purple knight

# SECURITY ASSESSMENT REPORT

v 5.0.2506.11001 | Community

Note: A typical Active Directory is in a constant state of flux, with hundreds or even thousands of changes made each day.
Purple Knight offers a helpful snapshot of your security posture, but it's no substitution for continuous monitoring of events taking place in your directory.
To learn more about a comprehensive, round-the-clock monitoring of all aspects of AD, click here.

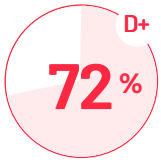
## SECURITY POSTURE OVERVIEW

This report summarizes the security assessment results performed in your hybrid identity environment on 10/4/2025 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 Entra tenant, Okta domain, or all.

- 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).
- Entra tenant: Purple Knight queried the selected Entra tenant focusing on some of the most common attack vectors that threat actors use to gain access to the Entra environment.
- Okta identity platform: Purple Knight queried the selected Okta domain checking for activities that may indicate unauthorized access attempts, suspicious behavior, or potential threats within the Okta infrastructure.

The report provides an overall security risk score as well as detailed results about each Indicator of Exposure (IOE) found. By uncovering 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 | **myzo.local** |
| No. of Domains | **1** |
| Duration | **00:00:36.4368220** |
| Run by | **MYZO\lacie.monica** |

**Indicators**

| | |
|---|---|
| Evaluated | **115** |
| Not selected | **1** |
| IOEs found | **17** |
| Passed | **98** |
| Failed to run | **0** |
| Not Relevant | **3** |
| Canceled | **0** |

## CRITICAL IOEs FOUND

**Permission changes on AdminSDHolder object**

This indicator checks for modifications on the access control lis...

Read More...

**Print spooler service is enabled on a DC**

This indicator checks for Domain Controllers running the print ...

Read More...

**Privileged Users with Weak Password Policy**

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

Read More...

## ADDITIONAL IOEs FOUND

| NAME | PLATFORM | SEVERITY LEVEL | ACTION |
|---|---|---|---|
| • LDAP signing is not required on Domain Controllers | AD | High | Read More... |
| • Privileged objects with unprivileged owners | AD | High | Read More... |
| • RC4 or DES encryption type are supported by Domain Controllers | AD | High | Read More... |
| • Unprivileged principals as DNS Admins | AD | High | Read More... |
| • Built-in domain Administrator account used within the last two weeks | AD | Medium | Read More... |
| • Changes to Default Domain Policy or Default Domain Controllers Policy in the last 7 days | AD | Medium | Read More... |
| • Changes to Pre-Windows 2000 Compatible Access Group membership | AD | Medium | Read More... |
| • Changes to privileged group membership in the last 7 days | AD | Medium | Read More... |
| • gMSA not in use | AD | Medium | Read More... |
| • Users with Kerberos pre-authentication disabled | AD | Medium | Read More... |
| • Recent privileged account creation activity | AD | Low | Read More... |
| • Unprivileged users can add computer accounts to the domain | AD | Low | Read More... |
| • AD objects created within the last 10 days | AD | Informational | Read More... |
| • Protected Users group not in use | AD | Informational | Read More... |

## INDICATORS FAILED TO RUN

None

**Notes**

## ACTIVE DIRECTORY RESULTS

### Categories


#### AD DELEGATION

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

Read More ...


#### ACCOUNT SECURITY

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

Read More ...


#### AD INFRASTRUCTURE SECURITY

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

Read More ...


#### GROUP POLICY SECURITY

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

Read More ...


#### KERBEROS SECURITY

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

Read More ...


#### HYBRID

Hybrid indicators help you understand and mitigate the risks associated with a hybrid identity

Read More ...

CATEGORY

# AD DELEGATION

C
84%

| WEIGHT | EVALUATED | INDICATORS FOUND |
|---|---|---|
| 3 | 18 | 4 |

AD delegation is a critical part of security and compliance. By delegating control over Active Directory, you can grant users or groups permissions without adding users to privileged groups.

SECURITY INDICATOR

## Inheritance enabled on AdminSDHolder object

Pass

A+
100%

SEVERITY
Critical

WEIGHT
10

### Security Frameworks
MITRE ATT&CK

- Defense Evasion
- Privilege Escalation

### Description
This indicator checks for inheritance enabled on the access control list (ACL) of the AdminSDHolder object.

### Likelihood of Compromise
The AdminSDHolder object in Active Directory holds the permissions that will be applied to privileged groups and users, including Domain Admins. By default, permissions on privileged users are more restrictive to protect them from compromise. If an organization adjusts the permissions on the AdminSDHolder object, including enabling inheritance, they may weaken the security of these privileged users.
An attacker may discover these weaker permissions on privileged users and groups, and with a greater surface area, an attacker has a stronger chance of formulating attack paths to compromise users such as a Domain Admin, and then compromising Active Directory.

### References
AdminSDHolder to improve Active Directory Security | Semperis
7 Active Directory Misconfigurations to Find and Fix-Now - Semperis
Appendix C - Protected Accounts and Groups in Active Directory | Microsoft Learn

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Permission changes on AdminSDHolder object

IOE Found

F
0%

SEVERITY
Critical

WEIGHT
10

### Security Frameworks
MITRE ATT&CK

- Defense Evasion
- Privilege Escalation

ANSSI

- vuln1_permissions_adminsdholder
- vuln2_permissions_adminsdholder
- vuln1_privileged_members_perm
- vuln2_privileged_members_perm

### Description
This indicator checks for modifications on the access control list (ACL) of the AdminSDHolder object.

### Likelihood of Compromise
The AdminSDHolder object in Active Directory holds the permissions that will be applied to privileged groups and users, including Domain Admins. By default, permissions on privileged users are more restrictive to protect them from compromise. If an organization adjusts the permissions on the AdminSDHolder object, they may weaken the security of these privileged users.
An attacker may discover these weaker permissions on privileged users and groups, and with a greater surface area, an attacker has a stronger chance of formulating attack paths to compromise users such as a Domain Admin, and then compromising Active

Directory.

### References

AdminSDHolder to improve Active Directory Security | Semperis
7 Active Directory Misconfigurations to Find and Fix-Now - Semperis
Appendix C - Protected Accounts and Groups in Active Directory | Microsoft Learn
Dangerous permissions on the adminSDHolder object | ANSSI
Constrained authentication delegation to a domain controller service | ANSSI

### Result

Found 1 domains with AdminSDHolder container permission changes in the last 6 months.

| Attribute | DistinguishedName | EventTimestamp | Ignored |
|---|---|---|---|
| nTSecurityDescriptor | CN=AdminSDHolder,CN=System,DC=myzo,DC=local | 10/3/2025 6:16:42 PM | False |

Showing 1 of 1

### Remediation Steps

Organizations should investigate the permissions on the AdminSDHolder object if modified, and use attack path analysis software, such as Forest Druid, to analyze attack paths to privileged users in Active Directory.
Organizations, if changing the permissions on AdminSDHolder, should have an established process in place for awareness. Unplanned changes to AdminSDHolder should be considered **highly suspicious** and **must** be investigated further. Unplanned changes to AdminSDHolder are a **very strong indicator** of compromise of Active Directory.

SECURITY INDICATOR

## Changes to AD Display Specifiers in the past 90 days

Pass

A+ 100%

SEVERITY
Low

WEIGHT
3

### Security Frameworks

MITRE ATT&CK

- Execution
- Defense Evasion

### Description

This indicator looks for changes made in the past 90 days to the adminContextMenu attribute on AD display specifiers. This attribute controls the right-click menus presented to users in the domain using MMC tools such as AD Users and Computers. Modifying these attributes can potentially allow attackers to get users to run arbitrary code if those menu options are clicked.

### Likelihood of Compromise

Attackers may utilize context menus as a stealthy way of getting various users in a domain to execute code. Modifying this attribute requires special permissions granted by default only to Domain Admins and Enterprise Admins and also requires the user to click on the illicit context menu item. See the this blog post for additional information.

### References

Semperis blog | Active Directory Security: Abusing Display Specifiers

### Result

No evidence of exposure.

### Remediation Steps

None

SECURITY INDICATOR

## Changes to default security descriptor schema in the last 90 days

Pass

A+ 100%

SEVERITY
High

WEIGHT
7

### Security Frameworks

MITRE ATT&CK

- Defense Evasion
- Privilege Escalation

MITRE D3FEND

- Detect - Domain Account Monitoring

### Description

This indicator detects changes made to the default security descriptor schema in the last 90 days. If an attacker gets access to the schema instance in a given forest, they can make changes to the defaultSecurityDescriptor attribute on any AD object class. These changes would then propagate as new default Access Control Lists (ACLs) on any newly created object in AD, potentially weakening

AD security posture.

### Likelihood of Compromise
Changes to the default security descriptor are not common. An admin should know that the change was made and be able to articulate the reason for the change. If the change was not intentional, the likelihood of compromise is very high. The chances of compromise are lower if the change hardens the setting instead of weakening it.

### References
audit-user-account-management of Microsoft

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Domain Controller owner is not an administrator

Pass


SEVERITY
High

WEIGHT
6

### Security Frameworks
MITRE ATT&CK

- Credential Access
- Privilege Escalation

MITRE D3FEND

- Harden - System Configuration Permissions

ANSSI

- vuln1_permissions_dc
- vuln2_permissions_dc

### 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.

### References
Dangerous ACLs expose domain controller objects (attack path) | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Non-default access to DPAPI key

Pass


SEVERITY
High

WEIGHT
7

### Security Frameworks
MITRE ATT&CK

- Credential Access

MITRE D3FEND

- Harden - User Account Permissions

ANSSI

- vuln1_permissions_dpapi
- vuln2_permissions_dpapi

### Description
This indicator uses API calls to check whether each DC has non-default principals permitted to retrieve the domain DPAPI backup

key (using LsaRetrievePrivateData).

### Likelihood of Compromise
An attacker could recover all domain data encrypted via DPAPI, if they gain access to such data.

### References
Dangerous ACLs expose DPAPI key objects (attack path) | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Enterprise Key Admins with full access to domain

Pass A+ 100%

SEVERITY
High

WEIGHT
7

### Security Frameworks
MITRE ATT&CK

- Credential Access
- Lateral Movement
- Privilege Escalation

MITRE D3FEND

- Harden - User Account Permissions

ANSSI

- vuln2_adupdate_bad

### Description
This indicator looks for evidence of a bug in certain versions of Windows Server 2016 Adprep that granted undue access to the Enterprise Key Admins group.

### Likelihood of Compromise
This issue was corrected in a subsequent release of Server 2016 and may not exist in your environment, but checking for it is definitely warranted, since it grants this group the ability to replicate all changes from AD (DCSync Attack).

### References
Bad Active Directory versions | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Foreign Security Principals in Privileged Group

Pass A+ 100%

SEVERITY
Medium

WEIGHT
5

### Security Frameworks
MITRE ATT&CK

- Defense Evasion
- Persistence

MITRE D3FEND

- Detect - Domain Account Monitoring

### Description
This indicator looks for members of privileged groups which are Foreign Security Principals. Special care should be taken when including accounts from other domains as members of privileged groups.

### Likelihood of Compromise
While not immediately indicative of an attack, privileged users that are not clearly marked as such (adminCount =1) represent an exposure in that they may be used nefariously without being detected. Since Foreign Security Principals do not have the adminCount attribute, they could miss being detected by some security auditing tools. Additionally, an attacker may add a

privileged account and attempt to hide it using this method.

**References**

audit-user-account-management of Microsoft

**Result**

No evidence of exposure.

**Remediation Steps**

None

SECURITY INDICATOR

## gMSA not in use

IOE Found

B 94%

SEVERITY
Medium

WEIGHT
4

**Security Frameworks**

MITRE ATT&CK

- Credential Access

**Description**

This indicator checks if there are enabled group Managed Service Account (gMSA) objects in the domain.

**Likelihood of Compromise**

The group Managed Service Account (gMSA) feature in Windows Server 2016 allows automatic rotation of passwords for service accounts, making them much more difficult for attackers to compromise. The feature should be used whenever possible for service accounts.

**References**

Get started with Group Managed Service Accounts

**Result**

Found 1 domains with no gMSA objects enabled.

| DomainName | Ignored |
|---|---|
| myzo.local | False |

Showing 1 of 1

**Remediation Steps**

Group Managed Service Accounts should be used to protect service accounts. See description for more information.

SECURITY INDICATOR

## Non-privileged users with access to gMSA passwords

Pass

A+ 100%

SEVERITY
High

WEIGHT
6

**Security Frameworks**

MITRE ATT&CK

- Credential Access

ANSSI

- vuln1_permissions_gmsa_keys
- vuln2_permissions_gmsa_keys

**Description**

This indicator looks for principals listed within MSDS-groupMSAmembership that are not in the built-in admin groups.

**Likelihood of Compromise**

An attacker that controls access to the gMSA account can retrieve passwords for resources managed with gMSA.

**References**

Dangerous ACLs expose gMSA key objects (attack path) | ANSSI

**Result**

No evidence of exposure.

**Remediation Steps**

None

SECURITY INDICATOR

## Built-in guest account is enabled

Pass

A+ 100%

SEVERITY
Low

WEIGHT
2

### Security Frameworks
MITRE ATT&CK

- Discovery
- Reconnaissance

MITRE D3FEND

- Evict - Account Locking

ANSSI

- vuln2_guest

### Description
This indicator checks if the built-in Active Directory "guest" account is enabled. The guest account allows for accounts with no password access to the domain and is disabled in most AD environments.

### Likelihood of Compromise
Attackers can take advantage of a guest account to enumerate open shares that are accessible to the "Everyone" setting, as is often the case. Additionally, attackers may utilize the limited access these accounts provide to conduct additional scanning for vulnerable users, shares and other network resources.

### References
Guest account enabled | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Users with permissions to set Server Trust Account

Pass

A+ 100%

SEVERITY
Critical

WEIGHT
8

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation

### Description
Checks for permissions on the domain NC head that enables a user to set a UAC flag - Server_Trust_Account on computer objects. This flag gives that computer object special permissions similar to a domain controller.

### Likelihood of Compromise
A persistence technique where an attacker with DS-Install-Replica permissions can manipulate the userAccountControl attribute to promote a compromised computer account to Domain Controller status. This enables privilege escalation through domain replication privileges, allowing attacks like DCSync to extract credentials.

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Non default value on ms-Mcs-AdmPwd SearchFlags

Pass

A+ 100%

SEVERITY
High

WEIGHT
7

### Security Frameworks
MITRE ATT&CK

- Credential Access

### Description
Some flags on the ms-Mcs-AdmPwd schema may inadvertently cause passwords to be visible to users allowing an attacker to use it as stealthy backdoor. This indicator looks for any changes to default searchFlags, which may create an exposure. Detection of changes to the default will result in a score of 80 for this indicator, signifying that a review should be conducted. Any removal of the default flags will result in a score of 0 due to their importance to security.

### Likelihood of Compromise
Even though schema changes are not common, a targeted schema change like this can leave the administrator passwords of 100s or 1000s of computers vulnerable to non-privileged users.

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Objects with Reanimate-Tombstones extended right

Pass A+ 100%

SEVERITY
Medium

WEIGHT
4

### Security Frameworks
MITRE ATT&CK

- Lateral Movement
- Privilege Escalation
- Persistence

MITRE D3FEND

- Isolate - User Account Permissions

### Description
This indicator checks if there are any non-default principals with the Reanimate-Tombstones extended right configured.

### Likelihood of Compromise
When an Active Directory object is deleted, it is by default transformed into a tombstone object and loses most of its attributes. If the Active Directory Recycle Bin optional feature is enabled, the object is instead transformed into a deleted-object, which maintains the state of the object before deletion and can be undeleted without loss of information.
By default, only domain administrators can restore deleted objects. For other users, restoring these types of AD deleted objects requires having the "Reanimate-Tombstones" extended right. It is not recommended to delegate this right to other users since tombstone reanimation is a highly privileged and infrequent operation.
Furthermore, this permission could assist attackers with privilege escalation and lateral movement opportunities, as it could permit them to restore account objects with access to more resources. As tombstones don't maintain the state of the original object, reanimating them essentially grants control over the account because the user must set a password for the restored account.

