 0 perimeter.

Download Forest Druid.

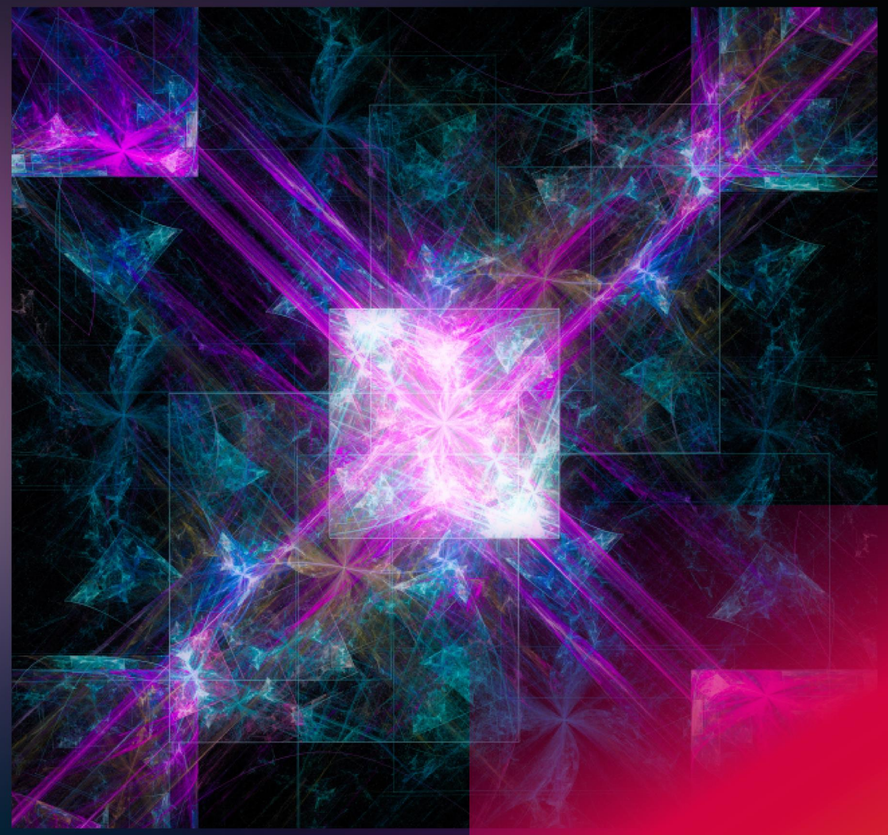
- Lock down excessive privileges
- Prioritize attack paths leading into the Tier 0 perimeter
- Made by the identity security experts

Request FREE access

purple-knight.com/forest-druid

semperis

Danke!



Severin Kopinski

Enterprise Sales Director