purple knight

SECURITY ASSESSMENT REPORT

v 4.2.2312.5001 | 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.

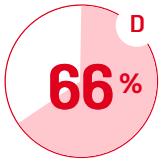
SECURITY POSTURE OVERVIEW

This report summarizes the security assessment results performed in your hybrid identity environment on 10/07/2024 by Semperis' Active Directory security assessment tool, Purple Knight. Depending on the environments selected for evaluation, the report includes the assessment results for an Active Directory forest, an Azure AD tenant, 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).
- Azure AD tenant: Purple Knight queried the selected Azure AD tenant focusing on some of the most common attack vectors that threat actors use to gain access to the Azure AD environment.
- 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	**ekoloclast.fr**
No. of Domains	**1**
Duration	**00:00:11.8600006**
Run by	**EKOLOCLAST\administrator**

Indicators

Evaluated	**106**
Not selected	**1**
IOEs found	**15**
Passed	**91**
Failed to run	**0**
Not Relevant	**2**
Canceled	**0**

CRITICAL IOEs FOUND

Inheritance enabled on AdminSDHolder object

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

Read More...

Permission changes on AdminSDHolder object

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

Read More...

Print spooler service is enabled on a DC

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

Read More...

Privileged Users with Weak Password Policy

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

Read More...

ADDITIONAL IOEs FOUND

NAME	PLATFORM	SEVERITY LEVEL	ACTION
• Built-in domain Administrator account used within the last two weeks	AD	Warning	Read More...
• Changes to Pre-Windows 2000 Compatible Access Group membership	AD	Warning	Read More...
• LDAP signing is not required on Domain Controllers	AD	Warning	Read More...
• Privileged accounts with a password that never expires	AD	Warning	Read More...
• RC4 or DES encryption type are supported by Domain Controllers	AD	Warning	Read More...
• AD objects created within the last 10 days	AD	Informational	Read More...
• Changes to MS LAPS read permissions	AD	Informational	Read More...
• gMSA not in use	AD	Informational	Read More...
• Protected Users group not in use	AD	Informational	Read More...
• Unprivileged users can add computer accounts to the domain	AD	Informational	Read More...
• Users with Password Never Expires flag set	AD	Informational	Read More...

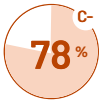
INDICATORS FAILED TO RUN

None

Notes

ACTIVE DIRECTORY RESULTS

Categories



AD DELEGATION

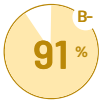
AD delegation is a critical part of security and compliance. By delegating control over Active

Read More ...

ACCOUNT SECURITY

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

Read More ...



AD INFRASTRUCTURE SECURITY

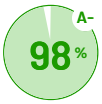
AD Infrastructure Security indicators pertain to the security configuration of core parts of AD's

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 ...

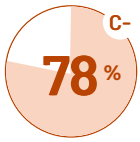
HYBRID

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

Read More ...

CATEGORY

AD DELEGATION



WEIGHT	EVALUATED	INDICATORS FOUND
3	18	5

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

IOE Found

SEVERITY	WEIGHT
Critical	10

Security Frameworks

MITRE ATT&CK

- Defense Evasion
- Privilege Escalation

Description

This indicator checks for inheritance being enabled on the Access Control List (ACL) of the AdminSDHolder object, which could indicate an attempt to modify permissions on privileged objects that are subject to AdminSDHolder (e.g. users or groups with adminCount=1).

Likelihood of Compromise

Changes to the AdminSDHolder object are very rare. 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.

Result

Found 1 domains containing an AdminSDHolder container with inheritance enabled.

DistinguishedName	Attribute	LastChange	Ignored
CN=AdminSDHolder,CN=System,DC=ekoloclast,DC=fr	nTSecurityDescriptor	10/07/2024 08:31:42	False

Showing 1 of 1

Remediation Steps

Check the permissions on the AdminSDHolder container and search for abnormal ACE \ owner.

SECURITY INDICATOR

Permission changes on AdminSDHolder object

IOE Found

SEVERITY	WEIGHT
Critical	10

Security Frameworks

MITRE ATT&CK

- Defense Evasion
- Privilege Escalation

ANSSI

- vuln1_permissions_adminsdholder
- vuln1_privileged_members_perm

Description

This indicator looks for Access Control List (ACL) changes on the AdminSDHolder object, which could indicate an attempt to modify permissions on privileged objects that are subject to AdminSDHolder (e.g. users or groups with adminCount=1).

Likelihood of Compromise

Changes to the AdminSDHolder object are very rare. 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.

Result

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

DistinguishedName	Attribute	EventTimestamp	Ignored

DistinguishedName	Attribute	EventTimestamp	Ignored
CN=AdminSDHolder,CN=System,DC=ekoloclast,DC=fr	nTSecurityDescriptor	10/07/2024 08:31:42	False

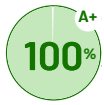
Showing 1 of 1

Remediation Steps
Check the permissions on the AdminSDHolder container and search for abnormal ACE \ owner.

SECURITY INDICATOR

Changes to AD Display Specifiers in the past 90 days

Pass



SEVERITY
Informational

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. (see this writeup for additional information).

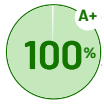
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Changes to default security descriptor schema in the last 90 days

Pass



SEVERITY
Warning

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.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Domain Controller owner is not an administrator

Pass

A+ 100%

SEVERITY
Warning

WEIGHT
6

Security Frameworks
MITRE ATT&CK

- Credential Access
- Privilege Escalation

MITRE D3FEND

- Harden - System Configuration Permissions

ANSSI

- vuln1_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.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Non-default access to DPAPI key

Pass

A+ 100%

SEVERITY
Warning

WEIGHT
7

Security Frameworks
MITRE ATT&CK

- Credential Access

MITRE D3FEND

- Harden - User Account Permissions

ANSSI

- vuln1_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.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Enterprise Key Admins with full access to domain

Pass

A+ 100%

SEVERITY
Warning

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).