### References
Restoring Deleted Objects | Microsoft Learn
Creating and Deleting Objects in Active Directory Domain Services | Microsoft Learn
Recycle Bin Optional Feature | Microsoft Learn

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Objects in privileged groups without adminCount=1 (SDProp)

Pass A+ 100%

SEVERITY
Medium

WEIGHT
4

### Security Frameworks
MITRE ATT&CK

- Defense Evasion
- Persistence

### Description

This indicator looks for objects in privileged groups with AdminCount not equal to 1. AdminCount is an object flag that is set by the SDProp process (run by default every 60 minutes) if that object's DACLs are modified to sync with the AdminSDHolder object through inheritance. If an object within these groups has an AdminCount not equal to 1 then it could signify that the DACLs were manually set (no inheritance) or that there is an issue with SDProp.

### Likelihood of Compromise
While not immediately indicative of an attack, privileged users that are not clearly marked as such (adminCount =1) represent an exposure in that they may be used nefariously without being detected. Additionally, an attacker may add a privileged account and attempt to hide it using this method.

### References
AdminSDHolder, protected groups and SDPROP | Microsoft Learn

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Changes to MS LAPS read permissions

Not Relevant


SEVERITY
Low

WEIGHT
3

### Security Frameworks
MITRE ATT&CK

- Credential Access
- Lateral Movement

MITRE D3FEND

- Harden - User Account Permissions

### Description
This indicator looks for permissions on computer accounts that could allow inadvertent exposure of local administrator accounts in environments that use the Microsoft LAPS solution. These permissions include Read access to ms-Mcs-AdmPwd as well as Write DACL and Owner (which would allow provisioning the read access). LAPS provides a method to rotate local administrator account passwords on servers and workstations.

### Likelihood of Compromise
Only authorized administrative users should have access to LAPS passwords. Attackers may use this capability to laterally move through a domain using local compromised administrator accounts.

### References
Local Administrator Password Solution (LAPS)

### Result
This indicator is not applicable as LAPS was not found in the forest.

### Remediation Steps
None

SECURITY INDICATOR

## Non-default principals with DC Sync rights on the domain

Pass


SEVERITY
Critical

WEIGHT
8

### Security Frameworks
MITRE ATT&CK

- Credential Access

ANSSI

- vuln1_permissions_naming_context
- vuln2_permissions_naming_context

### 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.

### References
Dangerous ACLs expose a naming context root (attack path) | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Privileged objects with unprivileged owners

IOE Found

F
0 %

SEVERITY
High

WEIGHT
6

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation

ANSSI

- vuln1_permissions_adminsdholder
- vuln2_permissions_adminsdholder

### Description
If a privileged object (as determined by adminCount=1) is owned by an account that is unprivileged, then any compromise of that unprivileged account could result in those privileged objects' delegation being modified, since owners can override any delegation on an object, if only temporarily.

### Likelihood of Compromise
Most privileged objects are owned by privileged groups or users. But if a privileged object were to be owned by an unprivileged account, it could be easily taken over. And even though SDProp might correct any delegation done by an attacker who has compromised an owner, the attacker could have up to 1 hour to perform any changes on the privileged object (e.g. group membership changes or password changes) before SDProp corrects it.

### References
Dangerous permissions on the adminSDHolder object | ANSSI

### Result
Found 16 privileged objects with unprivileged owner.

| Owner | DistinguishedName | Ignored |
|---|---|---|
| Could not read owner | CN=Administrator,CN=Users,DC=myzo,DC=local | False |
| Could not read owner | CN=Administrators,CN=Builtin,DC=myzo,DC=local | False |
| Could not read owner | CN=Print Operators,CN=Builtin,DC=myzo,DC=local | False |
| Could not read owner | CN=Backup Operators,CN=Builtin,DC=myzo,DC=local | False |
| Could not read owner | CN=Replicator,CN=Builtin,DC=myzo,DC=local | False |
| Could not read owner | CN=krbtgt,CN=Users,DC=myzo,DC=local | False |
| Could not read owner | CN=Domain Controllers,CN=Users,DC=myzo,DC=local | False |
| Could not read owner | CN=Schema Admins,CN=Users,DC=myzo,DC=local | False |
| Could not read owner | CN=Enterprise Admins,CN=Users,DC=myzo,DC=local | False |
| Could not read owner | CN=Domain Admins,CN=Users,DC=myzo,DC=local | False |

Showing 10 of 16
View additional results...

### Remediation Steps
Remove unprivileged owner from privileged objects.

SECURITY INDICATOR

## Unprivileged users can add computer accounts to the domain

IOE Found

B+
96 %

SEVERITY
Low

WEIGHT
3

### Security Frameworks

MITRE ATT&CK

- Credential Access
- Lateral Movement

ANSSI

- vuln4_user_accounts_machineaccountquota

### Description

This indicator checks for an AD configuration that allows unprivileged domain members to add computer accounts to the domain. By default, members of the Authenticated Users group can add up to 10 machine accounts to a domain. If the ms-DS-MachineAccountQuota attribute on the domain naming context head is not set to 0, regular users have this ability.The ability to do this confers certain rights on those created machine accounts that can be abused by a variety of Kerberos-based attacks. Note: This configuration may be enabled but be already mitigated by GPO settings (User Right: "Add workstations to domain" configured with only high-privileged group(s)/account(s)) linked to Domain Controllers OU that are not checked by this indicator.

### Likelihood of Compromise

The ability to add computer accounts to a domain without restrictions or monitoring present opportunities for attackers to add their own accounts or take advantage of uncontrolled computers with vulnerabilities, thereby extending their reach and entrenching themselves in the environment.

### References

Unrestricted domain join | ANSSI

### Result

Found 1 domains in which regular users can add computer accounts.

| MachineAccountQuota | DistinguishedName | Ignored |
|---|---|---|
| 10 | DC=myzo,DC=local | False |

Showing 1 of 1

### Remediation Steps

Set the ms-DS-MachineAccountQuota attribute on the domain NC head to 0 to disable regular users' ability to add computer accounts.

CATEGORY

# ACCOUNT SECURITY

C+ 89%

| WEIGHT | EVALUATED | INDICATORS FOUND |
|---|---|---|
| 6 | 34 | 9 |

Account Security indicators pertain to security weaknesses on individual accounts--built-in or otherwise, within Active Directory.

SECURITY INDICATOR

## Abnormal Password Refresh

Pass A+ 100%

SEVERITY
Medium

WEIGHT
5

### Security Frameworks
MITRE ATT&CK

- Credential Access
- Persistence

### Description
This indicator looks for user accounts with a recent pwdLastSet change without a corresponding password replication.

### Likelihood of Compromise
If an administrator marks the option "User must change password at next logon" and then clears (i.e. unchecks) the option later, the pwdLastSet is updated without the password actually being changed. This could be an administrative error or an attempt to bypass the organization's password policy.

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Built-in domain Administrator account with old password (180 days)

Pass A+ 100%

SEVERITY
Medium

WEIGHT
4

### Security Frameworks
MITRE ATT&CK

- Credential Access

MITRE D3FEND

- Harden - Strong Password Policy

ANSSI

- vuln1_password_change_priv

### Description
This indicator checks if the password of the built-in Domain Administrator account is older than 180 days.

### Likelihood of Compromise
The built-in Domain Administrator account is a well-known SID that is easily discoverable, regardless of attempts to obfuscate the account, such as renaming it.
It is recommended that this account is not used for administration of Active Directory, but due to lack of use, this account in many organizations also goes unmonitored. Attackers may target this account for brute force password attacks.

### References
Security identifiers | Microsoft Learn
Privileged account passwords age too old | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

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

IOE Found

B-
91 %

SEVERITY
Medium

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.

| EventTimestamp | DistinguishedName | Ignored |
|---|---|---|
| 10/4/2025 2:50:48 PM | CN=Administrator,CN=Users,DC=myzo,DC=local | False |

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.

SECURITY INDICATOR

## Computer Accounts in Privileged Groups

Pass

A+
100%

SEVERITY
High

WEIGHT
6

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation

### Description
This indicator looks for computer accounts that are members of built-in privileged groups.

### Likelihood of Compromise
If a computer account is a member of a domain privileged group, then anyone that compromises that computer account (i.e. becomes administrator) can act as a member of that group. Generally speaking, there is little reason for normal computer accounts to be part of privileged groups.

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Privileged users that are disabled

Pass

A+
100%

SEVERITY
Low

WEIGHT
3

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation

MITRE D3FEND

- Harden - User Account Permissions

### Description
This indicator looks for privileged user accounts, as indicated by their adminCount attribute set to 1, that are disabled. If a privileged account is disabled, it should be removed from its privileged group(s) to prevent inadvertent misuse.

### Likelihood of Compromise
When a user is disabled, it tends to not be monitored as closely as active accounts. If this user is also a privileged user, then it becomes a target for takeover if an attacker can enable the account.

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## OU permissions enabling BadSuccessor dMSA escalation

Pass A+ 100%

SEVERITY
High

WEIGHT
7

### Security Frameworks
MITRE ATT&CK

- Credential Access
- Privilege Escalation

MITRE D3FEND

- Model - Access Modeling

### Description
This indicator checks for excessive permissions to create delegated Managed Service Accounts (dMSAs) within Active Directory organizational units (OU) or NC head (NC Head is the top-level object of a Naming Context (NC) in Active Directory) across domains that contain Windows Server 2025 domain controllers. The indicator identifies non-privileged identities that have been granted CreateChild, GenericAll, WriteDACL, or WriteOwner permissions on OUs or NC head, which could enable the execution of the "BadSuccessor" Privilege Escalation attack. The "BadSuccessor" attack is a technique which exploits vulnerabilities in Microsoft's Active Directory and enables domain takeover. The attack leverages a feature called Delegated Managed Service Accounts (dMSA), which was introduced in Windows Server 2025.

### Likelihood of Compromise
Excessive OU-level permissions, such as CreateChild on an OU or write rights on a dMSA object, can be abused to elevate privileges. In particular, the "BadSuccessor" attack simulates a completed dMSA migration to inherit a target account's security context. In environments with weak OU/NC head ACLs, the risk is moderate to high, although enhanced controls in Windows Server 2025 domains can reduce exposure.

### References
BadSuccessor: Abusing dMSA to Escalate Privileges in Active Directory
KB5008383 — Active Directory permissions updates (CVE-2021-42291)
Setting up delegated Managed Service Accounts

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Enabled admin accounts that are inactive

Pass A+ 100%

SEVERITY
Medium

WEIGHT
4

### Security Frameworks
MITRE ATT&CK

- Credential Access
- Privilege Escalation

MITRE D3FEND

- Evict - Account Locking

ANSSI

- vuln1_user_accounts_dormant

### Description
This indicator looks for admin accounts that are enabled, but have not logged in for the past 90 days. Attackers who can compromise these accounts may be able to operate unnoticed.

### Likelihood of Compromise
While the presence of an unused admin account is not automatically a problem, removing these accounts reduces the attack surface of AD.

### References
Dormant accounts | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Ephemeral Admins

Pass

A+ 100%

SEVERITY
Low

WEIGHT
3

### Security Frameworks
MITRE ATT&CK

- Persistence

MITRE D3FEND

- Harden - User Account Permissions

### Description
This indicator looks for users which were added and removed from an admin group within a 48 hour span of time. Such short-lived accounts may indicate malicious activity.

### Likelihood of Compromise
In most environments, management of admin accounts is tightly controlled and audited. This indicator provides a fast method to create a list of ephemeral admins for investigation and review.

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## FGPP not applied to Global group

Pass

A+ 100%

SEVERITY
Medium

WEIGHT
5

### Security Frameworks
MITRE ATT&CK

- Persistence
- Credential Access

MITRE D3FEND

- Harden - Strong Password Policy

### Description
This indicator looks for FGPP targeted to a Universal or Domain Local group.

### Likelihood of Compromise
Changing a group's scope settings from Global group to Universal or Domain Local group, will result in FGPP settings no longer applying to that group, and decreasing its password security controls.

### References
NIST.SP.800-63-3

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Forest contains more than 50 privileged accounts

Pass

A+ 100%

SEVERITY
Medium

WEIGHT
5

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation
- Reconnaissance

ANSSI

- vuln1_privileged_members
- vuln2_privileged_members

### Description
This indicator counts the number of privileged user accounts defined in the forest, where 50 is deemed the upper limit for these types of accounts. A privileged account is defined as any user with the AdminCount attribute set to 1.

### Likelihood of Compromise
In general, the more privileged accounts you have, the more opportunities there are for attackers to compromise one of those accounts. 50 is an arbitrary number, but the number should reflect the absolute maximum allowed. If business needs dictate many privileged accounts, consider implementing a tiered administration model to further isolate those privileged accounts and their potential impact from compromise.

### References
Enterprise access model | Microsoft Learn
Large privileged group member count | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## AD objects created within the last 10 days

IOE Found

A+ 100%

SEVERITY
Informational

WEIGHT
1

### Security Frameworks
MITRE ATT&CK

- Lateral Movement
- Persistence

MITRE D3FEND

- Detect - Domain Account Monitoring

### Description
This indicator looks for any AD objects that were created within the last 10 days. It is meant to be used for threat hunting, post-breach investigation or compliance validation.

### Likelihood of Compromise
In some environments, object creation happens consistently; however, recently added accounts should be reviewed to ensure they are legitimate.

### References
Audit User Account Management | Microsoft Learn

### Result
Found 359 objects that were created in the last 10 days.

| DistinguishedName | ObjectName | ObjectClass | EventTimestamp |
|---|---|---|---|
| DC=myzo,DC=local | myzo | domainDNS | 10/4/2025 3:00:41 AM |
| CN=Users,DC=myzo,DC=local | Users | container | 10/4/2025 3:00:49 AM |
| CN=Computers,DC=myzo,DC=local | Computers | container | 10/4/2025 3:00:49 AM |
| OU=Domain Controllers,DC=myzo,DC=local | Domain Controllers | organizationalUnit | 10/4/2025 3:00:49 AM |
| CN=System,DC=myzo,DC=local | System | container | 10/4/2025 3:00:49 AM |
| CN=LostAndFound,DC=myzo,DC=local | LostAndFound | lostAndFound | 10/4/2025 3:00:49 AM |
| CN=Infrastructure,DC=myzo,DC=local | Infrastructure | infrastructureUpdate | 10/4/2025 3:00:49 AM |
| CN=ForeignSecurityPrincipals,DC=myzo,DC=local | ForeignSecurityPrincipals | container | 10/4/2025 3:00:49 AM |
| CN=Program Data,DC=myzo,DC=local | Program Data | container | 10/4/2025 3:00:49 AM |
| CN=Microsoft,CN=Program Data,DC=myzo,DC=local | Microsoft | container | 10/4/2025 3:00:49 AM |

Showing 10 of 359
View additional results...

### Remediation Steps
Ensure that the new objects are known and legitimate.

SECURITY INDICATOR

## Recent privileged account creation activity

IOE Found

C+ 88%

SEVERITY
Low

WEIGHT
3

### Security Frameworks
MITRE ATT&CK

- Persistence

MITRE D3FEND

- Detect - Domain Account Monitoring

### Description
This indicator looks for any users or groups that were created within the last month. Privileged accounts and groups are defined by having their adminCount attribute set to 1.

### Likelihood of Compromise
In most environments, creation of privileged accounts and groups is tightly controlled and audited. This indicator provides a fast method to create a list of new privileged accounts (where adminCount = 1) for investigation and review.

### References
audit-user-account-management of Microsoft

### Result
Found 3 objects that were created in the last 30 days and are members of a privileged group.

| DistinguishedName | SamAccountName | EventTimestamp | Ignored |
|---|---|---|---|
| CN=Administrator,CN=Users,DC=myzo,DC=local | Administrator | 10/4/2025 3:00:50 AM | False |
| CN=krbtgt,CN=Users,DC=myzo,DC=local | krbtgt | 10/4/2025 3:01:33 AM | False |
| CN=Lacie Monica,CN=Users,DC=myzo,DC=local | lacie.monica | 10/4/2025 3:48:40 PM | False |

Showing 3 of 3

### Remediation Steps
Review the list and verify that all privileged accounts and groups that were recently created are valid. Ideally, all privileged account creation goes through an approval-based workflow and gets periodic attestation.

SECURITY INDICATOR

## Distributed COM Users group or Performance Log Users group are not empty

Pass

A+ 100%

SEVERITY
High

WEIGHT
6

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation
- Credential Access

MITRE D3FEND

- Harden - User Account Permissions

### Description
This indicator checks if either the Distributed COM Users group and/or Performance Log Users group in Active Directory are populated.

### Likelihood of Compromise
Members of the Distributed COM Users or Performance Log Users Groups can remotely trigger actions and relay the authentication of users connected to the target server, including Domain Controllers.

