semperis

Why Active Directory is the prime cyberattack target

… and what to do about it!

Guido Grillenmeier

Semperis Principal Technologist

12 Years Microsoft MVP

guidog@semperis.com

www.linkedin.com/in/guidogrillenmeier

SIKKERHETS FESTIVALEN

August 30, 2023
Lillehammer

WhoAMi

Guido Grillenmeier

Semperis Principal Technologist EMEA

1996

2003 – 2015

2015

2018

2021

hp invent

Microsoft MVP Most Valuable Professional

Category: Directory Services

Hewlett Packard Enterprise

DXC.technology

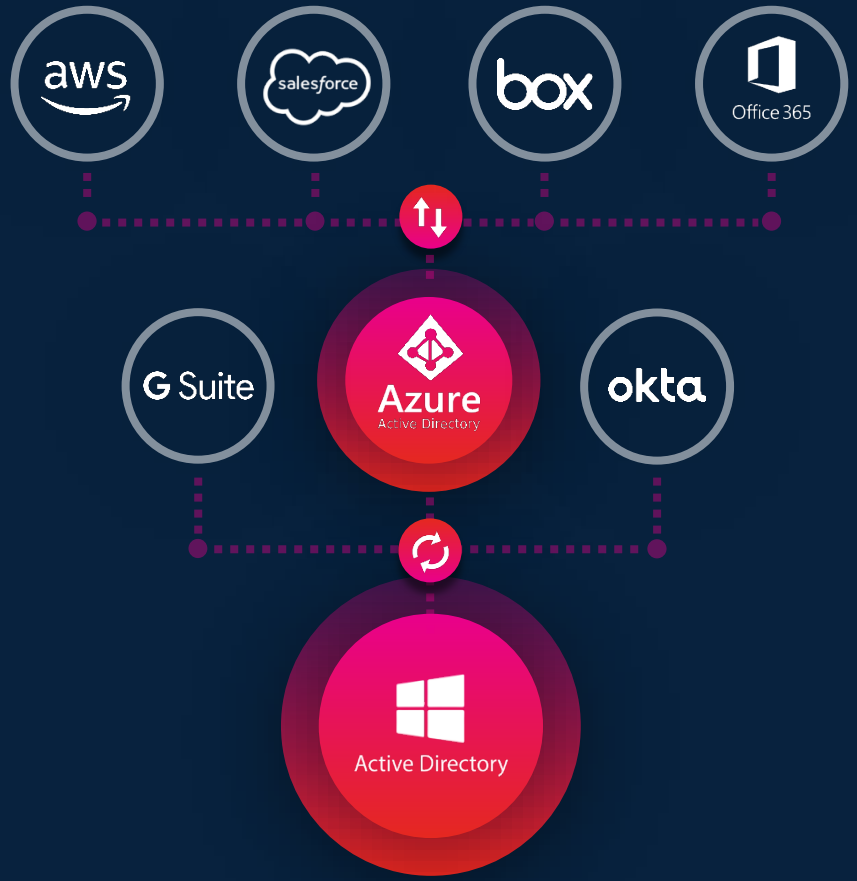
semperis

semperis

KEYS TO THE KINGDOM

If Active Directory isn't secure, nothing is

- 80% of all breaches involve credential abuse
- Systemic 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

Password attacks every second (2021)

***Source**: Alex Weinert, VP of Identity Security, Microsoft*

Password attacks every second (2023)