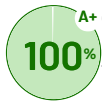
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Foreign Security Principals in Privileged Group

Pass



SEVERITY
Warning

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.

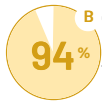
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

gMSA not in use

IOE Found



SEVERITY
Informational

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. For more information on

gMSA see the Microsoft article: here.

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.

Result
Found 1 domains with no gMSA objects enabled.

DomainName	Ignored
ekoloclast.fr	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

SEVERITY
Warning

WEIGHT
6

Security Frameworks
MITRE ATT&CK

- Credential Access

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.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Built-in guest account is enabled

Pass

SEVERITY
Informational

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.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Users with permissions to set Server Trust Account

Pass

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 originally reported by Stealthbits researchers, an attacker that is able to seed authenticated user(s) with these permissions can then utilize their access to these users to "promote" any computer they control to Domain Controller status, enabling privilege escalation to AD services and carrying out credential access attacks such as DCSync. More information available here.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Non default value on ms-Mcs-AdmPwd SearchFlags

Pass

SEVERITY
Warning

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.

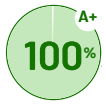
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Objects in privileged groups without adminCount=1 (SDProp)

Pass



SEVERITY
Informational

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. For more information see: https://docs.microsoft.com/en-us/previous-versions/technet-magazine/ee361593(v=msdn.10)

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.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Changes to MS LAPS read permissions

IOE Found

B- 92%

SEVERITY
Informational

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 (https://www.microsoft.com/en-us/download/details.aspx?id=46899). 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.

Result
Found 2 computers on which some normal users can read their LAPS password.

DistinguishedName	Access	Ignored
CN=P0232,CN=Computers,DC=ekoloclast,DC=fr	BUILTIN\Account Operators GenericAll on: All Properties	False
CN=P0600,OU=Communication,OU=LabOrdinateurs,DC=ekoloclast,DC=fr	BUILTIN\Account Operators GenericAll on: All Properties; EKOLOCLAST\GrpSecuriteMdp ReadProperty, ExtendedRight on: ms-mcs-admpwd; EKOLOCLAST\GrpRdsAccess ReadProperty, ExtendedRight on: ms-mcs-admpwd	False

Showing 2 of 2

Remediation Steps
Ensure that there are no unnecessary principals who can read computer administrator account passwords via Extended Rights on the ms-Mcs-AdmPwd attribute.

SECURITY INDICATOR

Non-default principals with DC Sync rights on the domain

Pass

A+ 100%

SEVERITY
Critical

WEIGHT
8

Security Frameworks

MITRE ATT&CK

- Credential Access

ANSSI

- vuln1_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.

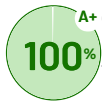
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Privileged objects with unprivileged owners

Pass



SEVERITY
Warning

WEIGHT
6

Security Frameworks
MITRE ATT&CK

- Privilege Escalation

ANSSI

- vuln1_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.

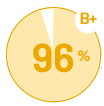
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Unprivileged users can add computer accounts to the domain

IOE Found



SEVERITY
Informational

WEIGHT
3

Security Frameworks
MITRE ATT&CK

- Credential Access
- Lateral Movement

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.

Result

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

DistinguishedName	MachineAccountQuota	Ignored
DC=ekoloclast,DC=fr	10	False

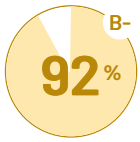
Showing 1 of 1

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



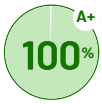
WEIGHT	EVALUATED	INDICATORS FOUND
6	30	7

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

SECURITY INDICATOR

Abnormal Password Refresh

Pass



SEVERITY	WEIGHT
Warning	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.

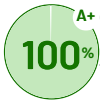
Remediation Steps

None

SECURITY INDICATOR

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

Pass



SEVERITY	WEIGHT
Informational	4

Security Frameworks

MITRE ATT&CK

- Credential Access

MITRE D3FEND

- Harden - Strong Password Policy

ANSSI

- vuln1_password_change_priv

Description

This indicator checks to see if the pwdLastSet attribute on the built-in Domain Administrator account has been changed within the last 180 days.

Likelihood of Compromise

If the password for the built-in Domain Administrator account is not being changed on a regular basis, this account can be vulnerable to brute force password attacks.

Result

No evidence of exposure.

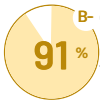
Remediation Steps

None

SECURITY INDICATOR

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

IOE Found



SEVERITY
Warning

WEIGHT
5

Security Frameworks
MITRE ATT&CK

- Credential Access

MITRE D3FEND

- Detect - Credential Compromise Scope Analysis
- Harden - Strong Password Policy

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

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

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

DistinguishedName	EventTimestamp	Ignored
CN=Administrator,CN=Users,DC=ekoloclast,DC=fr	02/07/2024 17:57:56	False

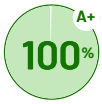
Showing 1 of 1

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



SEVERITY
Warning

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.

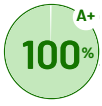
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Privileged users that are disabled

Pass



SEVERITY
Informational

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.

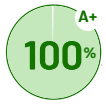
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Enabled admin accounts that are inactive

Pass



SEVERITY
Warning

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.

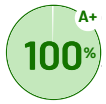
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Ephemeral Admins

Pass



SEVERITY
Informational

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.

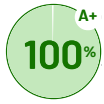
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

FGPP not applied to Group

Pass



SEVERITY	WEIGHT
Warning	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.

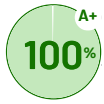
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Forest contains more than 50 privileged accounts

Pass



SEVERITY	WEIGHT
Warning	5

Security Frameworks
MITRE ATT&CK

- Privilege Escalation
- Reconnaissance

ANSSI

- vuln1_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.