### References
Hello: I'm your Domain Admin and I want to authenticate against you

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Unprivileged accounts with adminCount=1

Pass

A+ 100%

SEVERITY
Low

WEIGHT
3

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation

### Description
This indicator looks for any users or groups that may have been under the control of SDProp (adminCount=1) but are no longer members of privileged groups and should not be considered privileged.

### Likelihood of Compromise
The most common scenario for this behavior is if a user is moved from a privileged group to a non-privileged one and their adminCount variable is not reset. While this is benign, it may cause issues for security controls that monitor privileged users and reduces the overall hygiene of the environment. In rare cases, this might also be evidence of an attacker that attempted to cover their tracks and remove a user they used for compromise.

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Users and computers with non-default Primary Group IDs

Pass

A+ 100%

SEVERITY
Low

WEIGHT
3

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation

ANSSI

- vuln1_primary_group_id_1000
- vuln3_primary_group_id_nochange

### Description
This indicator returns a list of users and computers whose Primary Group IDs (PGIDs) are not the defaults for domain users and computers. Users created in the domain will have a default PGID of 513 (Domain Users) or 514 (Domain Guests) while computers are 515 (Domain Computers), 516 (Domain Controllers), or 521 (RODC). The Primary Group ID is not automatically changed when a user is moved to a different group (i.e. a user moved into Domain Admins will not be assigned PGID 512). This fact can be used to hide users with privileges to systems that rely on PGID, while hiding the user from queries that rely on enumerating the member attribute without the PGID. Additionally, group objects' member attribute will not list the user objects with PGID of those groups.

### Likelihood of Compromise

Modifying the Primary Group ID is a stealthy way for an attacker to escalate privileges without triggering member attribute auditing for group membership changes.

**References**

Accounts with PrimaryGroupID lower than 1000 | ANSSI
Accounts with modified PrimaryGroupID | ANSSI

**Result**

No evidence of exposure.

**Remediation Steps**

None

SECURITY INDICATOR

## Users and computers without readable PGID

Pass

A+ 100%

SEVERITY
Medium

WEIGHT
5

**Security Frameworks**

MITRE ATT&CK

- Defense Evasion

**Description**

This indicator finds users and computers for whom it can't read the PGID. This may be due to the default permission of Read access having been removed, which could indicate an attempt to hide the user (in combination with removal of the memberOf attribute).

**Likelihood of Compromise**

Can be used for hiding users in certain groups (non SDProp protected).

**Result**

No evidence of exposure.

**Remediation Steps**

None

SECURITY INDICATOR

## Users with old passwords

Pass

A+ 100%

SEVERITY
Low

WEIGHT
2

**Security Frameworks**

MITRE ATT&CK

- Credential Access
- Persistence

MITRE D3FEND

- Harden - Strong Password Policy

**Description**

This indicator looks for user accounts whose password has not changed in over 180 days. This could make these account ripe for password guessing attacks.

**Likelihood of Compromise**

Stale passwords that aren't changed over a long period of time and are not supported by multi-factor authentication are ripe targets for attackers. These present opportunities for attackers to move laterally through the environment or elevate privileges.

**References**

NIST.SP.800-63-3

**Result**

No evidence of exposure.

**Remediation Steps**

None

SECURITY INDICATOR

## Admins with old passwords

Pass

A+ 100%

SEVERITY
Low

WEIGHT
2

### Security Frameworks
MITRE ATT&CK

- Discovery

MITRE D3FEND

- Harden - Strong Password Policy

ANSSI

- vuln1_password_change_priv

### Description
This indicator looks for admin accounts whose password has not changed in over 180 days. This could make these accounts ripe for password guessing attacks.

### Likelihood of Compromise
An administrator account whose password hasn't changed in a while could be a target for attackers looking for privileged accounts that can provide elevated access to the environment.

### References
NIST.SP.800-63-3
Privileged account passwords age too old | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Operators Groups that are not empty

Pass

A+ 100%

SEVERITY
High

WEIGHT
6

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation
- Credential Access

MITRE D3FEND

- Harden - User Account Permissions

### Description
This indicator checks if the Account Operators, Server Operators, Backup Operators and Print Operators groups in Active Directory are populated.

### Likelihood of Compromise
The operator groups in Active Directory, Account Operators, Server Operators, Backup Operators, and Print Operators, all provide users within these groups certain privileges over different critical domain resources in Active Directory and different levels of access to domain controllers.
An attacker may target users in these groups for further privilege escalation and lateral movement in Active Directory.

### References
Active Directory security groups | Microsoft Learn

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Changes to Pre-Windows 2000 Compatible Access Group membership

IOE Found

B-
91 %

SEVERITY
Medium

WEIGHT
5

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation

### Description
This indicator looks for changes to the built-in group "Pre-Windows 2000 Compatible Access". This group grants read-only access to Active Directory.

### Likelihood of Compromise
As part of a layered approach to security and to ensure that non-authenticated users cannot read Active Directory, it's best to ensure this group does not contain the "Anonymous Logon" or "Everyone" groups.

### References
Understanding the Risks of Pre-Windows 2000 Compatible Access Settings | Semperis blog

### Result
Found 1 objects in the Pre-Windows 2000 Compatible Access group.

| DistinguishedName | Member | Operation | EventTimestamp | Ignored |
|---|---|---|---|---|
| CN=Pre-Windows 2000 Compatible Access,CN=Builtin,DC=myzo,DC=local | NT AUTHORITY\Authenticated Users | Risky Member Added During Domain Creation | 10/4/2025 3:01:33 AM | False |

Showing 1 of 1

### Remediation Steps
Confirm that any addition or removals from Pre-Windows 2000 Compatible Access group are valid and properly accounted for.

SECURITY INDICATOR

## Changes to privileged group membership in the last 7 days

IOE Found

D-
50 %

SEVERITY
Medium

WEIGHT
5

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation
- Persistence

### Description
This indicator looks for changes to the built-in privileged groups within the last 7 days, which could indicate attempts to escalate privilege.

### Likelihood of Compromise
Recent additions or deletions to privileged group members could be normal operational changes or could indicate attempts at persistence or cleaning up of tracks after an attack (e.g. detection of temporary group membership changes).

### Result
Found 6 changes on privileged groups' membership.

| DistinguishedName | MemberDistinguishedName | MemberSamAccountName | Operation | EventTimestamp | Ign |
|---|---|---|---|---|---|
| CN=Administrators,CN=Builtin,DC=myzo,DC=local | CN=Domain Admins,CN=Users,DC=myzo,DC=local | Domain Admins | Added | 10/4/2025 3:01:33 AM | Fals |
| CN=Administrators,CN=Builtin,DC=myzo,DC=local | CN=Enterprise Admins,CN=Users,DC=myzo,DC=local | Enterprise Admins | Added | 10/4/2025 3:01:33 AM | Fals |
| CN=Administrators,CN=Builtin,DC=myzo,DC=local | CN=Administrator,CN=Users,DC=myzo,DC=local | Administrator | Added | 10/4/2025 3:00:50 AM | Fals |
| CN=Domain Admins,CN=Users,DC=myzo,DC=local | CN=Administrator,CN=Users,DC=myzo,DC=local | Administrator | Added | 10/4/2025 3:01:33 AM | Fals |
| CN=Schema Admins,CN=Users,DC=myzo,DC=local | CN=Administrator,CN=Users,DC=myzo,DC=local | Administrator | Added | 10/4/2025 3:01:33 AM | Fals |

| DistinguishedName | MemberDistinguishedName | MemberSamAccountName | Operation | EventTimestamp | Ign |
|---|---|---|---|---|---|
| CN=Enterprise Admins,CN=Users,DC=myzo,DC=local | CN=Administrator,CN=Users,DC=myzo,DC=local | Administrator | Added | 10/4/2025 3:01:33 AM | Fals |

Showing 6 of 6

### Remediation Steps
Confirm that any additions/removals from privileged groups are valid and properly accounted for.

SECURITY INDICATOR

## Privileged Users with Weak Password Policy

IOE Found


SEVERITY
Critical

WEIGHT
8

### Security Frameworks
MITRE ATT&CK

- Discovery

MITRE D3FEND

- Harden - Strong Password Policy

ANSSI

- vuln2_privileged_members_password

### Description
This indicator looks for privileged users in each domain that don't have a strong password policy enforced, according to ANSSI framework. It checks both FGPP (Fine-Grained Password Policy) and the password policy applied to the domain. A strong password as defined by ANSSI is at least 8 characters long and updated no later than every 3 years.

### Likelihood of Compromise
Weak passwords are easier to crack via brute-force attacks, they can provide attackers opportunities for moving laterally or escalating privileges. The risk is even higher for privileged accounts, for when easily compromised, they improve the attacker's chance to quickly advance within the network.

### References
NIST.SP.800-63-3
Privileged group members with weak password policy | ANSSI

### Result
Found 2 privileged users who do not comply with strong password policies.

| DistinguishedName | PasswordPolicyDistinguishedName | MaxAge | MinAge | MinLength | ComplexityEnabled | History |
|---|---|---|---|---|---|---|
| CN=Administrator,CN=Users,DC=myzo,DC=local | DC=myzo,DC=local | 42 | 1 | 4 | False | 24 |
| CN=Lacie Monica,CN=Users,DC=myzo,DC=local | DC=myzo,DC=local | 42 | 1 | 4 | False | 24 |

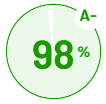
Showing 2 of 2

### Remediation Steps
Apply appropriate password policies for privileged users.

SECURITY INDICATOR

## Protected Users group not in use

IOE Found




SEVERITY
Informational

WEIGHT
1

### Security Frameworks
MITRE ATT&CK

- Credential Access

ANSSI

- vuln3_protected_users

### Description
This indicator checks if privileged users are in the Protected Users security group.

### Likelihood of Compromise
The Protected Users security group was introduced in Server 2012 R2 Active Directory to minimize credential exposure for privileged accounts. As a defense in depth measure privileged accounts, such as Domain Admins, should be added to the Protected

Users security group.
Attackers targeting privileged accounts in Active Directory will find a much higher level of friction in certain types of attempts to compromise the accounts due to the protections offered.

**References**

Protected Users Security Group | Microsoft Learn
Privileged accounts outside of the Protected Users group | ANSSI

**Result**

Found 2 privileged users that are not members of the Protected Users group.

| DistinguishedName | SamAccountName | Enabled | Ignored |
|---|---|---|---|
| CN=Administrator,CN=Users,DC=myzo,DC=local | Administrator | True | False |
| CN=Lacie Monica,CN=Users,DC=myzo,DC=local | lacie.monica | True | False |

Showing 2 of 2

**Remediation Steps**

Ensure that all privileged users are members of the Protected Users group. If using a pre 2012-R2 schema, then the protected users group does not exist. This is an exposure, but the remediation is to upgrade the schema.

SECURITY INDICATOR

## Recent SIDHistory changes on objects

Pass

A+ 100%

SEVERITY
Medium

WEIGHT
5

**Security Frameworks**

MITRE ATT&CK

- Privilege Escalation

ANSSI

- vuln2_sidhistory_dangerous

**Description**

This indicator checks for any recent changes to SIDHistory on objects.

**Likelihood of Compromise**

Security Identifier (SID) history is used by Active Directory to maintain access rights during domain migrations.
An attacker can abuse SID history by injecting a privileged SID into the SIDHistory of another user object, allowing the user to act with the same privileges. Writing to the SIDHistory does require privileges in Active Directory, so it is likely that Active Directory is already compromised; this method is primarily used by an attacker for gaining persistence.

**References**

How to Defend Against SID History Injection | Semperis Guides
Accounts or groups with unexpected SID history | ANSSI

**Result**

No evidence of exposure.

**Remediation Steps**

None

SECURITY INDICATOR

## Shadow Credentials on privileged objects

Pass

A+ 100%

SEVERITY
High

WEIGHT
6

**Security Frameworks**

MITRE ATT&CK

- Credential Access
- Lateral Movement

MITRE D3FEND

- Harden - User Account Permissions

**Description**

This indicator looks for users with write access to the msDS-KeyCredentialLink attribute of privileged users and DCs.

**Likelihood of Compromise**

Attackers who can write to these privileged objects and Kerberos PKINIT is enabled will be able to elevate privileges to them.

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## User accounts using Smart Card authentication with old password

Pass

A+ 100%

SEVERITY
High

WEIGHT
6

### Security Frameworks
MITRE ATT&CK

- Credential Access

MITRE D3FEND

- Harden - Credential Rotation

### Description
This indicator looks for user accounts that are using Smart Card authentication whose password has not changed in the last 90 days.

### Likelihood of Compromise
A user may use a Smart Card for authentication instead of a password. By default, accounts with the "Smart Card required" flag enabled have disabled password rotation, which may weaken your organization's password rotation practices. This static password hash is used for signing Kerberos tickets and if compromised may lead to credential-theft based attacks including Silver Ticket attacks.

### References
Set-ADDomain

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Trust accounts with old passwords

Pass

A+ 100%

SEVERITY
Low

WEIGHT
3

### Security Frameworks
MITRE ATT&CK

- Initial Access

MITRE D3FEND

- Harden - Strong Password Policy

ANSSI

- vuln2_trusts_accounts

### Description
This indicator looks for trust accounts whose password has not changed within the last year. This could mean that a trust relationship was removed but its corresponding trust account wasn't cleaned up.

### Likelihood of Compromise
Trust accounts facilitate authentication across trusts. As such they should be protected just like privileged user accounts. Normally trust account passwords are rotated automatically so a trust account without a recent password change could indicate an orphaned trust account.

### References
NIST.SP.800-63-3
Trust account passwords unchanged for more than a year | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Unprivileged principals as DNS Admins

IOE Found


SEVERITY
High

WEIGHT
7

### Security Frameworks
MITRE ATT&CK

- Execution
- Privilege Escalation

ANSSI

- vuln1_permissions_msdns
- vuln1_dnsadmins

### Description
This indicator looks for any member of the DnsAdmins group that is not a privileged user. DnsAdmins itself is not considered a privileged group and is not protected by the AdminSDHolder SDProp mechanism. However as some research has shown, a member of this group can remotely load a DLL onto a domain controller running DNS and execute code as SYSTEM.

### Likelihood of Compromise
Administration of DNS is often delegated to non-AD administrators (i.e., administrators with job responsibilities in networking, DNS, DHCP, etc.). These administration accounts may not have the same security controls as the AD administrator accounts, making them prime targets for compromise.

### References
How Potential Attackers Can Achieve Privileged Persistence on a DC through DnsAdmins | Semperis blog
Dangerous ACLs expose MicrosoftDNS server objects (attack path) | ANSSI
Dangerous permissions on the DnsAdmins group | ANSSI

### Result
Found 5 objects which are not privileged but are members of the DNS Admins group.

| DistinguishedName | SamAccountName | DomainName | Ignored |
|---|---|---|---|
| CN=Senior management,CN=Users,DC=myzo,DC=local | Senior management | myzo.local | False |
| CN=Letizia Deeanne,CN=Users,DC=myzo,DC=local | letizia.deeanne | myzo.local | False |
| CN=Becki Annabella,CN=Users,DC=myzo,DC=local | becki.annabella | myzo.local | False |
| CN=Merrielle Gisela,CN=Users,DC=myzo,DC=local | merrielle.gisela | myzo.local | False |
| CN=Fiorenze Nadia,CN=Users,DC=myzo,DC=local | fiorenze.nadia | myzo.local | False |

Showing 5 of 5

### Remediation Steps
Remove unprivileged principals that are a member of the DNS Admins group.

SECURITY INDICATOR

## User accounts that use DES encryption

Pass


SEVERITY
Medium

WEIGHT
4

### Security Frameworks
MITRE ATT&CK

- Credential Access

ANSSI

- vuln2_kerberos_properties_deskey

### Description
This indicator identifies user accounts with the "Use Kerberos DES encryption types for this account" flag set. DES is an older cipher with a 56-bit key length that is relatively easy to crack. The only legitimate use for this flag is to support older systems and environments that only support DES.

### Likelihood of Compromise
Attackers can easily crack DES passwords using widely available tools, making these accounts ripe for takeover.

### References

Use of Kerberos with weak encryption | ANSSI

**Result**
No evidence of exposure.

**Remediation Steps**
None

SECURITY INDICATOR

## Users with Password Never Expires flag set

Pass

A+ 100%

SEVERITY
Informational

WEIGHT
1

**Security Frameworks**
MITRE ATT&CK

- Credential Access

MITRE D3FEND

- Harden - Strong Password Policy

ANSSI

- vuln2_dont_expire

**Description**
This indicator identifies user accounts where the Password Never Expires flag is set. These accounts can be targets for brute force password attacks, given that their passwords may not be strong when they were set. These accounts also tend to be service accounts with privileged access to applications and services, including Kerberos-based services.

