Security Assessment

The Semperis Research Team continuously studies the ways cyber criminals are plotting to compromise organizations' information systems -- particularly by exploiting vulnerabilities in Active Directory. Leveraging the threat intelligence from our research team, Semperis is constantly updating the list of published security indicators available in our security assessment solutions:

- Purple Knight: Runs as a stand alone utility that queries your Active Directory environment providing a snapshot of your Active Directory security posture.
- Directory Services Protector Intelligence: Continuously monitors Active Directory for indicators of exposure, detects advanced attacks, and enables rapid response.

Both solutions perform a comprehensive set of tests against the most common and effective attack vectors to uncover risky configurations and security weaknesses. The following tables include the latest list of security indicators evaluated. In addition to the name and brief description of each security indicator, the following information is provided:

- SEVERITY: The severity level assigned based on proven risk analysis.
- FRAMEWORK: Indicates the security and governmental frameworks to which an IOE is aligned. It lists the MITRE ATT&CK® tactic categories and French National Agency for the Security of Information Systems (ANSSI) rules that correlate to each security indicator.
- PRE- / POST-ATTACK: Indicates what stage in the attack continuum (pre-attack or post-attack) each security indicator assists in providing defense:
    - The pre-attack security indicators focus on risky Active Directory configurations that could be exploited by an attacker. The pre-attack indicators help you understand how your Active Directory may be compromised and changes that could indicate nefarious behavior.
    - The post-attack security indicators look for evidence of actual compromise of Active Directory. The post-attack indicators help you understand how your Active Directory was compromised, revealing information such as evidence of backdoor accounts and suspicious recent changes.

*Denotes a new security indicator that was added since last major release.

Account Security

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

Table 1: Security Indicators: Account Security

INDICATOR OF EXPOSURE (IOE)	DESCRIPTION	SEVERITY	FRAMEWORK	PRE- / POST-ATTACK
AD objects created within the last 10 days	Looks for any AD objects that were recently created. Allows you to spot unknown or illegitimate accounts. Meant to be used for threat hunting, post-breach investigation, or compromise validation.	Informational	MITRE: Lateral Movement MITRE: Persistence	Pre-attack Post-attack
Admins with old passwords	Looks for Admin accounts whose password has not changed in over 180 days. If Admin account passwords are not changed on a regular basis, these accounts could be ripe for password guessing attacks.	Warning	MITRE: Discovery ANSSI: vuln1_ password_ change_priv	Pre-attack
Built-in domain Administrator account used within the last two weeks	Checks to see if the lastLogonTimestamp for the built-in Domain Administrator account has been recently updated. Could indicate that the user has been compromised.	Warning	MITRE: Defense Evasion	Pre-attack Post-attack
Built-in domain Administrator account with old password (180 days)	Checks to see if the pwdLastSet attribute on the built-in Domain Administrator account has been changed within the last 180 days. If this password is not changed on a regular basis, this account can be vulnerable to brute force password attacks.	Informational	MITRE: Credential Access	Pre-attack
Changes to privileged group membership in the last 7 days	Looks for recent changes to the built-in privileged groups. Could indicate attempts to escalate privilege.	Warning	MITRE: Persistence MITRE: Privilege Escalation	Pre-attack Post-attack
Computer accounts in privileged groups	Looks for computer accounts that are a member of a domain privileged group. If a computer account is a member of the domain privileged group, then anyone that compromises that computer account can act as a member of that group.	Warning	MITRE: Privilege Escalation	Pre-attack

Table 1: Security Indicators: Account Security (continued)

INDICATOR OF EXPOSURE (IOE)	DESCRIPTION	SEVERITY	FRAMEWORK	PRE- / POST-ATTACK
Enabled admin accounts that are inactive	Looks for admin accounts that are enabled, but have not log in for the past 90 days. Attackers who can compromise these accounts will be able to operate unnoticed.	Warning	MITRE: Credential Access MITRE: Privilege Escalation ANSSI: vuln1_ user_accounts_ dormant	Pre-attack
Forest contains more than 50 privileged accounts	Counts the number of privileged accounts defined in the forest. In general, the more privileged accounts you have, the more opportunities there are for attackers to compromise one of these accounts.	Informational	MITRE: Privilege Escalation MITRE: Reconnaissance ANSSI: vuln1_ privileged_ members	Pre-attack
Privileged accounts with a password that never expires	Identifies privileged accounts (adminCount = 1) where the "Password Never Expires" flag is set. User accounts whose passwords never expire are ripe targets for brute force password guessing. If these accounts are also administrative or privileged accounts, this makes them more of a target.	Warning	MITRE: Credential Access MITRE: Privilege Escalation ANSSI: vuln1_ dont_expire_priv	Pre-attack
Privileged users that are disabled	Looks for privileged user accounts that are disabled. If a privileged account is disabled, it should be removed from its privileged group(s) to prevent inadvertent misuse.	Informational	MITRE: Privilege Escalation	Pre-attack
* Privileged users with weak password policy	Looks for privileged users in each domain that do not have a strong password policy enforced, according to ANSSI framework . It checks both the Fine-Grained Password Policy (FGPP) and the password policy applied to the domain. A strong password defined by ANSSI is at least eight characters long and updated no later than every three years.	Critical	MITRE: Discovery	Pre-attack