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.

Result
Found 17 objects that were created in the last 10 days.

DistinguishedName	ObjectClass	Name	EventTimestamp
CN=pbx,CN=Users,DC=ekoloclast,DC=fr	user	pbx	01/07/2024 23:19:40
CN={1CF1C83F-AC59-496F-AD9F-D2F06B7718DE},CN=Policies,CN=System,DC=ekoloclast,DC=fr	groupPolicyContainer	{1CF1C83F-AC59-496F-AD9F-D2F06B7718DE}	02/07/2024 00:17:56
CN=Machine,CN={1CF1C83F-AC59-496F-AD9F-D2F06B7718DE},CN=Policies,CN=System,DC=ekoloclast,DC=fr	container	Machine	02/07/2024 00:17:56
CN=User,CN={1CF1C83F-AC59-496F-AD9F-D2F06B7718DE},CN=Policies,CN=System,DC=ekoloclast,DC=fr	container	User	02/07/2024 00:17:56
CN=Class Store,CN=Machine,CN={1CF1C83F-AC59-496F-AD9F-D2F06B7718DE},CN=Policies,CN=System,DC=ekoloclast,DC=fr	classStore	Class Store	02/07/2024 00:19:26
CN=Packages,CN=Class Store,CN=Machine,CN={1CF1C83F-AC59-496F-AD9F-D2F06B7718DE},CN=Policies,CN=System,DC=ekoloclast,DC=fr	classStore	Packages	02/07/2024 00:19:26
CN=52f08a7b-9242-413b-be62-9d96b7b9f556,CN=Packages,CN=Class Store,CN=Machine,CN={1CF1C83F-AC59-496F-AD9F-D2F06B7718DE},CN=Policies,CN=System,DC=ekoloclast,DC=fr	packageRegistration	52f08a7b-9242-413b-be62-9d96b7b9f556	02/07/2024 00:19:26
CN={9E29C765-DCE1-42CB-BAAC-C3C49DE4D86F},CN=Policies,CN=System,DC=ekoloclast,DC=fr	groupPolicyContainer	{9E29C765-DCE1-42CB-BAAC-C3C49DE4D86F}	03/07/2024 17:42:56
CN=Machine,CN={9E29C765-DCE1-42CB-BAAC-C3C49DE4D86F},CN=Policies,CN=System,DC=ekoloclast,DC=fr	container	Machine	03/07/2024 17:42:56
CN=User,CN={9E29C765-DCE1-42CB-BAAC-C3C49DE4D86F},CN=Policies,CN=System,DC=ekoloclast,DC=fr	container	User	03/07/2024 17:42:56

Showing 10 of 17
View additional results...

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

MITRE D3fend based on the reference: audit-user-account-management of Microsoft

SECURITY INDICATOR

Recent privileged account creation activity

Pass

A+ 100%

SEVERITY
Informational

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.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Unprivileged accounts with adminCount=1

Pass

SEVERITY
Informational

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

SEVERITY
Informational

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.

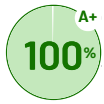
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Users and computers without readable PGID

Pass



SEVERITY
Warning

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).

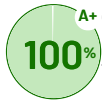
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Users with old passwords

Pass



SEVERITY
Informational

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.

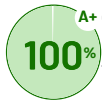
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Admins with old passwords

Pass



SEVERITY
Informational

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.

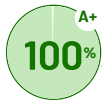
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Operators Groups that are not empty

Pass



SEVERITY
Warning

WEIGHT
6

Security Frameworks
MITRE ATT&CK

- Privilege Escalation
- Credential Access

MITRE D3FEND

- Harden - User Account Permissions

Description
Operator groups (Account Operators, Server Operators, Backup Operators, Print Operators) can take indirect control of the domain. These groups have write access to critical resources of the domain.

Likelihood of Compromise
Operators groups have write access to critical resources of the domain, attackers that are members of these groups change, modify and add different critical domain resources.

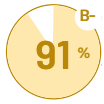
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Changes to Pre-Windows 2000 Compatible Access Group membership

IOE Found



SEVERITY
Warning

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. For more information see the following Semperis blog entry.

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.

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

Group distinguished name	Member	Operation	EventTimestamp	Ignored
CN=Pre-Windows 2000 Compatible Access,CN=Builtin,DC=ekoloclast,DC=fr	NT AUTHORITY\Authenticated Users	Risky Member Added During Domain Creation	15/05/2024 20:10:39	False

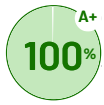
Showing 1 of 1

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

Pass



SEVERITY
Warning

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
No evidence of exposure.

Remediation Steps
None

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.

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

DistinguishedName	PasswordPolicyDN	Max Age	Min Age	Min Length	Complexity Enabled	History	Ignored
CN=Administrator,CN=Users,DC=ekoloclast,DC=fr	DC=ekoloclast,DC=fr	42	1	7	True	24	False
CN=Localadmin,OU=LabSecurite,DC=ekoloclast,DC=fr	DC=ekoloclast,DC=fr	42	1	7	True	24	False

Showing 2 of 2

Remediation Steps
Apply appropriate password policies for privileged users.

MITRE D3fend based on the reference: NIST.SP.800-63-3

SECURITY INDICATOR

Protected Users group not in use

IOE Found

A- 98%

SEVERITY
Informational

WEIGHT
1

Security Frameworks
MITRE ATT&CK

- Credential Access

ANSSI

- vuln3_protected_users

Description
The Protected Users group was introduced in Server 2012-R2 Active Directory to minimize credential exposure for privileged accounts. Users in the Protected Users group are more secure when authenticating to Windows resources. The differences include no longer caching clear-text passwords, even when Windows Digest is enabled, NTLM will no longer cache clear-text passwords, and Kerberos will no longer create DES or RC4 keys. When logging into domain controllers, members of the Protected Users group cannot authenticate via NTLM (Kerberos only), use DES or RC4 for Kerberos pre-authentication, and cannot be delegated with constrained or unconstrained delegation.