**Likelihood of Compromise**
Passwords that never expire may be weak and easier to crack. These credentials can provide attackers opportunities for moving laterally or escalating privileges.

**References**
NIST.SP.800-63-3
Accounts with never-expiring passwords | ANSSI

**Result**
No evidence of exposure.

**Remediation Steps**
None

SECURITY INDICATOR

## Privileged accounts with a password that never expires

Pass

A+ 100%

SEVERITY
High

WEIGHT
6

**Security Frameworks**
MITRE ATT&CK

- Credential Access
- Privilege Escalation

MITRE D3FEND

- Harden - Strong Password Policy

ANSSI

- vuln1_dont_expire_priv

**Description**
This indicator identifies privileged accounts (adminCount attribute set to 1) where the Password Never Expires flag is set.

**Likelihood of Compromise**
User accounts whose passwords never expire are ripe targets for brute force password guessing. If these users are also administrative or privileged accounts, this makes them even more of a target.

**References**
NIST.SP.800-63-3
Privileged accounts with never-expiring passwords | ANSSI

**Result**
No evidence of exposure.

**Remediation Steps**
None

SECURITY INDICATOR

## User accounts with password not required

Pass

A+ 100%

SEVERITY
High

WEIGHT
6

**Security Frameworks**
MITRE ATT&CK

- Lateral Movement

MITRE D3FEND

- Harden - Strong Password Policy

**Description**
This indicator identifies user accounts where a password is not required.

**Likelihood of Compromise**
Accounts with weak access controls are often targeted by attackers seeking to move laterally or gain a persistent foothold within the environment.

**References**
NIST.SP.800-63-3

**Result**
No evidence of exposure.

**Remediation Steps**
None

SECURITY INDICATOR

## User accounts that store passwords with reversible encryption

Pass

A+ 100%

SEVERITY
Medium

WEIGHT
4

**Security Frameworks**
MITRE ATT&CK

- Credential Access

MITRE D3FEND

- Harden - Strong Password Policy

ANSSI

- vuln3_reversible_password

**Description**
This indicator looks for user accounts with the ENCRYPTED_TEXT_PWD_ALLOWED flag enabled. The secure way of storing passwords is by utilizing one-way encryption where it is mathematically impossible to derive the original password from the ciphertext. This setting encrypts the source password such that it is possible to derive the original. This setting is used when an application or service utilizes authentication protocols that require the original password, e.g. CHAP or IAS.

**Likelihood of Compromise**
Attackers may be able to derive these users' passwords from the ciphertext and take over these accounts.

**References**
NIST.SP.800-63-3
Accounts with passwords stored using reversible encryption | ANSSI

**Result**
No evidence of exposure.

**Remediation Steps**
None

SECURITY INDICATOR

## Users with Kerberos pre-authentication disabled

IOE Found

B-
91 %

SEVERITY
Medium

WEIGHT
5

### Security Frameworks

MITRE ATT&CK

- Credential Access

ANSSI

- vuln1_kerberos_properties_preauth_priv
- vuln2_kerberos_properties_preauth

### Description

This indicator identifies users with Kerberos pre-authentication disabled, which exposes them to potential ASREP-Roasting attacks, such as 'Kerberoasting'.

### Likelihood of Compromise

If an account has Kerberos pre-authentication disabled, it makes it easier for attackers to send dummy requests to a DC to try and crack its Ticket Granting Ticket (TGT).

### References

Kerberos Pre-Authentication: Why It Should Not Be Disabled | Microsoft Learn
Kerberos preauthentication disabled for privileged accounts | ANSSI

### Result

Found 1 users with pre-authentication disabled.

| DistinguishedName | Ignored |
|---|---|
| CN=Halli Juditha,CN=Users,DC=myzo,DC=local | False |

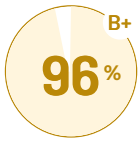
Showing 1 of 1

### Remediation Steps

Ensure that pre-authentication is enabled on all users if possible; if not possible, consider reducing their privileges instead.

CATEGORY

# AD INFRASTRUCTURE SECURITY




| WEIGHT | EVALUATED | INDICATORS FOUND |
|---|---|---|
| 7 | 33 | 2 |

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

SECURITY INDICATOR

## Unexpected accounts in Cert Publishers Group

Pass


SEVERITY
High

WEIGHT
6

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation
- Credential Access

MITRE D3FEND

- Harden - User Account Permissions

### Description
This indicator checks to see if the Cert Publishers Group contains members that aren't expected to be there.

### Likelihood of Compromise
Individuals belonging to Cert Publishers Group have the ability to introduce a potentially harmful Certificate Authority (CA) within an ADCS environment, that will be trusted by all clients. Although certificates issued by this CA may not receive automatic trust for client authentication via PKINIT or SChannel, they remain susceptible to exploitation for other malicious purposes. The combination of Cert Publishers membership and write access to NTAuthcertificates poses the greatest risk in such situations, allowing the forging and solicitation of certificates for client authentication against any user in the domain.

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Anonymous access to Active Directory enabled

Pass


SEVERITY
High

WEIGHT
7

### Security Frameworks
MITRE ATT&CK

- Defense Evasion
- Initial Access
- Persistence
- Privilege Escalation

MITRE D3FEND

- Harden - User Account Permissions

ANSSI

- vuln2_compatible_2000_anonymous

### Description
It is possible, though not recommended, to enable anonymous access to AD. This indicator looks for the presence of the flag that enables anonymous access. Anonymous access would allow unauthenticated users to query AD.

### Likelihood of Compromise
Anonymous access to Active Directory allows an attacker to enumerate accounts and perform attacks like password spray, as well as to enumerate the domain to gather information that can model attack paths. This is a significant risk as the complexity of AD often presents many opportunities for attackers and anonymous access allows them an easy way to find such opportunities.

### References
6.1.1.2.4.1.2 dSHeuristics | Microsoft Learn
The "Pre-Windows 2000 Compatible Access" group includes "Anonymous" | ANSSI

**Result**
No evidence of exposure.

**Remediation Steps**
None

SECURITY INDICATOR

## Anonymous NSPI access to AD enabled

Pass

A+ 100%

SEVERITY
High

WEIGHT
6

**Security Frameworks**
MITRE ATT&CK

- Initial Access

MITRE D3FEND

- Harden - User Account Permissions

ANSSI

- vuln1_dsheuristics_bad
- vuln2_dsheuristics_bad
- vuln3_dsheuristics_bad

**Description**
Anonymous name service provider interface (NSPI) access on AD is a feature that allows anonymous RPC-based binds to AD. This indicator detects when NSPI access is enabled.

**Likelihood of Compromise**
NSPI access is rarely ever enabled so if you find it enabled, this should be a cause for concern.
**References**
6.1.1.2.4.1.2 dSHeuristics | Microsoft Learn
Dangerous dsHeuristics settings | ANSSI

**Result**
No evidence of exposure.

**Remediation Steps**
None

SECURITY INDICATOR

## Dangerous control paths expose certificate containers

Pass

A+ 100%

SEVERITY
High

WEIGHT
7

**Security Frameworks**
MITRE ATT&CK

- Credential Access

MITRE D3FEND

- Harden - Credential Transmission Scoping

ANSSI

- vuln1_adcs_control

**Description**
This indicator looks for non-default principals with permissions on the NTAuthCertificates container. This container holds the intermediate CA certificates that can be used to authenticate to AD.

**Likelihood of Compromise**
These control paths allow adding a malicious certificate authority, which allow an attacker to authenticate as arbitrary users or services.
**References**
Dangerous ACLs expose certificate containers (attack path) | ANSSI

**Result**
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Certificate templates with 3 or more insecure configurations

Pass

A+ 100%

SEVERITY
High

WEIGHT
7

### Security Frameworks
MITRE ATT&CK

- Credential Access
- Privilege Escalation

MITRE D3FEND

- Detect - Certificate Analysis

ANSSI

- vuln1_adcs_template_auth_enroll_with_name

### Description
This indicator checks if certificate templates in the forest have a minimum of three insecure configurations - Manager approval is disabled, No authorized signatures are required, SAN enabled, Authentication EKU present.

### Likelihood of Compromise
The following configurations of a certificate template can be exploited by adversaries:
1. Manager approval is disabled - new certificates are automatically approved if the user has the correct enrollment rights.
2. No authorized signatures are required - CSRs (Certificate Signing Requests) are not signed by any existing authorized certificate.
3. SAN (Subject Alternative Name) Enabled - Allowing the creator of a certificate template to specify the subjectAltName in the CSR, thus they can make the request as anyone, even a domain admin.
4. Authentication EKU (Enhanced Key Usage) present - if present, the EKU created from the certificate template will allow the user to authenticate with it.

### References
NIST-SP1800-16B
Dangerous enrollment permission on authentication certificate templates | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Dangerous control paths expose certificate templates

Pass

A+ 100%

SEVERITY
High

WEIGHT
7

### Security Frameworks
MITRE ATT&CK

- Credential Access

ANSSI

- vuln1_adcs_template_control

MITRE D3FEND

- Detect - Certificate Analysis

### Description
This indicator looks for non-default principals with the ability to write properties on a certificate template.

### Likelihood of Compromise
Controlling certificate templates allows one to have the certificate authority issue an arbitrary certificate. It becomes possible to obtain a smartcard authentication certificate for any user, thus stealing his identity.

### References
NIST-SP1800-16B
Dangerous ACLs expose certificate template objects (attack path) | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Certificate templates that allow requesters to specify a subjectAltName

Pass

A+ 100%

SEVERITY
Critical

WEIGHT
8

### Security Frameworks
MITRE ATT&CK

- Credential Access
- Privilege Escalation

MITRE D3FEND

- Detect - Certificate Analysis

ANSSI

- vuln1_adcs_template_auth_enroll_with_name

### Description
This indicator checks if certificate templates are enabling requesters to specify a subjectAltName in the CSR.

### Likelihood of Compromise
When certificate templates allow requesters to specify a subjectAltName in the CSR, the result is that they can request a certificate as anyone. For example, a domain admin. When that is combined with an authentication EKU present in the certificate template it can become extremely dangerous.

### References
NIST-SP1800-16B
Dangerous enrollment permission on authentication certificate templates | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Computers with older OS versions

Pass

A+ 100%

SEVERITY
Medium

WEIGHT
4

### Security Frameworks
MITRE ATT&CK

- Lateral Movement
- Persistence

MITRE D3FEND

- Harden - Software Update

### Description
This indicator looks for machine accounts that are running versions of Windows older than Server 2012-R2 and Windows 8.1.

### Likelihood of Compromise
Computers running older and unsupported OS versions could be targeted with known or unpatched exploits.

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Computers with password last set over 90 days ago

Pass

A+ 100%

SEVERITY
High

WEIGHT
6

### Security Frameworks
MITRE ATT&CK

- Credential Access

MITRE D3FEND

- Harden - Strong Password Policy

ANSSI

- vuln2_password_change_server_no_change_90

### Description
This indicator looks for computer accounts that have not rotated their passwords in the last 90 days. These passwords should be changed automatically every 30 days by default.

### Likelihood of Compromise
Computer accounts should automatically rotate their passwords every 30 days as they are prime targets for attackers. Objects that are not doing this could show evidence of tampering.

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Domain Controllers with old passwords

Pass

A+ 100%

SEVERITY
Low

WEIGHT
3

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation
- Resource Development

MITRE D3FEND

- Harden - Strong Password Policy

ANSSI

- vuln1_password_change_dc_no_change

### Description
This indicator looks for domain controller machine accounts whose password has not been reset in over 45 days. By default, machine accounts including DCs, automatically reset their passwords every 30 days. Any machine accounts with passwords older than that could indicate a DC that is no longer functioning in the domain.

### Likelihood of Compromise
A DC that is not updating its machine account password regularly could be more easily taken over. From an operational standpoint, it could also indicate a communication problem with the rest of the domain.

### References
NIST.SP.800-63-3
Domain controllers with passwords unchanged for more than 45 days | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Dangerous Trust Attribute Set

Pass

A+ 100%

SEVERITY
High

WEIGHT
7

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation

MITRE D3FEND

- Harden - Domain Trust Policy

ANSSI

- vuln1_trusts_domain_notfiltered
- vuln3_trusts_tgt_deleg

### Description
This indicator identifies trusts set with either TRUST_ATTRIBUTE_CROSS_ORGANIZATION_ENABLE_TGT_DELEGATION or TRUST_ATTRIBUTE_PIM_TRUST. These bits will either allow a kerberos ticket to be delegated or reduce the protection that SID Filtering provides.

### Likelihood of Compromise
An attacker that has compromised a remote domain can spoof any user or machine in the local domain. This can allow the attacker to access any resource as well as escalate their privileges, thus compromising the entire forest.

### References
Unfiltered outbound domain trust relationship | ANSSI
Inbound trust relationships with delegation | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Print spooler service is enabled on a DC

IOE Found

D+ 73%

SEVERITY
Critical

WEIGHT
8

### Security Frameworks
MITRE ATT&CK

- Execution
- Lateral Movement
- Privilege Escalation

MITRE D3FEND

- Harden - Software Update

### Description
This indicator checks for Domain Controllers running the print spooler service.
This indicator **requires** the local server to be running the print spooler service to function, or it will return **Failed to run**.

### Likelihood of Compromise
The Windows print spooler service is vulnerable to remote code execution if unpatched, commonly referred to as **PrintNightmare**. These vulnerabilities are documented in CVE-2021-34527 and CVE-2021-1675.
The print spooler service can also be used by an attacker in combination with unconstrained Kerberos delegation and TGT delegation enabled across trusts.

### References
What You Need to Know about PrintNightmare, the Critical Windows Print Spooler Vulnerability - Semperis
CVE-2021-34527 - Security Update Guide - Microsoft - Windows Print Spooler Remote Code Execution Vulnerability
CVE-2021-1675 - Security Update Guide - Microsoft - Windows Print Spooler Remote Code Execution Vulnerability
CVE-2019-0683 - Security Update Guide - Microsoft - Active Directory Elevation of Privilege Vulnerability

### Result
Found 1 DCs that have the Print Spooler service running.

| HostName | Ignored |
|---|---|
| WIN-9R40GBIS0S3.myzo.local | False |

### Remediation Steps
Print spooler services are enabled by default. If not absolutely required, disable the service on all domain controllers. If required, make sure the server is fully patched and follow Microsoft guidance here.

SECURITY INDICATOR

## Evidence of Mimikatz DCShadow attack

Pass

A+ 100%

SEVERITY
Critical

WEIGHT
10

### Security Frameworks
MITRE ATT&CK

- Defense Evasion

MITRE D3FEND

- Isolate - Execution Isolation
- Detect - Domain Account Monitoring

### Description
This indicator checks for certain evidence of a DCShadow attack performed using Mimikatz.

### Likelihood of Compromise
DCShadow attacks allow attackers that have achieved privileged domain access to inject 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. Mimikatz is a widely used tool used by both legitimate pen-testers as well as attackers. An attacker will use a DCShadow attack to establish persistence in Active Directory, creating backdoors to retain access even if the original privileged access compromise is resolved

### References
Why Most Organizations Still Can't Defend against DCShadow - Semperis
Audit User Account Management - Windows 10 | Microsoft Learn

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Unsecured DNS configuration

Pass

A+ 100%

SEVERITY
High

WEIGHT
7

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation

ANSSI

- vuln1_dnszone_bad_prop
- vuln3_dnszone_bad_prop

### Description
This indicator looks for DNS zones configured with ZONE_UPDATE_UNSECURE, which allows updating a DNS record anonymously.

### Likelihood of Compromise
An attacker could leverage this exposure to arbitrarily add a new DNS record or replace an existing record to spoof a management interface, then wait for incoming connections in order to steal credentials.

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Domain Controllers in inconsistent state

Pass

A+ 100%

SEVERITY
Low

WEIGHT
3

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation
- Resource Development

ANSSI

- vuln1_dc_inconsistent_uac

### Description
This indicator looks for Domain Controllers that may be in an inconsistent state, indicating a possible rogue or otherwise non-functional DC. DCs in a consistent state are characterized by the following:
1. UserAccountControl attribute on the DC machine object has the SERVER_TRUST_ACCOUNT flag set.
2. A corresponding object of type server exists for the DC in the configuration partition.
3. That server object must have a child NTDS Settings object of type nTDSDSA.