***Source**: Alex Weinert, VP of Identity Security, Microsoft*

semperis

#1 NEW TARGET

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

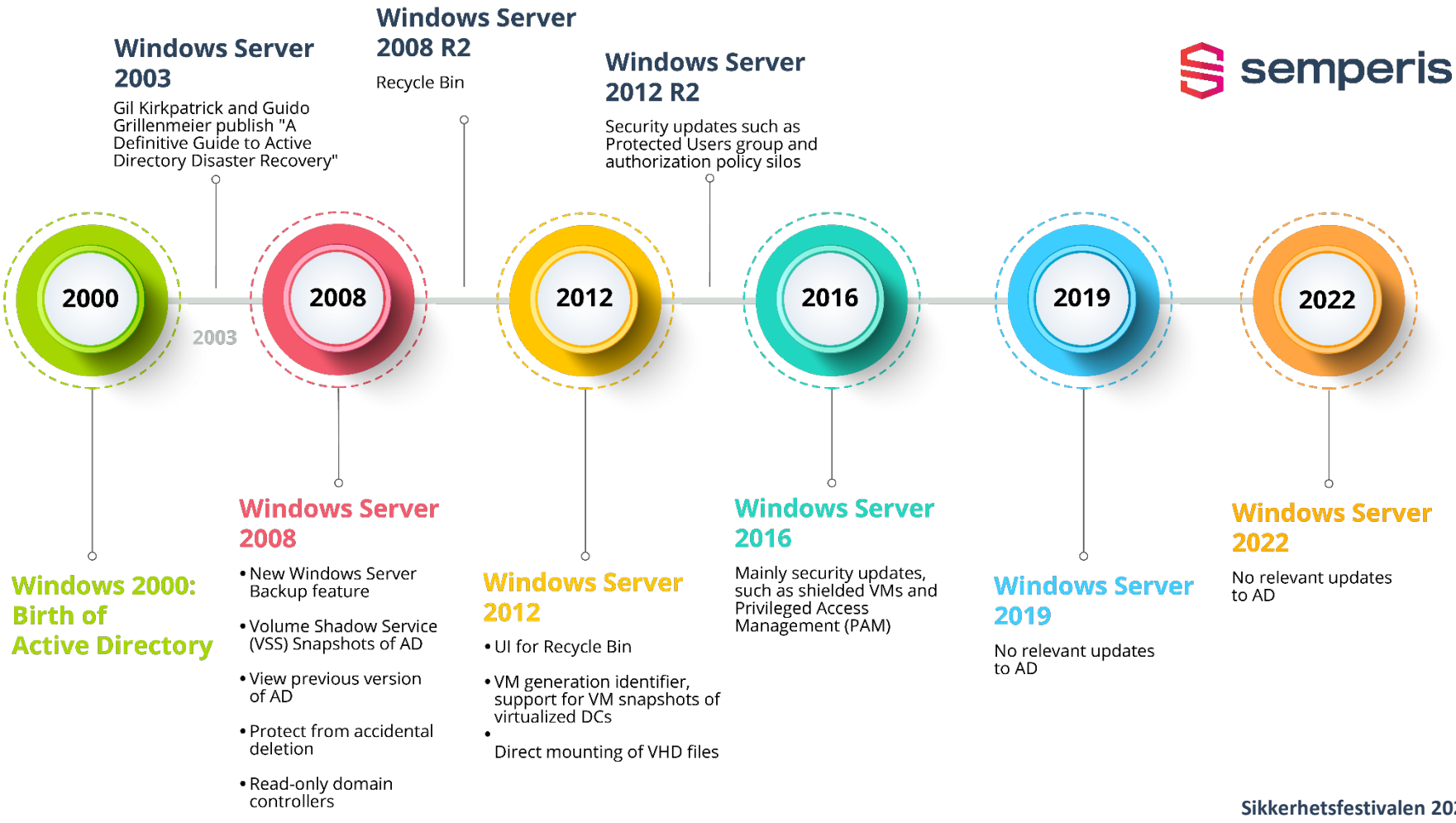
- Mandiant

MICROSOFT EXCHANGE

SOLARWINDS

NTT COMMUNICATIONS

MAERSK


Windows Server 2003
Gil Kirkpatrick and Guido Grillenmeier publish "A Definitive Guide to Active Directory Disaster Recovery"
Windows Server 2008 R2
Recycle Bin
Windows Server 2012 R2
Security updates such as Protected Users group and authorization policy silos
2000
2003
2008
2012
2016
2019
2022
Windows 2000: Birth of Active Directory
Windows Server 2008
• New Windows Server Backup feature
• Volume Shadow Service (VSS) Snapshots of AD
• View previous version of AD
• Protect from accidental deletion
• Read-only domain controllers
Windows Server 2012
• UI for Recycle Bin
• VM generation identifier, support for VM snapshots of virtualized DCs
• Direct mounting of VHD files
Windows Server 2016
Mainly security updates, such as shielded VMs and Privileged Access Management (PAM)
Windows Server 2019
No relevant updates to AD
Windows Server 2022
No relevant updates to AD

semperis

Phases of a Ransomware-Attack

semperis

Initial Access

- Phishing emails
- Malicious websites
- Targeted attacks with **stolen credentials**

BYOVD

Post Exploit

- Download of malware for **Recon-Phase**
- Connection to C2* systems
- Remote connection established

Reconnaissance

- Evaluation of **AD vulnerabilities** to gain domain-dominance
- Lateral movement to other systems
- Credential harvesting and privilege escalation

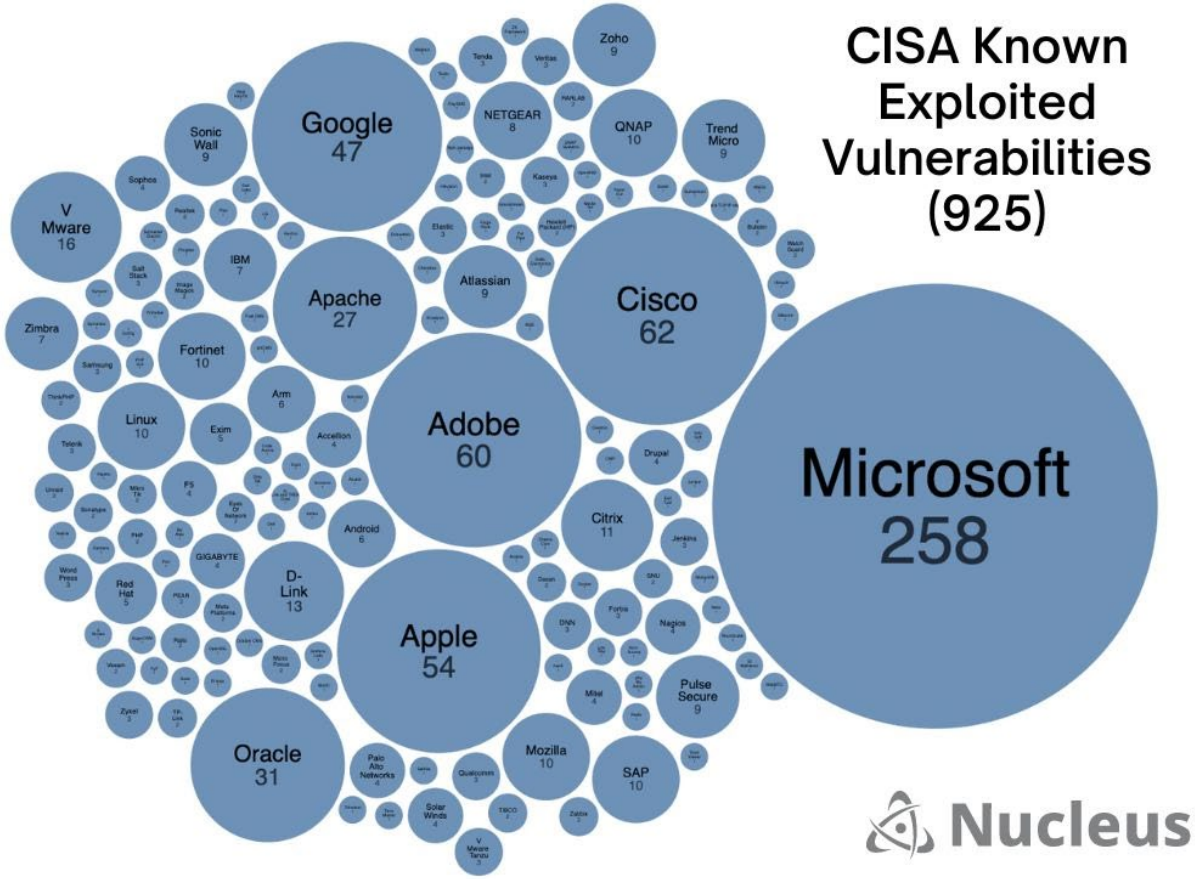
Core attack

- Access to and Extraction of core-business data
- Encryption of devices, often **including AD DCs**