Likelihood of Compromise
The Protected Users group provides privileged users with additional protection from direct credential theft attacks. Ideally, all privileged users are members of the Protected Users group. For more information, see https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group.

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

DistinguishedName	SamAccountName	Enabled	Ignored
CN=Administrator,CN=Users,DC=ekoloclast,DC=fr	Administrator	True	False
CN=Localadmin,OU=LabSecurite,DC=ekoloclast,DC=fr	Localadmin	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
Warning

WEIGHT
5

Security Frameworks
MITRE ATT&CK

- Privilege Escalation

ANSSI

- vuln2_sidhistory_dangerous

Description
This indicator detects any recent changes to sIDHistory on objects, including changes to non-privileged accounts where privileged SIDs are added.

Likelihood of Compromise
Attackers need privileged access to AD to be able to write to sIDHistory, but if such rights exist then writing privileged SIDs to regular user accounts is a stealthy way of creating backdoor accounts.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Trust accounts with old passwords

Pass

SEVERITY
Informational

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.

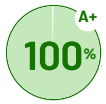
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Unprivileged principals as DNS Admins

Pass



SEVERITY
Warning

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. For more information on how DNS admins can abuse privileges see this blog post.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

User accounts that use DES encryption

Pass

SEVERITY
Informational

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.

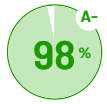
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Users with Password Never Expires flag set

IOE Found



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.

Result
Found 2 users with password never expires.

DistinguishedName	SamAccountName	PasswordLastSet	ServicePrincipalName	Ignored
CN=user test,OU=LabUtilisateurs,DC=ekoloclast,DC=fr	usertest	27/05/2024 07:45:17		False

DistinguishedName	SamAccountName	PasswordLastSet	ServicePrincipalName	Ignored
CN=pbx,CN=Users,DC=ekoloclast,DC=fr	pbx	01/07/2024 21:19:40		False

Showing 2 of 2

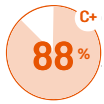
Remediation Steps
Move any user accounts away from Password Never Expires by having a good password rotation scheme and ensure any accounts that require this flag have the least privileges required. If this is a service account, considering using Group Managed Service Accounts (gMSA).

MITRE D3fend based on the reference: NIST.SP.800-63-3

SECURITY INDICATOR

Privileged accounts with a password that never expires

IOE Found



SEVERITY
Warning

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.

Result
Found 1 users with password never expires.

DistinguishedName	SamAccountName	PasswordLastSet	ServicePrincipalName	Ignored
CN=Localadmin,OU=LabSecurite,DC=ekoloclast,DC=fr	Localadmin	29/05/2024 15:42:42		False

Showing 1 of 1

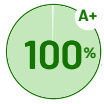
Remediation Steps
Enforce that users with privileged access must change their passwords on a regular basis and ensure that those passwords are complex and ideally require MFA to authenticate.

MITRE D3fend based on the reference: NIST.SP.800-63-3

SECURITY INDICATOR

User accounts with password not required

Pass



SEVERITY
Warning

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.

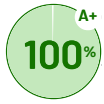
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

User accounts that store passwords with reversible encryption

Pass



SEVERITY
Informational

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.

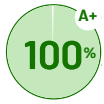
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Users with Kerberos pre-authentication disabled

Pass



SEVERITY
Warning

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'. please refer to this resource: https://social.technet.microsoft.com/wiki/contents/articles/23559.kerberos-pre-authentication-why-it-should-not-be-disabled.aspx.

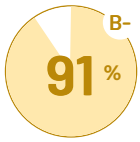
Likelihood of Compromise
If an account has Kerberos pre-authentication disabled, it makes it easier for attackers to send dummy requests to a DC to try and crack its Ticket Granting Ticket (TGT).

Result
No evidence of exposure.

Remediation Steps
None

CATEGORY

AD INFRASTRUCTURE SECURITY



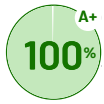
WEIGHT	EVALUATED	INDICATORS FOUND
7	30	2

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

SECURITY INDICATOR

Anonymous access to Active Directory enabled

Pass



SEVERITY	WEIGHT
Warning	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.

Result

No evidence of exposure.

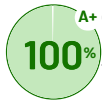
Remediation Steps

None

SECURITY INDICATOR

Anonymous NSPI access to AD enabled

Pass



SEVERITY	WEIGHT
Warning	6

Security Frameworks

MITRE ATT&CK

- Initial Access

MITRE D3FEND

- Harden - User Account Permissions

ANSSI

- vuln1_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.

Result

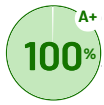
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Dangerous control paths expose certificate containers

Pass



SEVERITY
Warning

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.

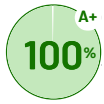
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Certificate templates with 3 or more insecure configurations

Pass



SEVERITY
Warning

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.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Dangerous control paths expose certificate templates

Pass

SEVERITY
Warning

WEIGHT
7

Security Frameworks
MITRE ATT&CK

- Credential Access

ANSSI

- vuln1_adcs_template_control

MITRE D3FEND

- Detect - Certificate Analysis

Description
This indicators 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.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Certificate templates that allow requesters to specify a subjectAltName

Pass

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.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Computers with older OS versions

Pass

A+ 100%

SEVERITY
Informational

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
Warning

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
Informational

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.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Dangerous Trust Attribute Set

Pass

SEVERITY
Warning

WEIGHT
7

Security Frameworks
MITRE ATT&CK

- Privilege Escalation

MITRE D3FEND

- Harden - Domain Trust Policy

ANSSI

- vuln1_trusts_domain_notfiltered

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.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Print spooler service is enabled on a DC

IOE Found

SEVERITY
Critical

WEIGHT
8

Security Frameworks
MITRE ATT&CK

- Execution
- Lateral Movement
- Privilege Escalation

MITRE D3FEND

- Harden - Software Update

Description
This indicator scans Domain Controllers for a running print spooler service. The scan requires a **local** print spooler service to be

running on the workstation.