### Likelihood of Compromise
Illegitimate machines acting as DCs could indicate someone has compromised the environment (e.g. using DCShadow or similar DC spoofing attacks). At the very least, partially functional legitimate DCs could represent a security risk if they are compromised.

### References
Domain controllers in inconsistent state | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Domains with obsolete functional levels

Pass

A+ 100%

SEVERITY
Low

WEIGHT
3

### Security Frameworks
MITRE ATT&CK

- Reconnaissance

MITRE D3FEND

- Harden - Software Update

ANSSI

- vuln1_functional_level
- vuln3_functional_level
- vuln4_functional_level

### Description
This indicator looks for AD domains that have a domain functional level set to Windows Server 2012 R2 or lower. These lower functional levels mean that newer security features available in AD cannot be leveraged. If the OS version of your domain controllers supports it, you should update to a newer domain functional level to take full advantage of security advancements in AD.

### Likelihood of Compromise
While domain functional level is not a weakness in and of itself, an attacker with knowledge of functional levels can adjust their approach to take advantage of lack of security features in AD.

### References
Forest and Domain Functional Levels
Insufficient forest and domains functional levels | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Operator groups no longer protected by AdminSDHolder and SDProp

Pass

A+ 100%

SEVERITY
Medium

WEIGHT
5

### Security Frameworks
MITRE ATT&CK

- Defense Evasion

MITRE D3FEND

- Harden - User Account Permissions

ANSSI

- vuln1_dsheuristics_bad
- vuln2_dsheuristics_bad
- vuln3_dsheuristics_bad

### Description
This indicator checks if dwAdminSDExMask mask on dsHeuristics has been set, which indicates a change to the SDProp behavior that could compromise security. Certain groups can be removed from SDProp protection with this setting.

### Likelihood of Compromise
Normally the default behavior for AdminSDHolder SDProp should be left intact. If its behavior is modified, this could indicate an attempt at defense evasion.

### References
6.1.1.2.4.1.2 dSHeuristics
Dangerous dsHeuristics settings | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## AD Certificate Authority with Web Enrollment - ESC8

Pass

A+ 100%

SEVERITY
Critical

WEIGHT
8

### Security Frameworks
MITRE ATT&CK

- Credential Access
- Privilege Escalation

### Description
This indicator attempts to identify AD CS servers in the domain that accept NTLM authentication to Web Enrollment Services. The script enumerates CAs in the Enrollment Services container, resolves their IP and attempts NTLM authentication to https://IP/certsrv and http://IP/certsrv. Note: This indicator currently does not identify EPA or other mitigations suggested by Microsoft.
The indicator will return a **Passed** if an enrollment service is contacted, but NTLM authentication is denied (positive effect on the posture score) for any endpoint.
The indicator will return an **IoE Found** if NTLM authentication is available on an enrollment service (negative effect on security posture) on any endpoint.
The indicator will **Fail to Run** (no effect on security posture score) if one of the following is true for all endpoints:

- **Cannot Resolve** - Enrollment Service Certificate found in AD CS container, but address cannot be resolved
- **Unreachable** - IP is resolved, but service cannot be reached

### Likelihood of Compromise
Attackers can exploit misconfigured Active Directory Certificate Services (AD CS) Web Enrollment to launch NTLM and Kerberos relay attacks, enabling them to authenticate as privileged users or computer accounts. One notable instance occurred in July 2021, when attackers combined this method with the PetitPotam attack on the MS-EFSRPC protocol, using only network access to coerce authentication. Other techniques allow any domain user to coerce a domain controller or computer account's authentication, relay it to AD CS Web Enrollment, and request a certificate for privileged access. This can ultimately result in domain takeover. For more information on this attack, often referred to as ESC8, consult detailed write-ups available online.

### References
KB5005413: Mitigating NTLM Relay Attacks on Active Directory Certificate Services (AD CS)

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Smart card password rotation disabled

Pass

A+ 100%

SEVERITY
Medium

WEIGHT
4

### Security Frameworks
MITRE ATT&CK

- Lateral Movement

ANSSI

- vuln4_smartcard_expire_passwords

### Description
This indicator checks whether the mcDS-ExpirePasswordsOnSmartCardOnlyAccounts attribute, which determines if smart card-only accounts must follow regular password rotation schedules, is disabled.

### Likelihood of Compromise
The msDS-ExpirePasswordsOnSmartCardOnlyAccounts attribute is a security configuration that determines if smart card-only accounts must follow regular password rotation schedules. When enabled, it ensures these specialized accounts comply with the domain's password policy. This security feature is available in domains operating at Windows Server 2016 functional level or higher. While not immediately indicative of an attack, when disabled, smart card-only accounts can maintain the same password indefinitely, potentially creating a security vulnerability that attackers can exploit for persistent access and lateral movement.

### References
Attribute msDS-ExpirePasswordsOnSmartCardOnlyAccounts
Missing password expiration for smart card users | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## gMSA objects with old passwords

Pass

A+ 100%

SEVERITY
High

WEIGHT
6

### Security Frameworks
MITRE ATT&CK

- Credential Access

### Description
This indicator looks for group managed service accounts that have not automatically rotated their passwords. These passwords should be changed automatically every 30 days by default.

### Likelihood of Compromise
gMSA accounts should automatically rotate their passwords every 30 days. Objects that are not doing this could show evidence of tampering.

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Domain Controllers that have not authenticated to the domain for more than 45 days

Pass

A+ 100%

SEVERITY
Medium

WEIGHT
4

### Security Frameworks
MITRE ATT&CK

- Credential Access
- Privilege Escalation

MITRE D3FEND

- Isolate - Execution Isolation

ANSSI

- vuln1_password_change_inactive_dc

### Description
Domain Controllers must authenticate and change their passwords at least every 30 days. Lack of domain authentication reveals out-of-sync machines. Out-of-sync domain controllers must be either reinstalled or removed. When reinstalling an out-of-sync domain controller, care must be taken not to introduce a new OWNER control path exposing its computer account. To avoid doing so, use of the Djoin utility is advised.

### Likelihood of Compromise
Domain Controllers that are not active in the domain would likely be out-of-sync with functional DCs and therefore a compromised offline DC may be of little value to an attacker. However, if an attacker could compromise an offline DC and crack credentials or re-connect it to the domain, they may be able to introduce unwanted changes to production AD that could compromise its security.

### References
Inactive domain controllers | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Query policies that have the attribute of LDAP deny list set

Pass

A+ 100%

SEVERITY
Medium

WEIGHT
5

### Security Frameworks
MITRE ATT&CK

- Impact

### Description
This security indicator is designed to check for LDAP IP deny lists across multiple domains in an Active Directory environment. For each available domain, it query the Active Directory for "query policies" associated with that domain, specifically looking for LDAP IP deny lists (ldapipdenylist attribute).

### Likelihood of Compromise
Unauthorized or unexpected entries in the LDAP IP deny list could suggest a security breach or an attempt to limit access to critical resources maliciously. The likelihood of compromise depends on the following factors:
1. Unexpected Changes: Unauthorized modifications to the LDAP IP deny list.
2. Unknown IP Addresses: Presence of IP addresses that are not recognized or authorized by the network administration team.
3. Security Policy Violations: Entries that violate the organization's established security policies.

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## LDAP signing is not required on Domain Controllers

IOE Found

C 82%

SEVERITY
High

WEIGHT
7

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation

- Credential Access

### Description
This indicator checks for domain controllers where LDAP signing is not required.

### Likelihood of Compromise
Unsigned network traffic is exposed to MiTM attacks, where attackers alter packets and forward them to the LDAP server, causing the server to make decisions based on forged requests from the LDAP client.

### References
Domain controller LDAP server signing requirements - Windows 10 | Microsoft Learn
Network security LDAP client signing requirements - Windows 10 | Microsoft Learn

### Result
Found 1 DCs that do not require LDAP Signing.

| DistinguishedName | HostName | State | Ignored |
|---|---|---|---|
| CN=WIN-9R40GBIS0S3,OU=Domain Controllers,DC=myzo,DC=local | WIN-9R40GBIS0S3.myzo.local | Ldap Signing Not Required | False |

Showing 1 of 1

### Remediation Steps
To remediate follow the steps below:
**If the steps are not followed in order, disruption to Active Directory may occur.**
1. Configure clients to request LDAP signing. Group policy: **Network security:LDAP client signing requirements**, select **Negotiate signing**.
2. When all clients request signing, configure domain controllers to require LDAP signing. Group policy: **Domain Controller:LDAP server signing requirements**, select **Require signing**.
3. Configure clients to require LDAP signing. Group policy: **Network security:LDAP client signing requirements**, select **Require signing**.
4. For full details on the process please see the reference articles.

SECURITY INDICATOR

## Non-standard schema permissions

Pass

A+ 100%

SEVERITY
High

WEIGHT
7

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation

ANSSI

- vuln1_permissions_schema
- vuln2_permissions_schema

MITRE D3FEND

- Harden - System Configuration Permissions

### Description
This indicator looks for additional principals with any permissions beyond generic Read to the schema partitions.Schema is one of three main Active Directory naming context. It contains every object attribute definitions of the forest.

### Likelihood of Compromise
By default, modification permissions on schema are limited to Schema Admins. These permissions grant the trusted Principal complete control over Active Directory.

### References
Dangerous ACLs expose schema objects (attack path) | vuln_permissions_schema | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## NTFRS SYSVOL Replication

Pass

A+ 100%

SEVERITY
High

WEIGHT
6

### Security Frameworks
MITRE ATT&CK

- Lateral Movement

ANSSI

- vuln2_sysvol_ntfrs

### Description
This indicator looks for indication of usage of FRS for sysvol replication. Domain Controllers are configured to use the NTFRS replication protocol (especially for SYSVOL replication). This protocol is obsolete and unnecessarily adds administrative interfaces to domain controllers. In addition, this protocol is no longer supported by the latest versions of Windows Server, which prevents migration to the latest versions.

### Likelihood of Compromise
NTFRS is an older protocol that has been replaced by DFSR. Attackers that can manipulate NTFRS vulnerabilities to compromise SYSVOL can potentially change GPOs and logon scripts to propagate malware and move laterally across the environment.

### References
Migrate SYSVOL replication to DFS Replication | Microsoft Learn
SYSVOL replication through NTFRS | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Outbound forest trust with SID History enabled

Pass

A+ 100%

SEVERITY
High

WEIGHT
6

### Security Frameworks
MITRE ATT&CK

- Lateral Movement

MITRE D3FEND

- Harden - Domain Trust Policy

ANSSI

- vuln1_trusts_forest_sidhistory

### Description
This indicator checks for outbound forest trusts that have the TRUST_ATTRIBUTE_TREAT_AS_EXTERNAL flag set to true.

### Likelihood of Compromise
If TRUST_ATTRIBUTE_TREAT_AS_EXTERNAL is set to true, the security of a cross-forest trust is relaxed and trusts are treated as equivalent to external trusts.
An attacker that compromises the remote Active Directory forest, with this set to true, can spoof most users and computers in the local Active Directory forest. This would allow the attacker to act as local users or computers and access resources they have privileges in. An attacker can also use this for privilege elevation and compromise the local forest.

### References
Active Directory Security Best Practices | Semperis
Outbound forest trust relationships with sID History enabled | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Domain trust to a third-party domain without quarantine

Pass

A+ 100%

SEVERITY
Medium

WEIGHT
5

### Security Frameworks
MITRE ATT&CK

- Lateral Movement

MITRE D3FEND

- Harden - Domain Trust Policy

ANSSI

- vuln1_trusts_domain_notfiltered

### Description
This indicator looks for outbound forest trusts that has Quarantine flag set to false, which means that the trusted domain is not subject to SID filtering.

### Likelihood of Compromise
An attacker having compromised the remote domain can spoof any user or machine on the local domain (except for accounts with a RID lower than 1000, excluding built-in accounts and groups). This attacker can therefore access every resource on the local domain. If a dangerous control path is exposed to any "spoofable" account (virtually any account other than the built-in ones), the attacker could also escalate his privileges up to "Domain Admins" and compromise the entire forest.

### References
Unfiltered outbound domain trust relationship | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Risky RODC credential caching

Pass A+ 100%

SEVERITY
Medium

WEIGHT
5

### Security Frameworks
MITRE ATT&CK

- Credential Access

MITRE D3FEND

- Harden - User Account Permissions

ANSSI

- vuln2_rodc_priv_revealed

### Description
This indicator checks the password replication policy on RODCs.

### Likelihood of Compromise
In many instances, read-only domain controllers (RODCs) are deployed in area where there is a lower level of physical security to the servers.
Attackers may try to target read-only domain controllers due to the lower level of security around these. While it is not a direct indicator of an attack, credentials for privileged users should not be cached on RODCs in the case the domain controller is compromised.

### References
RODC Features | Microsoft Learn
Dangerous configuration of read-only domain controllers (RODC) (neverReveal) | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Privileged user credentials cached on RODC

Pass A+ 100%

SEVERITY
Medium

WEIGHT
4

### Security Frameworks
MITRE ATT&CK

- Lateral Movement

- Privilege Escalation

### Description
This indicator checks for privileged user credentials that are cached to RODCs.

### Likelihood of Compromise
In many instances, read-only domain controllers (RODCs) are deployed in area where there is a lower level of physical security to the servers.
Attackers may try to target read-only domain controllers due to the lower level of security around these. While it is not a direct indicator of an attack, credentials for privileged users should not be cached on RODCs in the case the domain controller is compromised.

### References
RODC Features | Microsoft Learn

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Well-known privileged SIDs in SIDHistory

Pass

A+ 100%

SEVERITY
Critical

WEIGHT
10

### Security Frameworks
MITRE ATT&CK

- Defense Evasion
- Privilege Escalation

ANSSI

- vuln2_sidhistory_dangerous
- vuln3_sidhistory_present

### Description
This indicator checks security principal SIDHistory for well-known privileged SIDs.

### Likelihood of Compromise
Security Identifier (SID) history is used by Active Directory to maintain access rights during domain migrations.
An attacker can abuse SID history by injecting a privileged SID into the SIDHistory of another user object, allowing the user to act with the same privileges. Writing to the SIDHistory does require privileges in Active Directory, so it is likely that Active Directory is already compromised; this method is primarily used by an attacker for gaining persistence.

### References
How to Defend Against SID History Injection | Semperis Guides
Accounts or groups with unexpected SID history | ANSSI
Accounts or groups with SID history set | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## SMB Signing is not required on Domain Controllers

Pass

A+ 100%

SEVERITY
Critical

WEIGHT
8

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation
- Credential Access

### Description
This indicator looks for domain controllers where SMB signing is not required.

### Likelihood of Compromise

Unsigned network traffic is susceptible to attacks abusing the NTLM challenge-response protocol. A common example of such attacks is SMB Relay, where an attacker is positioned between the client and the server in order to capture data packets transmitted between the two, thus gaining unauthorized access to the server or other servers on the network.

**References**

Configure SMB Signing with Confidence

**Result**

No evidence of exposure.

**Remediation Steps**

None

SECURITY INDICATOR

## SMBv1 is enabled on Domain Controllers

Pass

A+ 100%

SEVERITY
Critical

WEIGHT
8

**Security Frameworks**

MITRE ATT&CK

- Privilege Escalation
- Credential Access

**Description**

This indicator looks for domain controllers where SMBv1 protocol is enabled.

**Likelihood of Compromise**

SMBv1 is an old protocol, considered unsafe and susceptible to all kinds of attacks. It was publicly deprecated by Microsoft in 2014.

**References**

Configure SMB Signing with Confidence

**Result**

No evidence of exposure.

**Remediation Steps**

None

SECURITY INDICATOR

## Weak certificate cipher

Pass

A+ 100%

SEVERITY
Critical

WEIGHT
8

**Security Frameworks**

MITRE ATT&CK

- Privilege Escalation

MITRE D3FEND

- Harden - Certificate-based Authentication

ANSSI

- vuln1_certificates_vuln

**Description**

This indicator looks for certificates stored in active directory with keysize smaller than 2048 bits or utilize DSA encryption.

**Likelihood of Compromise**

Weak certificates can be abused by attackers to gain access to systems who use certificate authentication.

**References**

Weak or vulnerable certificates | ANSSI

**Result**

No evidence of exposure.

**Remediation Steps**

None

SECURITY INDICATOR

## Zerologon vulnerability

Not Selected

N/A

SEVERITY
Critical

WEIGHT
10

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation

### Description
This indicator checks for security vulnerability CVE-202-1472.

### Likelihood of Compromise
Commonly referred to as **Zerologon**, CVE-2020-1472, is a vulnerability an attacker can use to gain Domain Administrator access against an unpatched domain controller. This vulnerability is considered critical because the attacker can perform the attack unauthenticated against Active Directory.