* C2 = Command-and-Control

IN → THROUGH → OUT

KEV – Known Exploited Vulnerabilities



Are you sure all your apps and drivers are properly patched?

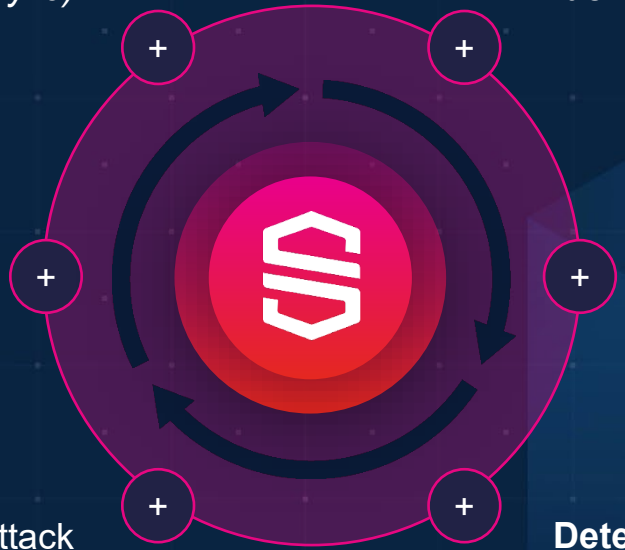
Source: Patrick Garrity from Nucleus, May 8, 2023

semperis

NIST Cybersecurity Framework

(Validate & Analyze)