The indicator will return "Fail to Run" if the spooler service is disabled on the local machine. The local print spooler service is enabled by default, and the vulnerability is on Domain Controllers only.

Keep in mind that if you're running the scan on a workstation that does not normally have the spooler service active, you can turn it on for the scan and turn it off afterwards.

Likelihood of Compromise
During June-July 2021, several critical flaws were found in Windows Print Spooler services - CVE-2021-1675 and CVE-2021-34527 which directly affects Print Spoolers on domain controllers, enabling remote code execution. See this link for Microsoft updates and patch information on this flaw.
In addition to this vulnerability, an existing weakness in print spoolers enabled on a DC, combined with unconstrained delegation object (see indicator 16 "Computer or user accounts with unconstrained delegation") may allow attackers to authenticate as that DC to any service (see this writeup for additional information).

Result
Found 2 DCs that have the Print Spooler service running.

FQDN	Ignored
EKO-MSTR.ekoloclast.fr	False
EKO-RDS.ekoloclast.fr	False

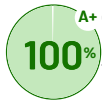
Showing 2 of 2

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



SEVERITY
Critical

WEIGHT
10

Security Frameworks
MITRE ATT&CK

- Defense Evasion

MITRE D3FEND

- Isolate - Execution Isolation
- Detect - Domain Account Monitoring

Description
DCShadow attacks enable 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. This indicator looks for evidence of a specific implementation of that attack by the popular Mimikatz tool.

Likelihood of Compromise
The Mimikatz tool is widely used by legitimate pen-testers as well as nefarious hackers. The criticality and impact of such an attack necessitate further investigation to ensure that no serious compromise has occurred.

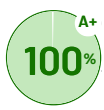
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Unsecured DNS configuration

Pass



SEVERITY
Warning

WEIGHT
7

Security Frameworks
MITRE ATT&CK

- Privilege Escalation

ANSSI

- vuln1_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

SEVERITY
Informational

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.

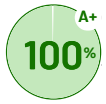
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Domains with obsolete functional levels

Pass



SEVERITY
Informational

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 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.

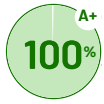
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Operator groups no longer protected by AdminSDHolder and SDProp

Pass



SEVERITY
Warning

WEIGHT
5

Security Frameworks
MITRE ATT&CK

- Defense Evasion

MITRE D3FEND

- Harden - User Account Permissions

ANSSI

- vuln1_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.

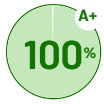
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

AD Certificate Authority with Web Enrollment - PetitPotam and ESC8

Pass



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. 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 may abuse a flaw in AD CS Web Enrollment that enables NTLM relay attacks to authenticate as a privileged user. An example of such attack was provided in July 2021 when chained with "PetitPotam" authentication coercion on MS-EFSRPC. The impact of such an attack can be privilege escalation to Domain Admin from network access only. More details about "ESC8" here.

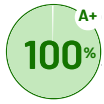
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

gMSA objects with old passwords

Pass



SEVERITY
Warning

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.

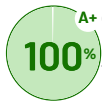
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

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

Pass



SEVERITY
Warning

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.

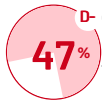
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

LDAP signing is not required on Domain Controllers

IOE Found



SEVERITY
Warning

WEIGHT
7

Security Frameworks
MITRE ATT&CK

- Privilege Escalation
- Credential Access

Description
This indicator looks 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.

Result
Found 3 DCs that do not require LDAP Signing.

DCName	DistinguishedName	State	Ignored
EKO-CORE.ekoloclast.fr	CN=EKO-CORE,OU=Domain Controllers,DC=ekoloclast,DC=fr	Ldap Signing Not Required	False
EKO-RDS.ekoloclast.fr	CN=EKO-RDS,OU=Domain Controllers,DC=ekoloclast,DC=fr	Ldap Signing Not Required	False
EKO-MSTR.ekoloclast.fr	CN=EKO-MSTR,OU=Domain Controllers,DC=ekoloclast,DC=fr	Ldap Signing Not Required	False

Showing 3 of 3

Remediation Steps
The following remediation steps use Group Policies. They should be followed by order and completed correctly to avoid disruptions in the domain:

1. Configure clients to request LDAP signing - Group Policy name:Network security:LDAP client signing requirements -> select Request signing in the dialog box.

2. When all clients request signing, configure domain controllers to require signing - Group Policy name:Domain controller:LDAP server signing requirements -> select Require signing.

3. Configure clients to require signing - Group Policy name:Network security:LDAP client signing requirements -> select Require signing in the dialog box.

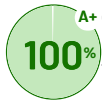
Following these steps will ensure that no client will stop working during the transition.

See more detailed info here, and here..

SECURITY INDICATOR

Non-standard schema permissions

Pass



SEVERITY
Warning

WEIGHT
7

Security Frameworks
MITRE ATT&CK

- Privilege Escalation

ANSSI

- vuln1_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. For additional information and remediation advice, see the ANSSI website.