### References
CVE-2020-1472 - Security Update Guide - Microsoft - Netlogon Elevation of Privilege Vulnerability

CATEGORY

## GROUP POLICY SECURITY

A 99%

| WEIGHT | EVALUATED | INDICATORS FOUND |
|---|---|---|
| 5 | 11 | 1 |

Group Policy Security indicators pertain to the security configuration of GPOs and their deployment within AD.

SECURITY INDICATOR

### Changes to Default Domain Policy or Default Domain Controllers Policy in the last 7 days

IOE Found

C+ 88%

SEVERITY
Medium

WEIGHT
4

#### Security Frameworks
MITRE ATT&CK

- Lateral Movement
- Persistence

#### Description
The Default Domain Policy and Default Domain Controllers Policy GPOs are special objects within AD, and control domain-wide and Domain Controller wide security settings. This indicator looks for changes to these two special GPOs within the last 7 days.

#### Likelihood of Compromise
Changes to the Default Domain Policy or Default Domain Controllers Policy should be accounted for by the administrators. If the change can not be accounted for, investigate the change looking for potential weakening of security posture and why the change was made.

#### Result
Found 2 sensitive policies in the organization that have been changed in the last 7 days.

| Version | GPOName | DomainName | EventTimestamp | Ignored |
|---|---|---|---|---|
| 4 | CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=myzo,DC=local | myzo.local | 10/4/2025 6:48:30 AM | False |
| 1 | CN={6AC1786C-016F-11D2-945F-00C04fB984F9},CN=Policies,CN=System,DC=myzo,DC=local | myzo.local | 10/3/2025 6:00:49 PM | False |

Showing 2 of 2

#### Remediation Steps
Review the changes and ensure that any changes to these two GPOs have gone through well-known change processes and that any changes made to these GPOs are well-documented. Investigate any undocumented changes.

SECURITY INDICATOR

### Writable shortcuts found in GPO

Pass

A+ 100%

SEVERITY
High

WEIGHT
6

#### Security Frameworks
MITRE ATT&CK

- Privilege Escalation
- Lateral Movement

MITRE D3FEND

- Detect - Script Execution Analysis
- Detect - File Creation Analysis

#### Description
This indicator looks for shortcuts within Group Policy Objects (GPOs) that are writable by low privilege users. GPOs are a powerful feature in Windows domains that are used to manage various settings and configurations for multiple computers and users. Shortcuts are links to files or applications that can be deployed using GPOs. When low privilege users have the ability to modify these shortcuts, it could potentially lead to security risks and unauthorized modifications. This indicator helps organizations to identify such misconfigurations and take appropriate actions.

#### Likelihood of Compromise
Changing a shortcut within a GPO, allows an attacker to perform the following:

- Unauthorized Modifications - Low privilege users could make unauthorized changes to the files, compromising their integrity and potentially causing unintended behavior or security vulnerabilities.
- Malicious Content Execution - If the files are replaced with malicious content, all users running them could unknowingly execute malicious code, leading to system compromise or unauthorized access to sensitive information.
- System Instability - Unauthorized modifications to files can result in system instability, causing application errors, data corruption, or system crashes.
- Compliance and Legal Consequences - If the affected files are critical for compliance or legal requirements, unauthorized modifications may lead to non-compliance, financial losses, reputational damage, or legal repercussions.

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Dangerous GPO logon script path

Pass

A+ 100%

SEVERITY
High

WEIGHT
7

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation
- Lateral Movement

MITRE D3FEND

- Detect - Script Execution Analysis
- Detect - File Creation Analysis

### Description
This indicator searches for logon script paths where the script does not exist and where a low-privilege user has permissions on the parent folder. Additionally, it checks for logon script paths where the script exists but low-privilege users have permissions to modify them.

### Likelihood of Compromise
By inserting a new logon script or changing an existing one using normal user that has the permissions to do so, an attacker can remotely run code on a larger part of the network without special privileges.

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## GPO with Scheduled Tasks configured

Pass

A+ 100%

SEVERITY
Low

WEIGHT
2

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation
- Lateral Movement

MITRE D3FEND

- Detect - Script Execution Analysis
- Detect - File Creation Analysis

### Description
When a scheduled task launches an executable, it checks to see if low-privilege users have permissions to modify GPOs.

### Likelihood of Compromise
Scheduled tasks configured through group policies can be risky if not set up correctly. They can cause unintended problems and potential security vulnerabilities in the following situations:
- **Missing path specification for executable files launched by the Task Scheduler:** When setting up a scheduled task, it's important to provide the complete path to the executable file. This helps reduce the risk of path manipulation attacks. Path manipulation involves manipulating the search path or taking advantage of vulnerabilities in the path resolution mechanism to execute a malicious program. By explicitly specifying the complete path, you minimize the reliance on potentially vulnerable search

path resolution mechanisms and decrease the chances of path manipulation exploits.

- **Executables located in unsecure locations:** If scheduled tasks are configured to launch executables from locations where standard users have write access, it poses a potential risk. Standard users having write access to these directories can replace the intended program with a malicious one. This can lead to privilege escalation, where the malicious program gains higher privileges than it should have, resulting in security breaches and compromising the system's security.

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Dangerous user rights granted by GPO

Pass

A+ 100%

SEVERITY
High

WEIGHT
7

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation

MITRE D3FEND

- Detect - Local Account Monitoring
- Harden - Strong Password Policy

### Description
Group Policy Objects (GPOs) are used to define security settings that apply to a group of users or computers in an Active Directory environment. GPOs can be used to grant dangerous user rights, such as the ability to bypass file system security, log on as a service, or even perform actions with elevated privileges. This indicator looks for non-privileged users who are granted elevated permissions through GPO.

### Likelihood of Compromise
An attacker can potentially exploit the user rights granted by a GPO to gain access to systems, steal sensitive information, or cause other types of damage. If these dangerous user rights are granted to a user or a group of users, it increases the risk of an attacker being able to gain access to sensitive data, systems or even perform malicious actions.

### References
MS User Rights Assignment

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## GPO Weak LM Hash storage enabled

Pass

A+ 100%

SEVERITY
High

WEIGHT
6

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation

MITRE D3FEND

- Harden - Strong Password Policy

### Description
This indicator detects when the "Network security: Do not store LAN Manager hash value on next password change" Group Policy Object setting is disabled within the Windows operating system.

### Likelihood of Compromise
When the "Network security: Do not store LAN Manger hash value on next password change" setting is disabled, LAN Manager (LM) hashes continue to be stored during password changes. Enabling this setting strengthens security by preventing the storage of weak LM hashes and promoting the use of stronger password storage mechanisms. If an attacker gains access to the system or manages to extract the stored LM hashes, they can employ offline cracking techniques to obtain the original passwords. Therefore, monitoring and enabling this setting is crucial for mitigating the risk of unauthorized access and data breaches caused by the exploitation of weak LM hashes.

### References

MS GPO information

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Reversible passwords found in GPOs

Pass

A+ 100%

SEVERITY
Critical

WEIGHT
8

### Security Frameworks
MITRE ATT&CK

- Credential Access

MITRE D3FEND

- Detect - Emulated File Analysis

### Description
This indicator looks in SYSVOL for GPOs that contain passwords that can be easily decrypted by an attacker ("Cpassword" entries). Until patch MS14-025, it was possible to store local admin and other high-value credentials in GPOs. The passwords stored in GPOs were encrypted using a global key that was published and easily available to any domain member for decryption.

### Likelihood of Compromise
Many shops stopped using the feature in GP Preferences to set passwords when Microsoft deprecated the feature in Group Policy, but existing password entries may not have been removed. This area is one of the first things attackers look for when they've gained access to an AD environment, as older systems may still utilize those credentials.

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## SYSVOL Executable Changes

Pass

A+ 100%

SEVERITY
Low

WEIGHT
3

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation
- Execution
- Persistence

MITRE D3FEND

- Detect - File Analysis

### Description
This indicator looks for modifications to executable files within SYSVOL. It only examines files and executables that have read access to them.

### Likelihood of Compromise
Changes to the executable files within SYSVOL should be accounted for by the administrators. If the change can not be accounted for, investigate the change looking for potential weakening of security posture and why the change was made.

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## GPO linking delegation at the AD Site level

Pass

A+ 100%

SEVERITY
High

WEIGHT
7

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation
- Execution

ANSSI

- vuln1_permissions_gpo_priv

### Description
When non-privileged users can link GPOs at the AD Site level, they have the ability to effect change on domain controllers as well as potentially elevate access and change domain-wide security posture. This indicator looks for non-default principals who have write permissions on the GPLink attribute or Write DACL/Write Owner on the object.

### Likelihood of Compromise
Just being able to link GPOs doesn't provide the whole picture. An attacker would need to find or edit a GPO that contains the instructions they want to achieve. However, if an attacker can find an existing GPO that meets their needs, then having this write permission gives them the keys to the kingdom.

### References
Dangerous ACLs expose GPOs applied to privileged group members (attack path) | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## GPO linking delegation at the domain controller OU level

Pass

A+ 100%

SEVERITY
High

WEIGHT
7

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation
- Execution

ANSSI

- vuln1_permissions_gpo_priv

### Description
When non-privileged users can link GPOs at the Domain Controllers OU level, they have the ability to effect change on domain controllers as well as potentially elevate access and change domain-wide security posture. This indicator looks for non-default principals who have write permissions on the GPLink attribute or Write DACL/Write Owner on the object.

### Likelihood of Compromise
Just being able to link GPOs doesn't provide the whole picture. An attacker would need to find or edit a GPO that contains the instructions they want to achieve. However, if an attacker can find an existing GPO that meets their needs, then having this write permission gives them the keys to the kingdom.

### References
Dangerous ACLs expose GPOs applied to privileged group members (attack path) | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## GPO linking delegation at the domain level

Pass

A+ 100%

SEVERITY
High

WEIGHT
7

### Security Frameworks
MITRE ATT&CK

- Defense Evasion
- Privilege Escalation

ANSSI

- vuln1_permissions_gpo_priv

### Description
When non-privileged users can link GPOs at the domain level, they have the ability to effect change across all users and computers in the domain as well as potentially elevate access and change domain-wide security posture. This indicator looks for non-default principals who have write permissions on the GPLink attribute or Write DACL/Write Owner on the object.

### Likelihood of Compromise
Just being able to link GPOs doesn't provide the whole picture. An attacker would need to find or edit a GPO that contains the instructions they want to achieve. However, if an attacker can find an existing GPO that meets their needs, then having this write permission gives them the keys to the kingdom.

### References
Dangerous ACLs expose GPOs applied to privileged group members (attack path) | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

CATEGORY

# KERBEROS SECURITY

A 99%

| WEIGHT | EVALUATED | INDICATORS FOUND |
|---|---|---|
| 8 | 19 | 1 |

Kerberos Security indicators pertain to the configuration of Kerberos capabilities on computer and user accounts within AD.

SECURITY INDICATOR

## Accounts with altSecurityIdentities configured

Pass A+ 100%

| SEVERITY | WEIGHT |
|---|---|
| High | 7 |

### Security Frameworks

MITRE ATT&CK

- Privilege Escalation

ANSSI

- vuln1_delegation_a2d2

### Description

It is possible to add values to the altSecurityIdentities attribute and essentially impersonate that account. The altSecurityIdentities attribute is a multi-valued attribute used to create mappings for X.509 certificates and external Kerberos accounts. This indicator checks for accounts with the altSecurityIdentities attribute configured.

### Likelihood of Compromise

This type of attack may be easy to spot as it is rarely configured during normal operations. However, it is possible for this attribute to be configured genuinely.

### References

Constrained authentication delegation to a domain controller service | ANSSI

### Result

No evidence of exposure.

### Remediation Steps

None

SECURITY INDICATOR

## Computer or user accounts with SPN that have unconstrained delegation

Pass A+ 100%

| SEVERITY | WEIGHT |
|---|---|
| Medium | 4 |

### Security Frameworks

MITRE ATT&CK

- Defense Evasion
- Lateral Movement

MITRE D3FEND

- Detect - Domain Account Monitoring

ANSSI

- vuln2_delegation_t4d

### Description

This indicator looks for computer or user accounts with SPN 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.

### References

audit-user-account-management of Microsoft
Unconstrained authentication delegation | ANSSI

**Result**
No evidence of exposure.

**Remediation Steps**
None

SECURITY INDICATOR

## Accounts with Constrained Delegation configured to krbtgt

Pass

A+ 100%

SEVERITY
Critical

WEIGHT
9

**Security Frameworks**
MITRE ATT&CK

- Privilege Escalation

MITRE D3FEND

- Detect - Domain Account Monitoring

ANSSI

- vuln1_delegation_a2d2

**Description**
This indicator checks for accounts that have constrained delegation configured to the KRBTGT account.

**Likelihood of Compromise**
In Active Directory it is possible to create a Kerberos delegation to the KRBTGT account. This type of delegation to a user or computer would allow that principal to generate a ticket granting service (TGS) request to the KRBTGT account as any user. An attacker may attempt to compromise any account that has a delegation to the KRBTGT account. This particular type of configuration allows for an attack similar to a Golden Ticket attack.

**References**
Constrained authentication delegation to a domain controller service | ANSSI

**Result**
No evidence of exposure.

**Remediation Steps**
None

SECURITY INDICATOR

## Accounts with Constrained Delegation configured to ghost SPN

Pass

A+ 100%

SEVERITY
High

WEIGHT
6

**Security Frameworks**
MITRE ATT&CK

- Privilege Escalation

ANSSI

- vuln1_delegation_a2d2

**Description**
When computers are decommissioned, delegation configuration to them is often not cleaned up. Such a delegation could allow an attacker that has the privileges to write to the ServicePrincipalName attribute of another service account, to escalate privileges on those services. This could result in escalating privileges by moving laterally across the infrastructure. This indicator looks for accounts that have Constrained Delegation configured to ghost SPNs.

**Likelihood of Compromise**
This type of attack should be easy to spot as the configured SPN within the msds-allowedtodelegateto attribute will not exist on the domain. However, if they are found, they would represent a significant risk and should be mitigated quickly.

**References**
Constrained authentication delegation to a domain controller service | ANSSI

**Result**
No evidence of exposure.

**Remediation Steps**
None

SECURITY INDICATOR

## Kerberos KRBTGT account with old password

Pass

A+ 100%

SEVERITY
Medium

WEIGHT
4

### Security Frameworks
MITRE ATT&CK

- Credential Access

MITRE D3FEND

- Harden - Strong Password Policy

ANSSI

- vuln2_krbtgt

### Description
This indicator checks the age of the password on the KRBTGT account.

### Likelihood of Compromise
The KRBTGT user account is a special user account in Active Directory that is a service account for the Key Distribution Center (KDC).
If an attacker is able to compromise the KRBTGT account, they will be able to perform golden ticket attacks in Active Directory, which allow the attacker to impersonate any user.
Beyond rotating the password twice a year, it is recommended that the password is rotated every time someone who had privileged access in Active Directory, such as a Domain Admin, leaves the organization. There are specific steps that are required to successfully rotate the KRBTGT password, please see the reference article from Semperis for further details.

### References
How to Defend Against Golden Ticket Attacks on Active Directory - Semperis
Active Directory Accounts | Microsoft Learn
Krbtgt account password unchanged for more than a year | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Objects with constrained delegation configured

Pass

A+ 100%

SEVERITY
Medium

WEIGHT
5

### Security Frameworks
MITRE ATT&CK

- Lateral Movement
- Privilege Escalation

MITRE D3FEND

- Detect - Domain Account Monitoring

### Description
This indicator looks for any objects that have values in the msDS-AllowedToDelegateTo attribute (i.e. Constrained Delegation) and does not have the UserAccountControl bit for protocol transition set.

### Likelihood of Compromise
Attackers may utilize delegations to move laterally or escalate privileges if they compromise a service that is trusted to delegate. While constrained delegation is less likely to be compromised than unconstrained delegation, knowing all of the accounts within your environment that have this defined and ensuring they have strong passwords is a good thing.

### References
audit-user-account-management of Microsoft

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Principals with constrained authentication delegation enabled for a DC service

Pass

A+ 100%

SEVERITY
High

WEIGHT
6

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation

MITRE D3FEND

- Detect - Domain Account Monitoring

### Description
This indicator looks for principals (computers or users) that have constrained delegation enabled for a service running on a DC. If an attacker can create such a delegation, they can authenticate to that service using any user that is not protected against delegation.