Identify: the risk



Recover: from the attack

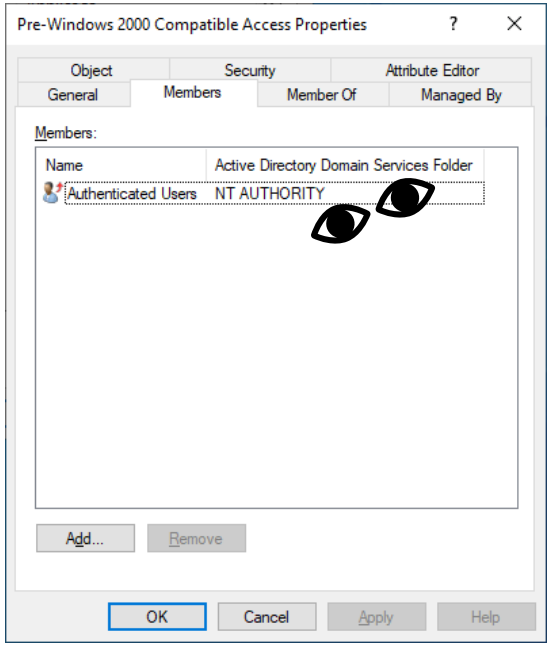
Protect: the service

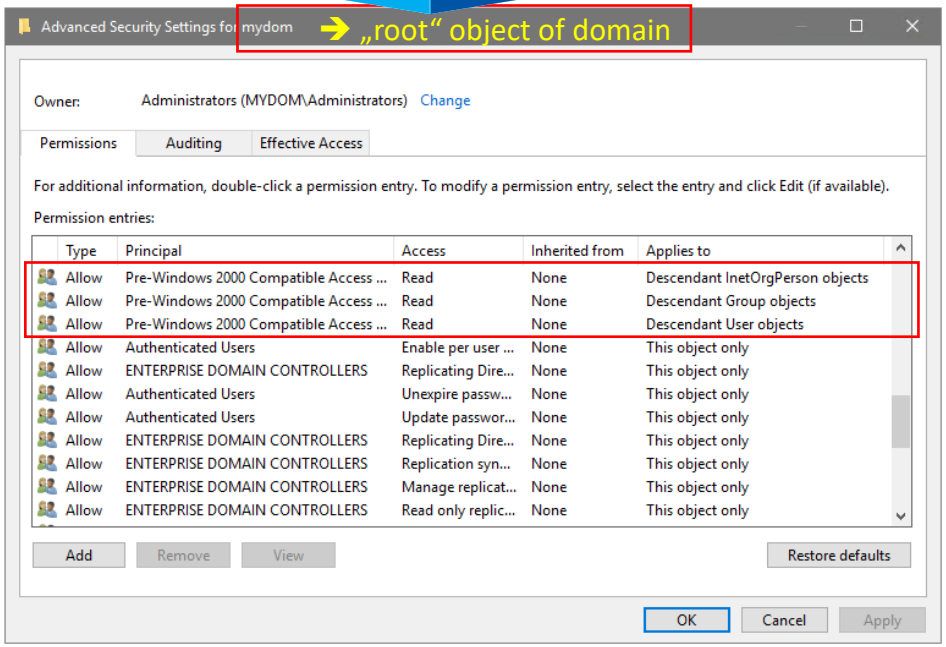
Respond: to the attack

Detect: the attack

Default Read-Permissions in AD

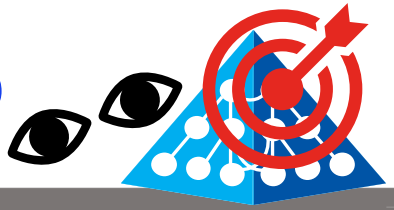
semperis



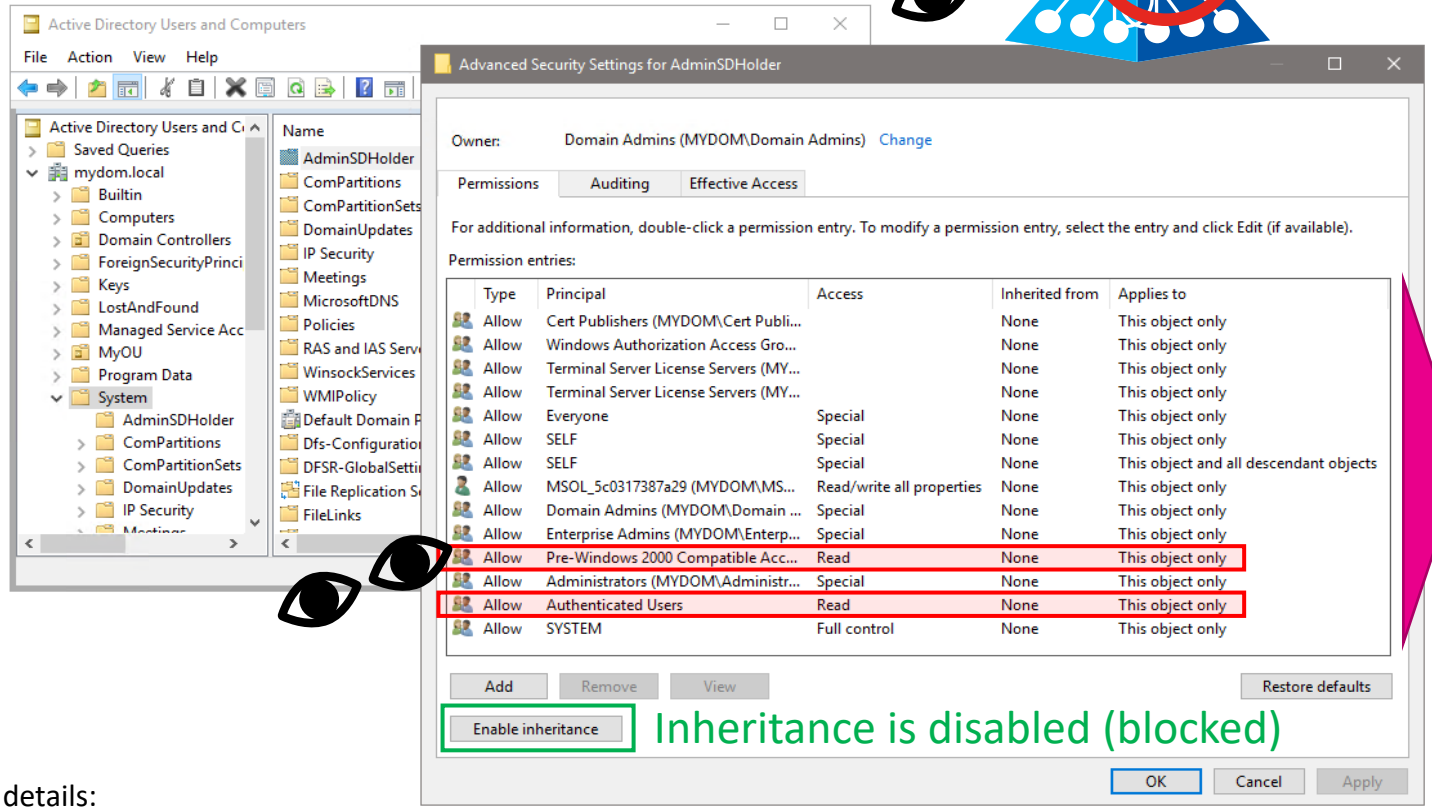


Details on the issues caused by this and why you should adjust it can be found on the Semperis BLOG
https://www.semperis.com/blog/security-risks-pre-windows-2000-compatibility-windows-2022