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.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

NTFRS SYSVOL Replication

Pass

A+ 100%

SEVERITY
Warning

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.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Outbound forest trust with SID History enabled

Pass

A+ 100%

SEVERITY
Warning

WEIGHT
6

Security Frameworks
MITRE ATT&CK

- Lateral Movement

MITRE D3FEND

- Harden - Domain Trust Policy

ANSSI

- vuln1_trusts_forest_sidhistory

Description
This indicator looks for outbound forest trusts that has TRUST_ATTRIBUTE_TREAT_AS_EXTERNAL flag set to true. If this bit is set, then a cross-forest trust to a domain is to be treated as an external trust for the purposes of SID Filtering. Cross-forest trusts are more stringently filtered than external trusts. This attribute relaxes those cross-forest trusts to be equivalent to external trusts.

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.

Result
No evidence of exposure.

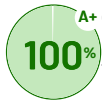
Remediation Steps

None

SECURITY INDICATOR

Domain trust to a third-party domain without quarantine

Pass



SEVERITY
Warning

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.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Risky RODC credential caching

Pass

SEVERITY
Warning

WEIGHT
5

Security Frameworks
MITRE ATT&CK

- Credential Access

MITRE D3FEND

- Harden - User Account Permissions

ANSSI

- vuln2_rodc_priv_revealed

Description
On a per-RODC basis, you can control which security principals are allowed to replicate their credentials to an RODC when they logon. If privileged users are in the allow list, that can expose their credentials to theft from these RODCs. This indicator looks for a Password Replication Policy that allows privileged objects.

Likelihood of Compromise
Generally, RODCs are at higher risk than standard DCs (e.g. deployed at remote sites with poor security). This makes them ripe targets for attackers and privileged credentials cached on these servers can elevate their access significantly.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Privileged user credentials cached on RODC

Pass

A+ 100%

SEVERITY
Informational

WEIGHT
4

Security Frameworks
MITRE ATT&CK

- Lateral Movement
- Privilege Escalation

Description
This indicator looks for privileged users with credentials that are cached to RODCs.

Likelihood of Compromise
While not immediately indicative of an attack, privileged user accounts are sensitive and should not be cached to RODCs since their physical security is not as robust as a full DCs would be.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Well-known privileged SIDs in sIDHistory

Pass

A+ 100%

SEVERITY
Warning

WEIGHT
7

Security Frameworks
MITRE ATT&CK

- Defense Evasion
- Privilege Escalation

ANSSI

- vuln2_sidhistory_dangerous
- vuln3_sidhistory_present

Description
This indicator looks for security principals that contain specific SIDs of accounts from built-in privileged groups within their sIDHistory attribute. This would allow those security principals to have the same privileges as those privileged accounts, but in a way that is not obvious to monitor (e.g. through group membership).

Likelihood of Compromise
Writing to sIDHistory requires special privileges. Therefore, anyone who can write to the sIDHistory attribute has likely compromised the domain already, but this method for gaining persistence can be very effective, given the difficulty administrators will have in detecting these kinds of privileged escalations.

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.

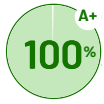
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

SMBv1 is enabled on Domain Controllers

Pass



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.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Weak certificate cipher

Pass

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.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Zerologon vulnerability

Not Selected

N/A

SEVERITY	WEIGHT
Critical	10

Security Frameworks

MITRE ATT&CK

- Privilege Escalation

Description

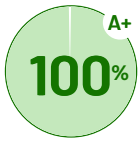
This indicator looks for security vulnerability to CVE-2020-1472, which was patched by Microsoft in August 2020. Without this patch, an unauthenticated attacker can exploit CVE-2020-1472 to elevate their privileges and get administrative access on the domain.

Likelihood of Compromise

While this exploit was patched by Microsoft, unpatched domain controllers still exist and there is exploit code in the wild that is actively taking advantage of this vulnerability.

CATEGORY

GROUP POLICY SECURITY



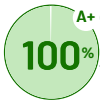
WEIGHT	EVALUATED	INDICATORS FOUND
5	10	0

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

Pass



SEVERITY	WEIGHT
Informational	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

No evidence of exposure.

Remediation Steps

None

SECURITY INDICATOR

Writable shortcuts found in GPO

Pass

SEVERITY	WEIGHT
Warning	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

SEVERITY
Warning

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

SEVERITY
Informational

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
Warning

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.

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.

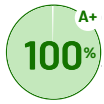
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

SYSVOL Executable Changes

Pass



SEVERITY
Informational

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.

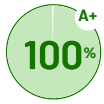
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

GPO linking delegation at the AD Site level

Pass



SEVERITY
Warning

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.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

GPO linking delegation at the domain controller OU level

Pass

SEVERITY
Warning

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.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

GPO linking delegation at the domain level

Pass

SEVERITY
Warning

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.

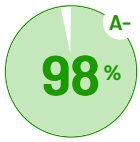
Likelihood of Compromise
Just being able to link GPOs doesn't provide the whole picture. An attacker would need to find or edit a GPO that contains the instructions they want to achieve. However, if an attacker can find an existing GPO that meets their needs, then having this write permission gives them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

Result
No evidence of exposure.

Remediation Steps
None

CATEGORY

KERBEROS SECURITY



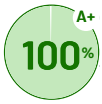
WEIGHT	EVALUATED	INDICATORS FOUND
8	18	1

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

SECURITY INDICATOR

Accounts with altSecurityIdentities configured

Pass



SEVERITY	WEIGHT
Warning	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.

Result

No evidence of exposure.

Remediation Steps

None

SECURITY INDICATOR

Computer or user accounts with SPN that have unconstrained delegation

Pass

SEVERITY	WEIGHT
Warning	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.

Result

No evidence of exposure.

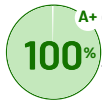
Remediation Steps

None

SECURITY INDICATOR

Accounts with Constrained Delegation configured to krbtgt

Pass



SEVERITY
Critical

WEIGHT
9

Security Frameworks
MITRE ATT&CK

- Privilege Escalation

MITRE D3FEND

- Detect - Domain Account Monitoring

ANSSI

- vuln1_delegation_a2d2

Description
It is possible to create a Kerberos delegation to the krbtgt account itself. Such a 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, which has the effect of generating a Ticket Granting Ticket (TGT) similar to a Golden Ticket. This indicator looks for accounts that have Constrained Delegation configured to the krbtgt service.