### Likelihood of Compromise
Constrained delegation allows a service to act on behalf of an authenticated user to another service. While this is sometimes necessary and requires the user to authenticate to the delegating service first, delegation to such services on domain controllers greatly increases risk. An attacker that is able to compromise such a service can significantly elevate their privileges in this way and infiltrate Active Directory.

### References
audit-user-account-management of Microsoft

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Kerberos protocol transition delegation configured

Pass

A+ 100%

SEVERITY
High

WEIGHT
6

### Security Frameworks
MITRE ATT&CK

- Credential Access
- Lateral Movement
- Privilege Escalation

### Description
This indicator looks for services that have been configured to allow Kerberos protocol transition. This capability enables a delegated service to use any available authentication protocol. This means that compromised services can reduce the quality of their authentication protocol to something that is more easily compromised (e.g. NTLM).

### Likelihood of Compromise
Protocol transition is not often used but when it is, it should be monitored closely for signs of abuse. In addition to compromising the authentication strength, this setting also allows attackers to request delegations with no authentication.

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Principals with constrained delegation using protocol transition enabled for a DC service

Pass

A+ 100%

SEVERITY
High

WEIGHT
7

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation

ANSSI

- vuln1_delegation_t2a4d

### Description
This indicator looks for principals (computers or users) that have constrained delegation using protocol transition defined against a service running on a DC.

### Likelihood of Compromise
Protocol transition (also known as T2A4D) allows any user to authenticate to a delegated service using any protocol such as NTLM. This allows the delegated service to request a TGS from Kerberos for any user without any proof such as that user's corresponding TGT or TGS. If an attacker can create such a delegation for a service that they control or compromise an existing service, they can effectively gain a TGS for any user with privileges to the DC.

### References
Constrained delegation with protocol transition to a privileged service | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Users with SPN defined

Pass

A+ 100%

SEVERITY
Low

WEIGHT
3

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation

MITRE D3FEND

- Detect - Domain Account Monitoring

### Description
This indicator provides a way to visually inventory all users accounts that have SPNs defined. Generally SPNs are only defined for "Kerberized" services, so if you see an account with an SPN that should not have one, this could be cause for concern.

### Likelihood of Compromise
SPNs are generally only defined for service accounts or other services that use Kerberos. If you see SPNs on other accounts, they are worth investigating to determine if they are just an administrative error.

### References
Audit User Account Management

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Primary users with SPN not supporting AES encryption on Kerberos

Pass

A+ 100%

SEVERITY
Medium

WEIGHT
5

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation
- Credential Access

ANSSI

- vuln3_kerberos_properties_encryption

### Description
This indicator shows all Primary users with SPNs that do not support AES-128 or AES-256 encryption type.

### Likelihood of Compromise
AES encryption is stronger than RC4 encryption. Configuring primary users with SPN to support AES encryption will not mitigate attacks such as Kerberoasting but does force AES by default, meaning that it is possible to monitor for encryption downgrade attacks to RC4 (Kerberoasting attacks)

### References
Network security: Configure encryption types allowed for Kerberos | Microsoft Learn
Service accounts supported encryption algorithms | ANSSI
Kerberos preauthentication disabled | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Privileged users with SPN defined

Pass

A+ 100%

SEVERITY
High

WEIGHT
6

### Security Frameworks
MITRE ATT&CK

- Credential Access
- Privilege Escalation

ANSSI

- vuln1_spn_priv

### 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.

### References
Privileged accounts with SPN | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Computer account takeover through Kerberos Resource-Based Constrained Delegation (RBCD)

Pass

A+ 100%

SEVERITY
Medium

WEIGHT
5

### Security Frameworks
MITRE ATT&CK

- Credential Access
- Lateral Movement
- Privilege Escalation

### Description
With sufficient permissions on a computer account and the ability to create another user or computer security principal, it is possible to compromise resources on that computer account using Kerberos resource-based constrained delegation (RBCD). This indicator looks for the msDS-AllowedToActOnBehalfOfOtherIdentity attribute on computer objects.

### Likelihood of Compromise
Attackers may utilize Kerberos RBCD configuration to escalate privileges through a computer they control if that computer has delegation to the target service.

### Result

No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Domain Controllers with Resource-Based Constrained Delegation (RBCD) enabled

Pass

A+ 100%

SEVERITY
High

WEIGHT
6

### Security Frameworks
MITRE ATT&CK

- Defense Evasion
- Lateral Movement
- Privilege Escalation

ANSSI

- vuln1_delegation_sourcedeleg

### Description
This indicator detects a configuration that grants certain accounts with complete delegation to domain controllers. Delegations towards privileged resources such as DCs should be avoided. Resource-based constrained delegation is configured on the target resource, as opposed to other delegation types that are configured on the accounts accessing the resource.

### Likelihood of Compromise
An attacker needs to know the Service Principal Name (SPN) of the object they want to delegate, as well as be able to populate the msDS-AllowedToActOnBehalfOfOtherIdentity attribute with a computer account that they control. This is sometimes possible when unprivileged users are by default allowed to create computer accounts (MachineAccountQuota) and write the attribute to the target computer.

### References
Resource-based constrained delegation on domain controllers | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

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

Pass

A+ 100%

SEVERITY
Critical

WEIGHT
9

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation

ANSSI

- vuln1_delegation_a2d2

### Description
This indicator checks if the KRBTGT account has resource-based constrained delegation (RBCD) defined.

### Likelihood of Compromise
In Active Directory it is possible to create a resource-based constrained delegation on the KRBTGT account.
An attacker may attempt to leverage this type of delegation to generate ticket granting service (TGS) requests to the KRBTGT account as any user. This particular type of attack is similar to a Golden Ticket attack.

### References
Resource-Based Constrained Delegation: Semperis AD 101
Constrained authentication delegation to a domain controller service | ANSSI

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Write access to RBCD on DC

Pass

A+ 100%

SEVERITY
High

WEIGHT
6

### Security Frameworks
MITRE ATT&CK

- Credential Access

### Description
This indicator looks for Write access on RBCD for Domain Controllers to users who are not in Domain Admins, Enterprise Admins and Built-in Admins groups.

### Likelihood of Compromise
This setting enables configuring RBCD on Domain Controllers. An attacker that is able to gain Write access to RBCD for a resource can cause that resource to impersonate any user (except where delegation is explicitly disallowed). Write on RBCD is always a high privilege, but when it is on a DC, the impact is substantial as an attacker can delegate to a controlled resource as a privileged user and abuse the DC services.

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## Write access to RBCD on krbtgt account

Pass

A+ 100%

SEVERITY
High

WEIGHT
7

### Security Frameworks
MITRE ATT&CK

- Credential Access

### Description
This indicator looks for Write access on RBCD for the krbtgt account to users who are not in Domain Admins, Enterprise Admins and Built-in Admins groups.

### Likelihood of Compromise
This setting enables configuring RBCD on the krbtgt account. An attacker that is able to gain Write access to RBCD for a resource can cause that resource to impersonate any user (except where delegation is explicitly disallowed). Write on RBCD is always a high privilege, but when it is on the krbtgt account, the impact is substantial because it allows the attacker to create TGS for krbtgt for any user, which can then be used as a TGT.

### Result
No evidence of exposure.

### Remediation Steps
None

SECURITY INDICATOR

## RC4 or DES encryption type are supported by Domain Controllers

IOE Found

C+ 88%

SEVERITY
High

WEIGHT
6

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation
- Credential Access

ANSSI

- vuln2_dc_crypto
- vuln3_dc_crypto

- vuln4_dc_crypto

### Description
This indicator checks if RC4 or DES encryption is supported by Domain Controllers

### Likelihood of Compromise
RC4 and DES are considered an insecure form of encryption, susceptible to various cryptographic attacks. Multiple vulnerabilities in the RC4 and DES algorithms allow MitM and deciphering attacks.

### References
CVE-2013-2566
CVE-2015-2808
DC/RODC supported encryption algorithms | ANSSI

### Result
Found 1 Domain Controllers that support RC4 or DES encryption

| DistinguishedName | SupportedEncryptionTypes | EventTimestamp | Ignored |
|---|---|---|---|
| CN=WIN-9R40GBIS0S3,OU=Domain Controllers,DC=myzo,DC=local | AES 128, AES 256, RC4_HMAC_MD5 | 10/3/2025 6:10:21 PM | False |

Showing 1 of 1

### Remediation Steps
It is best practice to disable support for RC4 and DES on domain controllers. Proceed with caution, as this can cause clients that request RC4 encrypted kerberos tickets by default to fail. Disable it by adding the group policy Network security: Configure encryption types allowed for Kerberos and select only AES-128, AES-256 encryption types, to a GPO that affects the Domain Controllers container. The group policy path is Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options.

SECURITY INDICATOR

## Users with the attribute userPassword set

Pass


SEVERITY
Medium

WEIGHT
5

### Security Frameworks
MITRE ATT&CK

- Privilege Escalation

MITRE D3FEND

- Detect - Domain Account Monitoring

### Description
This indicator checks for the attribute of userPassword existing on accounts.

### Likelihood of Compromise
The attribute is saving passwords in clear text and can be queried using LDAP by everyone, which can potentially expose passwords. This attribute is not supposed to be visible but can be queried using LDAP. These days Active Directory is using another attribute named unicodePwd (unless the heuristic fUserPwdSupport is set).A misconfigured application can change the user password using this old mechanism and change the userPassword attribute which, and as a consequence, set the user password in clear text.

### References
3.1.1.3.1.5.2 userPassword | Microsoft Learn

### Result
No evidence of exposure.

### Remediation Steps
None

CATEGORY

## HYBRID

N/A

| WEIGHT | EVALUATED | INDICATORS FOUND |
|---|---|---|
| 7 | 0 | 0 |

Hybrid indicators help you understand and mitigate the risks associated with a hybrid identity environment. Active Directory is a perimeter point for Entra and a popular attack vendor. Understanding where the Active Directory perimeter is connecting to Entra provides clarity for how to secure the Active Directory entry point.

SECURITY INDICATOR

### Resource Based Constrained Delegation applied to AZUREADSSOACC account

Not Relevant

N/A

SEVERITY
Medium

WEIGHT
5

#### Security Frameworks
MITRE ATT&CK

- Lateral Movement
- Credential Access

#### Description
This indicator looks for Resource Based Constrained Delegation configured on the Entra Seamless SSO account.

#### Likelihood of Compromise
When configuring Entra Seamless SSO, a computer account is created in Active Directory, AZUREADSSOACC. This computer account is used by Entra ID to decrypt Kerberos tickets that are used as part of the seamless SSO mechanism between Active Directory and Entra ID. If resource-based constrained delegation is configured on the AZUREADSSOACC computer account, an account with the delegation would be able to generate Ticket Granting Service (TGS) requests to Entra ID on behalf of the AZUREADSSOACC account, and impersonate any user in the Entra tenant that is synchronized from Active Directory.
An attacker can use this method to move laterally from Active Directory into Entra ID.

#### References
Microsoft Entra Connect: Seamless single sign-on - Microsoft Entra ID | Microsoft Learn
Microsoft Entra Connect: Seamless Single Sign-On - How it works - Microsoft Entra ID | Microsoft Learn

#### Result
This indicator is only relevant for environments with AAD Connect. No IDs for AAD Connect were detected in the environment.

#### Remediation Steps
None

SECURITY INDICATOR

### SSO computer account with password last set over 90 days ago

Not Relevant

N/A

SEVERITY
High

WEIGHT
6

#### Security Frameworks
MITRE ATT&CK

- Credential Access

ANSSI

- vuln2_password_change_server_no_change_90

#### Description
This indicator checks the Entra Seamless Single Sign-On computer account, AZUREADSSOACC, to determine if the password has been rotated in the last 90 days.

#### Likelihood of Compromise
When configuring Entra Seamless SSO, a computer account is created in Active Directory, AZUREADSSOACC. This computer account is used by Entra ID to decrypt Kerberos tickets that are used as part of the seamless SSO mechanism between Active Directory and Entra ID. Because this is not an actual computer that is a member of Active Directory, the password for it cannot automatically be rolled over every 30 days. If an attacker compromises this account, they can generate Ticket Granting Service (TGS) request to Entra ID and impersonate any user in the Entra tenant that is synchronized from Active Directory.
An attacker can use this to move laterally from Active Directory into Entra ID.

#### References
Microsoft Entra Connect SSO FAQ - Microsoft Entra ID | Microsoft Learn
Microsoft Entra Connect: Seamless single sign-on - Microsoft Entra ID | Microsoft Learn

Managed service accounts with passwords unchanged for more than 90 days | ANSSI

**Result**
This indicator is only relevant for environments with Entra Connect. No IDs for Entra Connect were detected in the environment.

**Remediation Steps**
None

**Notes**

## Appendix 1 - Domains list

- myzo.local

## Appendix 2 - Scoring method

How do we determine the tests' score

The risk scores included in this report reveal the security posture of the Active Directory environment that was assessed. Risk scores are represented by percentage and letter grade. It is recommended to aim for the highest score possible; a 100% (A+) risk score indicates that there were no Indicators of Exposure (IOEs) found for the security indicators that were assessed. The following explanation is intended to help you understand the scoring methodology and factors used to calculate the risk scores presented in this report.

Risk scores:
The Security Assessment report provides the following risk scores:

- Security Indicator risk score: Each individual security indicator evaluated is assigned a score according to its internal logic and the relative number of results found. The individual security indicator score is assigned a weight (value between 1-10) according to the risk of the IOE found and the likelihood of compromise. This weighted score, together with a general factor of the industry risk, affects the score assigned to the relevant category.
- Category risk score:The security indicators included in the tool cover a range of categories that represent different aspects of Active Directory security posture. The category risk score is based on the test results and severity of each individual security indicator that was evaluated within the relevant category.
- Overall risk score: The overall risk score is derived from a weighted average of all indicator results, which are aggregated according to their respective severity levels.

**NOTE:** When calculating the risk scores, only security indicators and categories included in the assessment are included (e.g., security indicators that passed and resulting in IOEs found). Security indicators that were not selected, cancelled, or failed to run are not taken into account. For an accurate assessment, it is recommended that you include all security indicators and all domains in the selected forest.