Default Read-Permissions in AD



semperis



AdminSDHolder

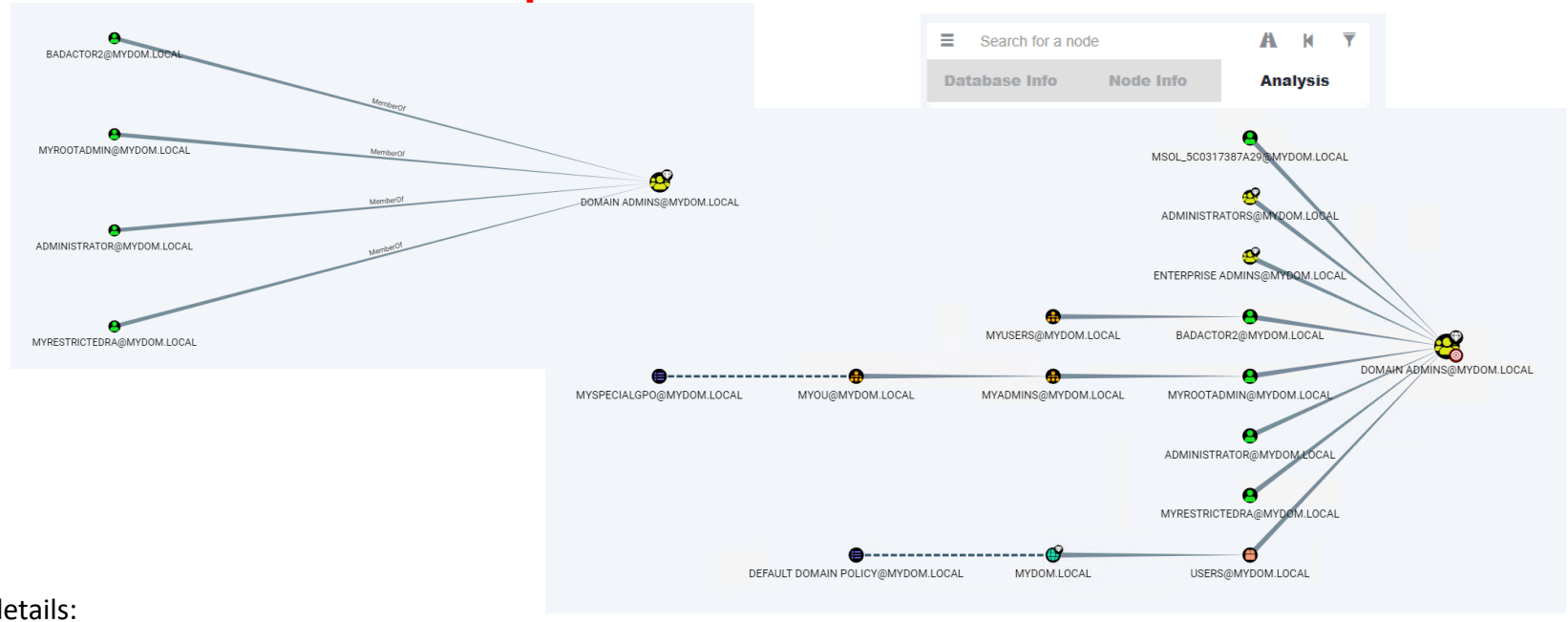
These permissions are “stamped” periodically on all your privileged groups and users (!)

More details:
https://www.semperis.com/resources/improving-your-active-directory-security-posture-adminsdholderto-the-rescue

Locking down permissions in AD will help!

Intruders often use Sharphound/Bloodhound for the initial reconnaissance of attack-paths to your AD

➔ **WITH** the **default AD permissions**, the intruder's work is EASY!

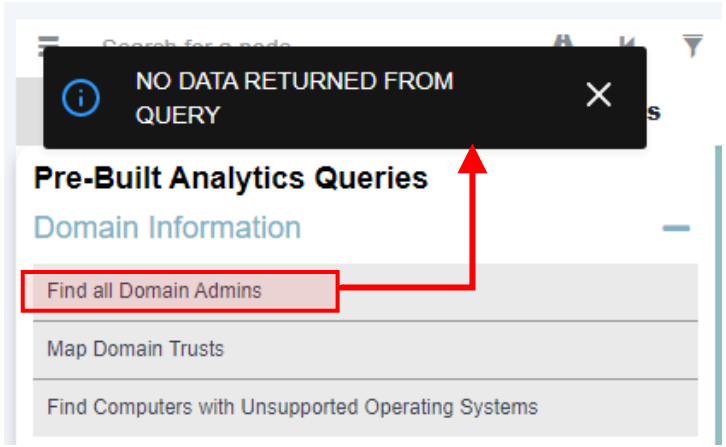


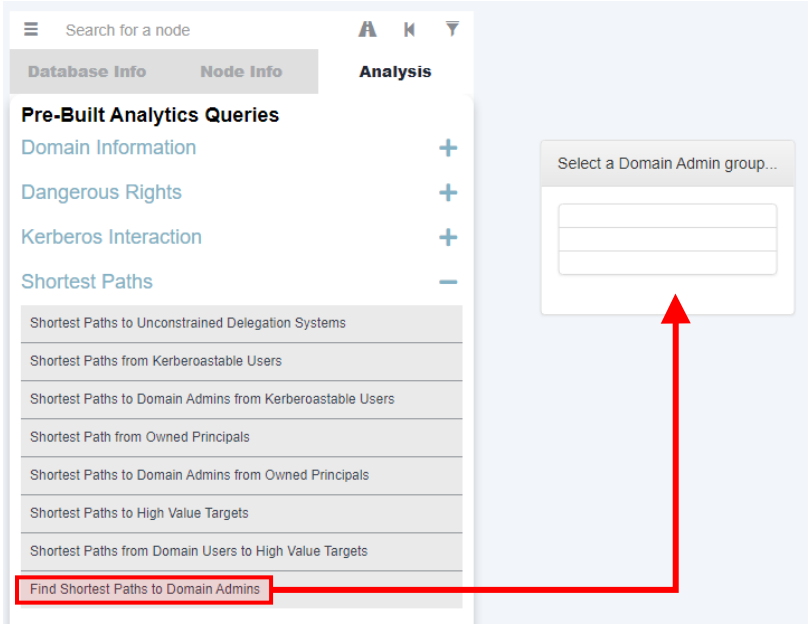
More details:
https://www.semperis.com/resources/improving-your-active-directory-security-posture-adminsdholderto-the-rescue

Locking down permissions in AD will help!

Intruders often use Sharphound/Bloodhound for the initial reconnaissance of attack-paths to your AD

➔ After **removing default read** from **Tier-0** objects, reconnaissance is HARD!





More details:
https://www.semperis.com/resources/improving-your-active-directory-security-posture-adminsdholderto-the-rescue

Free AD vulnerability scanning tools

semperis

- Requires installation of Java and NeoJ4 DB
- Separate extraction of AD data through additional tool (Sharphound) – which is then processed by BloodHound tool for visualization of attack-path

- Powerful UI tool from Semperis for visualization of attack-path
- Easy to use—no setup required
- Built to help AD defenders

- Command-line tool for evaluating security posture of an AD domain

- Powerful UI-tool from Semperis for evaluating security posture of a complete AD forest
- Continuously updated with new indicators of exposure (IOEs) and indicators of compromise (IOCs)

FREE → www.purple-knight.com
www.purple-knight.com/forest-druid

Sample vulnerabilities found by Purple Knight

CRITICAL IOEs FOUND

Non-default principals with DC Sync rights on the domain

Any security principals with Replicate Changes All and Replicate Directory Changes permissions on the domain naming context object can potenti...