Likelihood of Compromise
This type of attack should be easy to spot as no delegations should normally be created to the krbtgt account. However, if they are found, they would represent a significant risk and should be mitigated quickly.

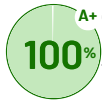
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Accounts with Constrained Delegation configured to ghost SPN

Pass



SEVERITY
Warning

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.

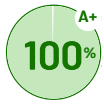
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Kerberos krbtgt account with old password

Pass



SEVERITY
Warning

WEIGHT
4

Security Frameworks
MITRE ATT&CK

- Credential Access

MITRE D3FEND

- Harden - Strong Password Policy

ANSSI

- vuln2_krbtgt

Description
The krbtgt user account is a special (disabled) user account in every Active Directory domain that has a special role in Kerberos function. If this account's password is compromised, Golden Ticket attacks can be performed to get access to any resource in the AD domain. This indicator looks for a krbtgt user account whose password hasn't been changed in the past 180 days. While Microsoft recommends changing the password every year, STIG recommends changing it every 180 days.

Likelihood of Compromise
The potential impact of a compromised krbtgt password is access to any and all connected services. These attacks typically require that an attacker gets access to the krbtgt hash through other compromise methods. This does not directly indicate compromise but should be remediated. A script for resetting the krbtgt password is available on Microsoft's GitHub here.
A more updated version is available on the script author's GitHub page here.

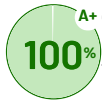
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Objects with constrained delegation configured

Pass



SEVERITY
Informational

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.

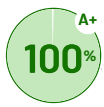
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Principals with constrained authentication delegation enabled for a DC service

Pass



SEVERITY
Warning

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.

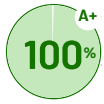
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Kerberos protocol transition delegation configured

Pass



SEVERITY
Warning

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

SEVERITY
Warning

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.

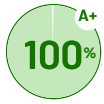
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Users with SPN defined

Pass



SEVERITY
Informational

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.

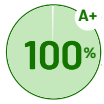
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Primary users with SPN not supporting AES encryption on Kerberos

Pass



SEVERITY
Warning

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)

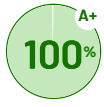
Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Privileged users with SPN defined

Pass



SEVERITY
Warning

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.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

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

Pass

SEVERITY
Informational

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

SEVERITY
Warning

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.

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
It is possible to create a Kerberos delegation on the krbtgt account itself. Such a 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, which has the effect of generating a Ticket Granting Ticket (TGT) similar to a Golden Ticket. This indicator looks for a krbtgt account that has Resource-Based Constrained Delegation (RBCD) defined.

Likelihood of Compromise
This type of attack should be easy to spot as no delegations should normally be created on the krbtgt account. However, if they are found, they would represent a significant risk and should be mitigated quickly.

Result
No evidence of exposure.

Remediation Steps
None

SECURITY INDICATOR

Write access to RBCD on DC

Pass

A+ 100%

SEVERITY
Warning

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.

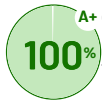
Remediation Steps

None

SECURITY INDICATOR

Write access to RBCD on krbtgt account

Pass



SEVERITY
Warning

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

SEVERITY
Warning

WEIGHT
6

Security Frameworks
MITRE ATT&CK

- Privilege Escalation
- Credential Access

ANSSI

- vuln2_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. See CVE-2013-2566 and CVE-2015-2808.

Result
Found 3 Domain Controllers that support RC4 or DES encryption

DistinguishedName	SupportedEncryptionTypes	EventTimestamp	Ignored
CN=EKO-CORE,OU=Domain Controllers,DC=ekoloclast,DC=fr	AES 128, AES 256, RC4_HMAC_MD5	25/06/2024 10:03:01	False
CN=EKO-RDS,OU=Domain Controllers,DC=ekoloclast,DC=fr	AES 128, AES 256, RC4_HMAC_MD5	25/06/2024 12:38:31	False
CN=EKO-MSTR,OU=Domain Controllers,DC=ekoloclast,DC=fr	AES 128, AES 256, RC4_HMAC_MD5	15/05/2024 18:13:21	False

Showing 3 of 3

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.

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 Azure AD and a popular attack vendor. Understanding where the Active Directory perimeter is connecting to Azure AD 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: Warning

WEIGHT: 5

Security Frameworks

MITRE ATT&CK

- Lateral Movement
- Credential Access

Description

This indicator looks for Resource Based Constrained Delegation configured for the Azure SSO account AZUREADSSOACC.

Likelihood of Compromise

It is possible to create a Kerberos Resource Based Constrained Delegation on the AZUREADSSOACC account itself. An account with such delegation would allow that principal to generate a Ticket Granting Service (TGS) request to the Azure tenant on behalf of the AZUREADSSOACC account as any user and impersonate that user.

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: Warning

WEIGHT: 6

Security Frameworks

MITRE ATT&CK

- Credential Access

ANSSI

- vuln2_password_change_server_no_change_90

Description

This indicator checks the SSO computer account (AZUREADSSOACC) to determine if the password has been rotated in the last 90 days.

Likelihood of Compromise

The computer account utilized for Azure SSO (AZUREADSSOACC) does not automatically change its password every 30 days. If the password for this account is compromised, an attacker could generate a Ticket Granting Service (TGS) request to the AZUREADSSOACC account as any user, which has the effect of generating a Ticket to azure and impersonate that user.