Scoring methods/factors:

Letter grading: Each score is assigned a suitable letter grade according to the following table:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| A+, A, A- | 98-100% | B+, B, B- | 90-97% | C+, C, C- | 75-89% | D+, D, D- | 44-74% | F | 0-43% |

**Risk factors:** To determine the risk level of a particular security indicator, the following factors are taken into consideration:

- Severity (Informational, Warning, Critical)
- Likelihood of compromise
- The DREAD Threat Probability Matrix

DREAD Threat Probability Matrix

| DREAD | | High(3) | Medium(2) | Low(1) |
|---|---|---|---|---|
| **D**amage potential | How bad would the attack be? | Significant damage: The attacker can subvert the security system and gain full trust authorization. | Moderate damage: The attacker can access/leak sensitive information. | Minimal damage: The attacker can only access/leak trivial information. |
| **R**eproducibility | How easy would it be to recreate the attack? | The attack can be consistently reproduced and does not require a specific timing window. | The attack can be reproduced, but only within a specific timing window and in a particular sequence. | The attack is very difficult to reproduce, even with knowledge of the security weakness/vulnerability. |
| **E**xploitability | How easy would it be to launch the attack? | A novice programmer could perform the attack with minimal effort. | Requires a skilled programmer to launch the attack and be able to repeat the steps. | Requires an extremely skilled programmer with in-depth knowledge to launch an attack. |
| **A**ffected users | How many users would be impacted? | A large percentage or all users are impacted; default configuration and key customers are impacted. | A moderate percentage of users are impacted; non-default configuration is impacted. | A very small percentage of users are impacted; anonymous users are affected |
| **D**iscoverability | How easy would it be for the attacker to discover this exposure? | Easily discovered. Published information explains the vulnerability and attack technique. The vulnerability is found in commonly used features and is very noticeable. | Would require some effort to discover and successfully exploit. The vulnerability is found in a seldomly-used part of the product and only a few users should discover it | Hard to discover. The issue is obscure, and it is unlikely that users would discover a way to cause damage. |

Notes

# Appendix 3 - ANSSI Scorecard

The following section displays the breakdown of indicators within the framework of the French National Agency for the Security of Information Systems (ANSSI).
For more information visit: https://www.cert.ssi.gouv.fr/uploads/ad_checklist.html

ANSSI LEVEL

**1**

Critical weaknesses and misconfigurations pose an immediate threat to all hosted resources. Corrective actions should be taken as soon as possible.

| EVALUATED | Indicators FOUND | PASSED | FAILED TO RUN | CANCELED | NOT SELECTED |
|---|---|---|---|---|---|
| 40/40 | 4 | 36 | 0 | 0 | 0 |

| ANSSI ID | INDICATOR NAME | |
|---|---|---|
| vuln1_password_change_priv | Built-in domain Administrator account with old password (180 days) | Full Results |
| vuln1_permissions_adminsdholder<br>vuln1_privileged_members_perm | Permission changes on AdminSDHolder object | Full Results |
| vuln1_delegation_a2d2 | Accounts with altSecurityIdentities configured | Full Results |
| vuln1_dsheuristics_bad | Anonymous NSPI access to AD enabled | Full Results |
| vuln1_adcs_control | Dangerous control paths expose certificate containers | Full Results |
| vuln1_adcs_template_auth_enroll_with_name | Certificate templates with 3 or more insecure configurations | Full Results |
| vuln1_adcs_template_control | Dangerous control paths expose certificate templates | Full Results |
| vuln1_adcs_template_auth_enroll_with_name | Certificate templates that allow requesters to specify a subjectAltName | Full Results |
| vuln1_password_change_dc_no_change | Domain Controllers with old passwords | Full Results |
| vuln1_delegation_a2d2 | Accounts with Constrained Delegation configured to krbtgt | Full Results |
| vuln1_trusts_domain_notfiltered | Dangerous Trust Attribute Set | Full Results |
| vuln1_delegation_a2d2 | Accounts with Constrained Delegation configured to ghost SPN | Full Results |
| vuln1_dnszone_bad_prop | Unsecured DNS configuration | Full Results |
| vuln1_dc_inconsistent_uac | Domain Controllers in inconsistent state | Full Results |
| vuln1_permissions_dc | Domain Controller owner is not an administrator | Full Results |
| vuln1_functional_level | Domains with obsolete functional levels | Full Results |
| vuln1_permissions_dpapi | Non-default access to DPAPI key | Full Results |
| vuln1_dsheuristics_bad | Operator groups no longer protected by AdminSDHolder and SDProp | Full Results |
| vuln1_user_accounts_dormant | Enabled admin accounts that are inactive | Full Results |
| vuln1_permissions_gmsa_keys | Non-privileged users with access to gMSA passwords | Full Results |
| vuln1_password_change_inactive_dc | Domain Controllers that have not authenticated to the domain for more than 45 days | Full Results |
| vuln1_privileged_members | Forest contains more than 50 privileged accounts | Full Results |

| ANSSI ID | INDICATOR NAME | |
|---|---|---|
| vuln1_primary_group_id_1000 | Users and computers with non-default Primary Group IDs | Full Results |
| vuln1_permissions_schema | Non-standard schema permissions | Full Results |
| vuln1_delegation_t2a4d | Principals with constrained delegation using protocol transition enabled for a DC service | Full Results |
| vuln1_password_change_priv | Admins with old passwords | Full Results |
| vuln1_trusts_forest_sidhistory | Outbound forest trust with SID History enabled | Full Results |
| vuln1_trusts_domain_notfiltered | Domain trust to a third-party domain without quarantine | Full Results |
| vuln1_spn_priv | Privileged users with SPN defined | Full Results |
| vuln1_delegation_sourcedeleg | Domain Controllers with Resource-Based Constrained Delegation (RBCD) enabled | Full Results |
| vuln1_delegation_a2d2 | krbtgt account with Resource-Based Constrained Delegation (RBCD) enabled | Full Results |
| vuln1_permissions_naming_context | Non-default principals with DC Sync rights on the domain | Full Results |
| vuln1_permissions_msdns<br>vuln1_dnsadmins | Unprivileged principals as DNS Admins | Full Results |
| vuln1_permissions_adminsdholder | Privileged objects with unprivileged owners | Full Results |
| vuln1_dont_expire_priv | Privileged accounts with a password that never expires | Full Results |
| vuln1_kerberos_properties_preauth_priv | Users with Kerberos pre-authentication disabled | Full Results |
| vuln1_certificates_vuln | Weak certificate cipher | Full Results |
| vuln1_permissions_gpo_priv | GPO linking delegation at the AD Site level | Full Results |
| vuln1_permissions_gpo_priv | GPO linking delegation at the domain controller OU level | Full Results |
| vuln1_permissions_gpo_priv | GPO linking delegation at the domain level | Full Results |

ANSSI LEVEL

**2**

Configuration and management weaknesses put all hosted resources at risk of a short-term compromise. Corrective actions should be carefully planned and implemented shortly.

| EVALUATED | Indicators FOUND | PASSED | FAILED TO RUN | CANCELED | NOT SELECTED |
|---|---|---|---|---|---|
| **26/27** | **5** | **21** | **0** | **0** | **0** |

| ANSSI ID | INDICATOR NAME | |
|---|---|---|
| vuln2_password_change_server_no_change_90 | SSO computer account with password last set over 90 days ago | Full Results |
| vuln2_permissions_adminsdholder<br>vuln2_privileged_members_perm | Permission changes on AdminSDHolder object | Full Results |
| vuln2_compatible_2000_anonymous | Anonymous access to Active Directory enabled | Full Results |
| vuln2_dsheuristics_bad | Anonymous NSPI access to AD enabled | Full Results |

| ANSSI ID | INDICATOR NAME | |
|---|---|---|
| vuln2_password_change_server_no_change_90 | Computers with password last set over 90 days ago | Full Results |
| vuln2_delegation_t4d | Computer or user accounts with SPN that have unconstrained delegation | Full Results |
| vuln2_permissions_dc | Domain Controller owner is not an administrator | Full Results |
| vuln2_permissions_dpapi | Non-default access to DPAPI key | Full Results |
| vuln2_dsheuristics_bad | Operator groups no longer protected by AdminSDHolder and SDProp | Full Results |
| vuln2_adupdate_bad | Enterprise Key Admins with full access to domain | Full Results |
| vuln2_permissions_gmsa_keys | Non-privileged users with access to gMSA passwords | Full Results |
| vuln2_guest | Built-in guest account is enabled | Full Results |
| vuln2_krbtgt | Kerberos KRBTGT account with old password | Full Results |
| vuln2_privileged_members | Forest contains more than 50 privileged accounts | Full Results |
| vuln2_permissions_schema | Non-standard schema permissions | Full Results |
| vuln2_sysvol_ntfrs | NTFRS SYSVOL Replication | Full Results |
| vuln2_privileged_members_password | Privileged Users with Weak Password Policy | Full Results |
| vuln2_dc_crypto | RC4 or DES encryption type are supported by Domain Controllers | Full Results |
| vuln2_sidhistory_dangerous | Recent SIDHistory changes on objects | Full Results |
| vuln2_permissions_naming_context | Non-default principals with DC Sync rights on the domain | Full Results |
| vuln2_rodc_priv_revealed | Risky RODC credential caching | Full Results |
| vuln2_sidhistory_dangerous | Well-known privileged SIDs in SIDHistory | Full Results |
| vuln2_trusts_accounts | Trust accounts with old passwords | Full Results |
| vuln2_permissions_adminsdholder | Privileged objects with unprivileged owners | Full Results |
| vuln2_kerberos_properties_deskey | User accounts that use DES encryption | Full Results |
| vuln2_dont_expire | Users with Password Never Expires flag set | Full Results |
| vuln2_kerberos_properties_preauth | Users with Kerberos pre-authentication disabled | Full Results |

ANSSI LEVEL

**3**

The Active Directory infrastructure does not appear to have been weakened from what default installation settings provide.

| EVALUATED | Indicators FOUND | PASSED | FAILED TO RUN | CANCELED | NOT SELECTED |
|---|---|---|---|---|---|
| 11/11 | 2 | 9 | 0 | 0 | 0 |

| ANSSI ID | INDICATOR NAME | |
|---|---|---|
| vuln3_dsheuristics_bad | Anonymous NSPI access to AD enabled | Full Results |

| ANSSI ID | INDICATOR NAME | |
|---|---|---|
| vuln3_trusts_tgt_deleg | Dangerous Trust Attribute Set | Full Results |
| vuln3_dnszone_bad_prop | Unsecured DNS configuration | Full Results |
| vuln3_functional_level | Domains with obsolete functional levels | Full Results |
| vuln3_dsheuristics_bad | Operator groups no longer protected by AdminSDHolder and SDProp | Full Results |
| vuln3_primary_group_id_nochange | Users and computers with non-default Primary Group IDs | Full Results |
| vuln3_kerberos_properties_encryption | Primary users with SPN not supporting AES encryption on Kerberos | Full Results |
| vuln3_protected_users | Protected Users group not in use | Full Results |
| vuln3_dc_crypto | RC4 or DES encryption type are supported by Domain Controllers | Full Results |
| vuln3_sidhistory_present | Well-known privileged SIDs in SIDHistory | Full Results |
| vuln3_reversible_password | User accounts that store passwords with reversible encryption | Full Results |

ANSSI LEVEL

## 4

The Active Directory infrastructure exhibits an enhanced level of security and management.

| EVALUATED | Indicators FOUND | PASSED | FAILED TO RUN | CANCELED | NOT SELECTED |
|---|---|---|---|---|---|
| 4/4 | 2 | 2 | 0 | 0 | 0 |

| ANSSI ID | INDICATOR NAME | |
|---|---|---|
| vuln4_functional_level | Domains with obsolete functional levels | Full Results |
| vuln4_smartcard_expire_passwords | Smart card password rotation disabled | Full Results |
| vuln4_dc_crypto | RC4 or DES encryption type are supported by Domain Controllers | Full Results |
| vuln4_user_accounts_machineaccountquota | Unprivileged users can add computer accounts to the domain | Full Results |

# Appendix 4

## Privileged objects with unprivileged owners result

Showing 16 of 16

| Owner | DistinguishedName | Ignored |
|---|---|---|
| Could not read owner | CN=Administrator,CN=Users,DC=myzo,DC=local | False |
| Could not read owner | CN=Administrators,CN=Builtin,DC=myzo,DC=local | False |
| Could not read owner | CN=Print Operators,CN=Builtin,DC=myzo,DC=local | False |
| Could not read owner | CN=Backup Operators,CN=Builtin,DC=myzo,DC=local | False |
| Could not read owner | CN=Replicator,CN=Builtin,DC=myzo,DC=local | False |
| Could not read owner | CN=krbtgt,CN=Users,DC=myzo,DC=local | False |
| Could not read owner | CN=Domain Controllers,CN=Users,DC=myzo,DC=local | False |
| Could not read owner | CN=Schema Admins,CN=Users,DC=myzo,DC=local | False |
| Could not read owner | CN=Enterprise Admins,CN=Users,DC=myzo,DC=local | False |
| Could not read owner | CN=Domain Admins,CN=Users,DC=myzo,DC=local | False |
| Could not read owner | CN=Server Operators,CN=Builtin,DC=myzo,DC=local | False |
| Could not read owner | CN=Account Operators,CN=Builtin,DC=myzo,DC=local | False |
| Could not read owner | CN=Read-only Domain Controllers,CN=Users,DC=myzo,DC=local | False |
| Could not read owner | CN=Key Admins,CN=Users,DC=myzo,DC=local | False |
| Could not read owner | CN=Enterprise Key Admins,CN=Users,DC=myzo,DC=local | False |
| Could not read owner | CN=Lacie Monica,CN=Users,DC=myzo,DC=local | False |

Saved to SI000025 tab in C:\Users\lacie.monica\Desktop\PK Community 5.0\Output\2025_10_04_08_42_44\Security_Assessment_Report_10_4_2025_8_42_44_AM.xlsx

## Appendix 5

### AD objects created within the last 10 days result

Showing 30 of 359

| DistinguishedName | ObjectName | ObjectClass | EventTimestamp |
|---|---|---|---|
| DC=myzo,DC=local | myzo | domainDNS | 10/4/2025 3:00:41 AM |
| CN=Users,DC=myzo,DC=local | Users | container | 10/4/2025 3:00:49 AM |
| CN=Computers,DC=myzo,DC=local | Computers | container | 10/4/2025 3:00:49 AM |
| OU=Domain Controllers,DC=myzo,DC=local | Domain Controllers | organizationalUnit | 10/4/2025 3:00:49 AM |
| CN=System,DC=myzo,DC=local | System | container | 10/4/2025 3:00:49 AM |
| CN=LostAndFound,DC=myzo,DC=local | LostAndFound | lostAndFound | 10/4/2025 3:00:49 AM |
| CN=Infrastructure,DC=myzo,DC=local | Infrastructure | infrastructureUpdate | 10/4/2025 3:00:49 AM |
| CN=ForeignSecurityPrincipals,DC=myzo,DC=local | ForeignSecurityPrincipals | container | 10/4/2025 3:00:49 AM |
| CN=Program Data,DC=myzo,DC=local | Program Data | container | 10/4/2025 3:00:49 AM |
| CN=Microsoft,CN=Program Data,DC=myzo,DC=local | Microsoft | container | 10/4/2025 3:00:49 AM |
| CN=NTDS Quotas,DC=myzo,DC=local | NTDS Quotas | msDS-QuotaContainer | 10/4/2025 3:00:49 AM |
| CN=Managed Service Accounts,DC=myzo,DC=local | Managed Service Accounts | container | 10/4/2025 3:00:49 AM |
| CN=Keys,DC=myzo,DC=local | Keys | container | 10/4/2025 3:00:49 AM |
| CN=WinsockServices,CN=System,DC=myzo,DC=local | WinsockServices | container | 10/4/2025 3:00:49 AM |
| CN=RpcServices,CN=System,DC=myzo,DC=local | RpcServices | rpcContainer | 10/4/2025 3:00:49 AM |
| CN=FileLinks,CN=System,DC=myzo,DC=local | FileLinks | fileLinkTracking | 10/4/2025 3:00:49 AM |
| CN=VolumeTable,CN=FileLinks,CN=System,DC=myzo,DC=local | VolumeTable | linkTrackVolumeTable | 10/4/2025 3:00:49 AM |
| CN=ObjectMoveTable,CN=FileLinks,CN=System,DC=myzo,DC=local | ObjectMoveTable | linkTrackObjectMoveTable | 10/4/2025 3:00:49 AM |
| CN=Default Domain Policy,CN=System,DC=myzo,DC=local | Default Domain Policy | domainPolicy | 10/4/2025 3:00:49 AM |
| CN=AppCategories,CN=Default Domain Policy,CN=System,DC=myzo,DC=local | AppCategories | classStore | 10/4/2025 3:00:49 AM |
| CN=Meetings,CN=System,DC=myzo,DC=local | Meetings | container | 10/4/2025 3:00:49 AM |
| CN=Policies,CN=System,DC=myzo,DC=local | Policies | container | 10/4/2025 3:00:49 AM |
| CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=myzo,DC=local | {31B2F340-016D-11D2-945F-00C04FB984F9} | groupPolicyContainer | 10/4/2025 3:00:49 AM |
| CN=User,CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=myzo,DC=local | User | container | 10/4/2025 3:00:49 AM |
| CN=Machine,CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=myzo,DC=local | Machine | container | 10/4/2025 3:00:49 AM |
| CN={6AC1786C-016F-11D2-945F-00C04fB984F9},CN=Policies,CN=System,DC=myzo,DC=local | {6AC1786C-016F-11D2-945F-00C04fB984F9} | groupPolicyContainer | 10/4/2025 3:00:49 AM |
| CN=User,CN={6AC1786C-016F-11D2-945F-00C04fB984F9},CN=Policies,CN=System,DC=myzo,DC=local | User | container | 10/4/2025 3:00:49 AM |
| CN=Machine,CN={6AC1786C-016F-11D2-945F-00C04fB984F9},CN=Policies,CN=System,DC=myzo,DC=local | Machine | container | 10/4/2025 3:00:49 AM |
| CN=RAS and IAS Servers Access Check,CN=System,DC=myzo,DC=local | RAS and IAS Servers Access Check | container | 10/4/2025 3:00:49 AM |
| CN=File Replication Service,CN=System,DC=myzo,DC=local | File Replication Service | nTFRSSettings | 10/4/2025 3:00:49 AM |

Saved to SI000044 tab in C:\Users\lacie.monica\Desktop\PK Community 5.0\Output\2025_10_04_08_42_44\Security_Assessment_Report_10_4_2025_8_42_44_AM.xlsx