Read More...

Zerologon vulnerability

This indicator looks for security vulnerability to CVE-2020-1472, which was patched by Microsoft in August 2020. Without this patch, an unauthent...

Read More...

ADDITIONAL IOEs FOUND

NAME	SEVERITY LEVEL	
Computer or user accounts with unconstrained delegation	Warning	Read More...
Domain Controller owner is not an administrator	Warning	Read More...
GPO linking delegation at the domain controller OU level	Warning	Read More...
GPO linking delegation at the domain level	Warning	Read More...
Privileged users with ServicePrincipalNames defined	Warning	Read More...
Risky RODC credential caching	Warning	Read More...
Unprivileged principals as DNS Admins	Warning	Read More...
Privileged users that are disabled	Informational	Read More...
Protected Users group in use	Informational	Read More...
Unprivileged users can add computer accounts to the domain	Informational	Read More...
User accounts with password not required	Informational	Read More...
Users with SPNs defined	Informational	Read More...

SECURITY INDICATOR

Non-default principals with DC Sync rights on the domain

IOE Found

F 50%

SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Critical	8	Credential Access

Description

Any security principals with Replicate Changes All and Replicate Directory Changes permissions on the domain naming context object can potentially retrieve password hashes for any and all users in an AD domain ("DCSync" attack). Additionally, Write DACL / Owner also allows assignment of these privileges. This can then lead to all kinds of credential-theft based attacks, including Golden and Silver Ticket attacks.

Likelihood of Compromise

DCSync is an attack for accessing credentials through this method. If an attacker gets ahold of these privileges, it is straight-forward to retrieve credential material using tools like Mimikatz, for any user in a domain.

Result

Simple user with permission to extract the passwords from your AD domain.

Found 1 objects with replication permissions.

DistinguishedName	Identity	Access	Enabled
DC=mychild,DC=mydom,DC=local	MYDOM\FredF	Allow: ExtendedRight on: DS-Replication-Get-Changes-All	True

Showing 1 of 1

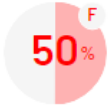
Remediation Steps

Ensure that there are no unnecessary replication permissions and investigate suspicious permissions. Under certain situations (e.g. Microsoft PAM Tiering), an empty group may appear in the results - this is normal but keep in mind that this is a highly privileged group.

SECURITY INDICATOR

Computer or user accounts with unconstrained delegation

IOE Found



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Warning	4	Defense Evasion, Lateral Movement

Description

This indicator looks for computer or user accounts that are trusted for unconstrained Kerberos delegation. These accounts store users' Kerberos TGT locally to authenticate to other systems on their behalf. Computers and users trusted with unconstrained delegation are good targets for Kerberos-based attacks.

Likelihood of Compromise

Attackers who control a service or user trusted for unconstrained delegation can dump local credentials and uncover cached TGT. These credentials could belong to users that accessed the service and who may be privileged.

Result

Found 1 objects configured with unconstrained Kerberos delegation.

Simple PC allowing any process to impersonate any user in your AD

DistinguishedName	DisplayName	UserAccountControl	ServicePrincipalName
CN=CHILDPC01,OU=MyComputers,OU=MyOU,DC=mychild,DC=mydom,DC=local	CHILDPC01$	528384 [TrustedForDelegation, WorkstationTrustAccount]	TERMSRV/CHILDPC01; TERMSRV/ChildPC01.mychild.mydom.local; RestrictedKrbHost/CHILDPC01; HOST/CHILDPC01; RestrictedKrbHost/ChildPC01.mychild.mydom.local; HOST/ChildPC01.mychild.mydom.local

Showing 1 of 1

Remediation Steps

Accounts that require Kerberos delegation should be set to constrain that delegation to the particular service or services that require delegation. Attempts should be made to have Kerberos-enabled accounts not be privileged accounts.

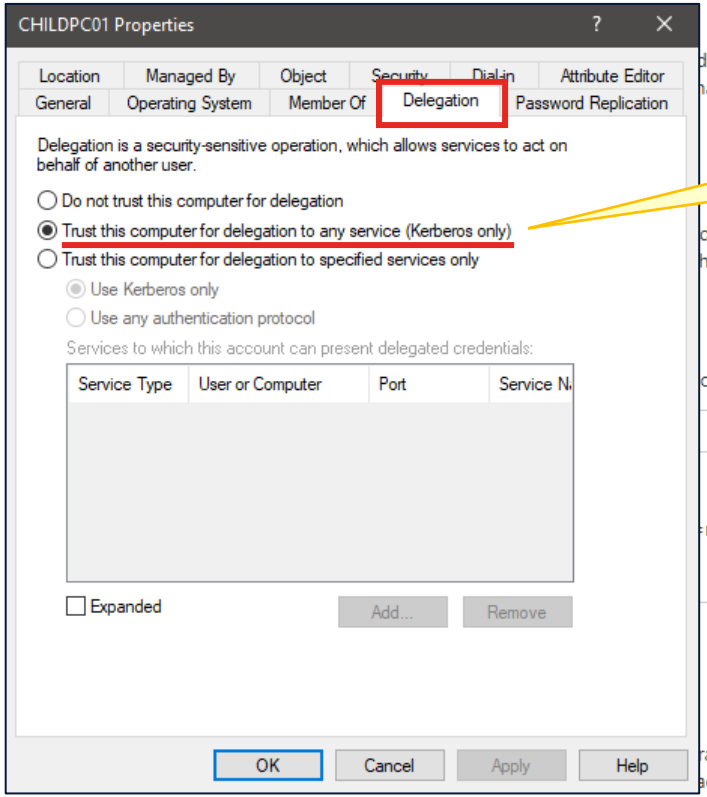
SECURITY INDICATOR

Computer or user accounts with unconstrained delegation

IOE Found

F 50%

SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Warning	4	Defense Evasion, Lateral Movement



d for unconstrained Kerberos delegation. These accounts store users' half. Computers and users trusted with unconstrained delegation are

Doesn't look so dangerous in the UI
… **who can grant this in your AD?**

delegation can dump local credentials and uncover cached TGT. These ho may be privileged.