Result

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

Remediation Steps

None

Notes

Appendix 1 - Domains list

- ekoloclast.fr

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+	100	A	99	A-	98	B+	96-97	B	93-95
B-	90-92	C+	86-89	C	81-85	C-	75-80	D+	67-74
D	58-66	D-	44-57	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)
Damage 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.
Reproducibility	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.
Exploitability	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.
Affected 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
Discoverability	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
39/39	2	37	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 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_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
vuln1_primary_group_id_1000	Users and computers with non-default Primary Group IDs	Full Results

ANSSI ID	INDICATOR NAME	
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 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
16/17	3	13	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_compatible_2000_anonymous	Anonymous access to Active Directory enabled	Full Results
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_adupdate_bad	Enterprise Key Admins with full access to domain	Full Results
vuln2_guest	Built-in guest account is enabled	Full Results

ANSSI ID	INDICATOR NAME	
vuln2_krbtgt	Kerberos krbtgt account with old password	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_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_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
6/6	1	5	0	0	0

ANSSI ID	INDICATOR NAME	
vuln3_functional_level	Domains with obsolete functional levels	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_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
2/2	1	1	0	0	0

ANSSI ID	INDICATOR NAME	
vuln4_functional_level	Domains with obsolete functional levels	Full Results
vuln4_dc_crypto	RC4 or DES encryption type are supported by Domain Controllers	Full Results

Appendix 4

AD objects created within the last 10 days result

Showing 17 of 17

DistinguishedName	ObjectClass	Name	EventTimestamp
CN=pbx,CN=Users,DC=ekoloclast,DC=fr	user	pbx	01/07/2024 23:19:40
CN={1CF1C83F-AC59-496F-AD9F-D2F06B7718DE},CN=Policies,CN=System,DC=ekoloclast,DC=fr	groupPolicyContainer	{1CF1C83F-AC59-496F-AD9F-D2F06B7718DE}	02/07/2024 00:17:56
CN=Machine,CN={1CF1C83F-AC59-496F-AD9F-D2F06B7718DE},CN=Policies,CN=System,DC=ekoloclast,DC=fr	container	Machine	02/07/2024 00:17:56
CN=User,CN={1CF1C83F-AC59-496F-AD9F-D2F06B7718DE},CN=Policies,CN=System,DC=ekoloclast,DC=fr	container	User	02/07/2024 00:17:56
CN=Class Store,CN=Machine,CN={1CF1C83F-AC59-496F-AD9F-D2F06B7718DE},CN=Policies,CN=System,DC=ekoloclast,DC=fr	classStore	Class Store	02/07/2024 00:19:26
CN=Packages,CN=Class Store,CN=Machine,CN={1CF1C83F-AC59-496F-AD9F-D2F06B7718DE},CN=Policies,CN=System,DC=ekoloclast,DC=fr	classStore	Packages	02/07/2024 00:19:26
CN=52f08a7b-9242-413b-be62-9d96b7b9f556,CN=Packages,CN=Class Store,CN=Machine,CN={1CF1C83F-AC59-496F-AD9F-D2F06B7718DE},CN=Policies,CN=System,DC=ekoloclast,DC=fr	packageRegistration	52f08a7b-9242-413b-be62-9d96b7b9f556	02/07/2024 00:19:26
CN={9E29C765-DCE1-42CB-BAAC-C3C49DE4D86F},CN=Policies,CN=System,DC=ekoloclast,DC=fr	groupPolicyContainer	{9E29C765-DCE1-42CB-BAAC-C3C49DE4D86F}	03/07/2024 17:42:56
CN=Machine,CN={9E29C765-DCE1-42CB-BAAC-C3C49DE4D86F},CN=Policies,CN=System,DC=ekoloclast,DC=fr	container	Machine	03/07/2024 17:42:56
CN=User,CN={9E29C765-DCE1-42CB-BAAC-C3C49DE4D86F},CN=Policies,CN=System,DC=ekoloclast,DC=fr	container	User	03/07/2024 17:42:56
CN=Class Store,CN=User,CN={9E29C765-DCE1-42CB-BAAC-C3C49DE4D86F},CN=Policies,CN=System,DC=ekoloclast,DC=fr	classStore	Class Store	03/07/2024 17:44:10
CN=Packages,CN=Class Store,CN=User,CN={9E29C765-DCE1-42CB-BAAC-C3C49DE4D86F},CN=Policies,CN=System,DC=ekoloclast,DC=fr	classStore	Packages	03/07/2024 17:44:10
CN=47fa54c6-b233-4d71-bcd8-1be346442bdd,CN=Packages,CN=Class Store,CN=User,CN={9E29C765-DCE1-42CB-BAAC-C3C49DE4D86F},CN=Policies,CN=System,DC=ekoloclast,DC=fr	packageRegistration	47fa54c6-b233-4d71-bcd8-1be346442bdd	03/07/2024 17:44:10
CN={B761ABCD-8B3E-4746-87A9-4536DE637D58},CN=Policies,CN=System,DC=ekoloclast,DC=fr	groupPolicyContainer	{B761ABCD-8B3E-4746-87A9-4536DE637D58}	04/07/2024 11:07:34
CN=Machine,CN={B761ABCD-8B3E-4746-87A9-4536DE637D58},CN=Policies,CN=System,DC=ekoloclast,DC=fr	container	Machine	04/07/2024 11:07:34
CN=User,CN={B761ABCD-8B3E-4746-87A9-4536DE637D58},CN=Policies,CN=System,DC=ekoloclast,DC=fr	container	User	04/07/2024 11:07:34
CN=kali,CN=Computers,DC=ekoloclast,DC=fr	computer	kali	08/07/2024 22:59:53

Saved to SI000044 tab in C:\Users\Administrator.EKOLOCLAST\Documents\PK Community 4.2\Output\07_10_2024_08_32_05\Security_Assessment_Report_10_07_2024_08_32_05.xlsx