Simple PC allowing any process to impersonate any user in your AD

on.

	DisplayName	UserAccountControl	ServicePrincipalName
-mydom,DC=local	CHILDPC01$	528384 [TrustedForDelegation, WorkstationTrustAccount]	TERMSRV/CHILDPC01; TERMSRV/ChildPC01.mychild.mydom.local; RestrictedKrbHost/CHILDPC01; HOST/CHILDPC01; RestrictedKrbHost/ChildPC01.mychild.mydom.local; HOST/ChildPC01.mychild.mydom.local

rain that delegation to the particular service or services that require accounts not be privileged accounts.

SECURITY INDICATOR

Domain Controller owner is not an administrator

IOE Found

F 50%

SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Warning	6	Privilege Escalation, Credential Access

Description

This indicator looks for Domain Controller computer accounts whose owner is not a Domain Admins, Enterprise Admins, or built-in Administrator account.

Likelihood of Compromise

Control of DC machine accounts allows for an easy path to compromising the domain. While Domain Controller objects are typically created during DCPromo by privileged accounts, if an accidental ownership change occurs on a DC object, it can have large consequences for security of the domain, since object owners can change permissions on the object to perform any number of actions.

Result

Found 1 domain controllers with non-default owners.

DistinguishedName	Owner
CN=CHILD-DC02,OU=Domain Controllers,DC=mychild,DC=mydom,DC=local	MYDOM\FredF

Showing 1 of 1

Simple user can change permission and password of your DC's computer account … and thus owns your AD forest

Remediation Steps

Ensure that only privileged Tier 0 admin accounts and the domain's built-in groups, such as Enterprise Admins, Domain Admins, and Administrators, have ownership of Domain Controller computer objects. Any unrecognized owner may be a sign of compromise.

SECURITY INDICATOR

Privileged users with ServicePrincipalNames defined

IOE Found

F
0 %

SEVERITY	WEIGHT
Warning	5

Description

This indicator looks for accounts with the adminCount attribute set to 1 AND ServicePrincipalNames (SPNs) defined on the account. In general, privileged accounts should not have SPNs defined on them, as it makes them targets for Kerberos-based attacks that can elevate privileges to those accounts. By default, the krbtgt account falls under this category but is a special case and is not considered part of this indicator.

Likelihood of Compromise

This is a significant issue that can allow an attacker to elevate privileges in a domain. Audit all accounts where privileged access is possible looking for anomalous access. If found, a breach or ongoing attack should be further investigated.

"Kerberoasting": Password **hash** of privileged account is made available to any user by locating the account via the SPN and requesting a TGS – allowing offline cracking of the hash.

Result

Found 2 privileged users with associated SPN.

DistinguishedName	SamAccountName	ServicePrincipalName	AES Enabled
CN=MyChildAdmin,OU=MyAdmins,OU=MyOU,DC=MyChild,DC=mydom,DC=local	MyChildAdmin	MSSQLSvc/dsp-sql.mychild.mydom.local:1469	False
CN=MyRootAdmin,OU=MyAdmins,OU=MyOU,DC=mydom,DC=local	MyRootAdmin	MSSQLSvc/other-sql.mydom.local:1469	False

Showing 2 of 2

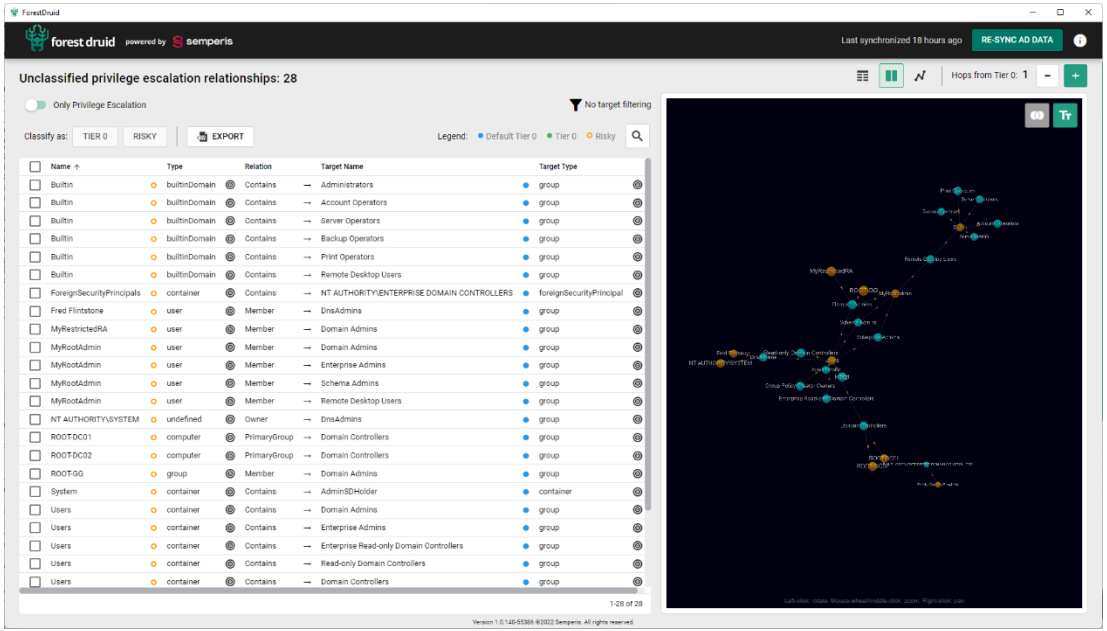
Remediation Steps

Remove SPN from privileged accounts when not required or mitigate by other means.

NEW COMMUNITY TOOL (FREE!)

Forest DRUID

- Tool for **inter-actively** analyzing difficult-to-locate AD security risks
- **Easy to setup and efficient to run** for gathering proper AD data (*permissions, relationships between objects etc.*)
- Concentrates on objects and relationships that could be a risk to Tier 0 (*Domain Controllers, Domain Admins etc.*)
- Helps the AD admin to **find risky relationships** that could allow attacks against AD

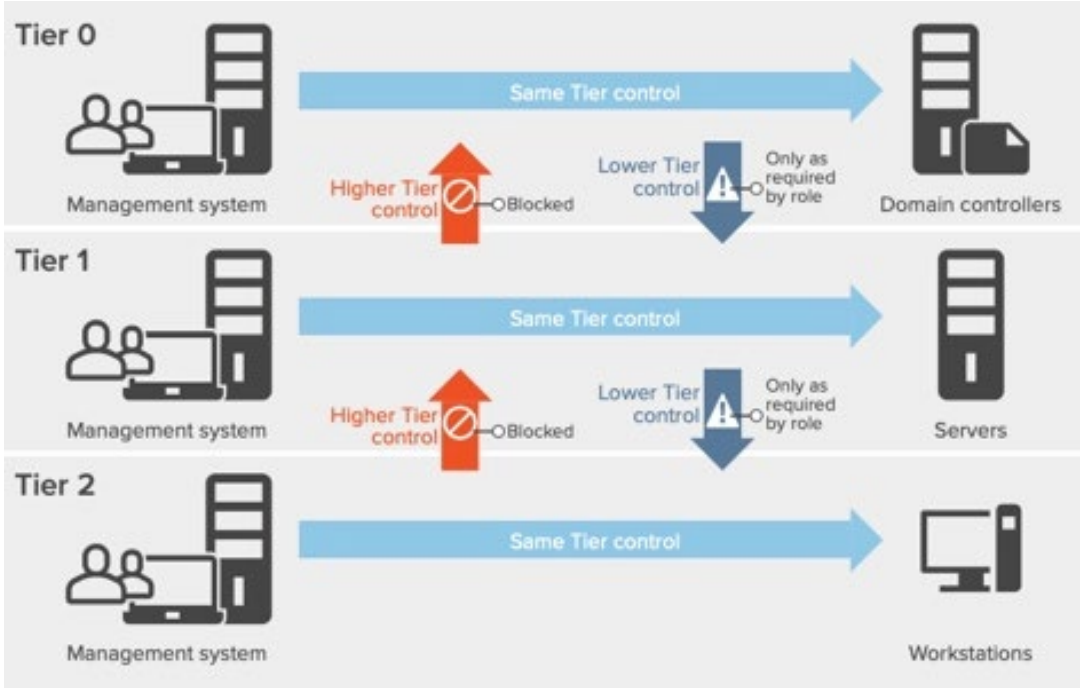


➔ Enables admins to discover and manage the *privileged-defined perimeter* of their Active Directory!

It’s never too late to invest in proper TIERING!

semperis

Focus on understanding and protecting your Tier 0 assets first ➔ *Forest DRUID helps!*



Source: Microsoft

Example of a Tiering Model

Tier 0	Domain Controllers (DCs), identity management resources, administrator user accounts and service accounts
Tier 1	Server, application, workstation admin authority
Tier 2	Standard user accounts, workstations, printers and devices

semperis

#1 Top Trend

Identity threat detection and response (ITDR) is a Gartner “top trend” for cybersecurity in 2022.

“While organizations understand the criticality of AD, the security of AD is often overlooked. If AD is breached, an attacker gets virtually unrestrained access to the organization’s entire network and resources. **This makes AD a prominent high-value target for threat actors**.”

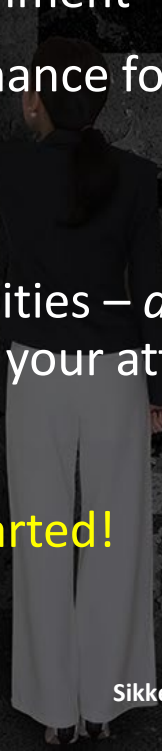
Gartner

Emerging Technologies and Trends Impact Radar: Security

KEY TAKE AWAYS

1. Active Directory is the Achilles heel of a Hybrid-Environment
2. Locking down the default AD security decreases the chance for intruders to elevate their privileges
3. Proper TIERING makes a difference – take it serious!
4. Continuously scanning both AD and AAD for vulnerabilities – *and fixing them, where possible* – is a key requirement to reduce your attack surface

➔ check out **Purple Knight** and **Forest Druid** to get started!



Thank you

Questions? Get in touch …

Guido Grillenmeier

Semperis Principal Technologist (EMEA)

guidog@semperis.com

www.linkedin.com/in/guidogrillenmeier

More Information

Purple Knight	www.purple-knight.com
Forest Druid	www.purple-knight.com/forest-druid
Pre-Win2k Group	https://www.semperis.com/blog/security-risks-pre-windows-2000-compatibility-windows-2022
AdminSDholder	https://www.semperis.com/resources/improving-your-active-directory-security-posture-adminsdholderto-the-rescue
DSDETECT	https://www.semperis.com/downloads/tools/public/dsdetect.zip
Hiding GPOs within a GPO	https://sdmsoftware.com/security-related/the-attack-of-the-trojan-gpos