Table 1: Security Indicators: Account Security (continued)

INDICATOR OF EXPOSURE (IOE)	DESCRIPTION	SEVERITY	FRAMEWORK	PRE- / POST-ATTACK
	Weak passwords are easier to crack via brute-force attacks and can provide attackers opportunities for moving laterally or escalating privileges. The risk is even higher for privileged accounts, for when compromised they improve the attacker's chance to quickly advance within the network.		ANSSI: vuln2_ privileged_ members_ password	
Protected Users group not in use	Detects when privileged users are not a member of the Protected Users group. The Protected Users group provides privileged users with additional protection from direct credential theft attacks.	Informational	MITRE: Credential Access ANSSI: vuln3_ protected_users	Pre-attack
Recent privileged account creation activity	Looks for any privileged users or groups (adminCount = 1) that were recently created. Allows you to spot privileged accounts and groups that were created without prior knowledge.	Informational	MITRE: Persistence	Pre-attack Post-attack
Recent sIDHistory changes on objects	Detects any recent changes to the sIDHistory on objects, including changes to non-privileged accounts where privileged SIDs are added. 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.	Warning	MITRE: Privilege Escalation	Pre-attack Post-attack
Security principals marked with adminCount=1	Checks for recent changes that have happened to the adminCount attribute. A change to the adminCount attribute could indicate that someone is trying to use an account as a backdoor for other activities.	Informational	MITRE: Privilege Escalation	Pre-attack Post-attack
Trust accounts with old passwords	Looks for trust accounts whose password has not changed within the last year. Trust accounts facilitate authentication across trusts and should be protected 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.	Informational	MITRE: Initial Access ANSSI: vuln2_ trusts_accounts	Pre-attack
Unprivileged principals as DNS Admins	Looks for any member of the DNS Admins group that is not a privileged user. Members of this group can be delegated to non-AD administrators (e.g. Admins with networking responsibilities, such as DNS, DHCP, etc.), which can result in these accounts being prime targets for compromise.	Warning	MITRE: Execution MITRE: Privilege Escalation ANSSI: vuln1_ permissions_msdn	Pre-attack

Table 1: Security Indicators: Account Security (continued)

INDICATOR OF EXPOSURE (IOE)	DESCRIPTION	SEVERITY	FRAMEWORK	PRE- / POST-ATTACK
			ANSSI: vuln1_ dnsadmins	
Unprotected accounts with adminCount=1	Looks for any users or groups that may be under the control of SDProp (adminCount=1) but are no longer members of privileged groups. Might be evidence of an attacker that attempted to cover their tracks and remove a user they used for compromise.	Informational	MITRE: Privilege Escalation	Pre-attack Post-attack
User accounts that store passwords with reversible encryption	Identifies accounts with the "ENCRYPTED_TEXT_PWD_ALLOWED" flag enabled. Attackers may be able to derive these users' passwords from the ciphertext and take over these accounts.	Informational	MITRE: Credential Access ANSSI: vuln3_ reversible_ password	Pre-attack
User accounts that use DES encryption	Identifies user accounts with the "Use Kerberos DES encryption types for this account" flag set. Attackers can easily crack DES passwords using widely available tools, making these accounts ripe for takeover.	Informational	MITRE: Credential Access ANSSI: vuln2_ kerberos_ properties_deskey	Pre-attack
User accounts with password not required	Identifies user accounts where a password is not required. Accounts with weak access controls are often targeted to move laterally or gain a persistence foothold with the environment.	Informational	MITRE: Lateral Movement	Pre-attack
Users and computers with non-default Primary Group IDs	Returns a list of all users and computers whose Primary Group IDs (PIDs) are not the defaults for domain users and computers. Modifying the Primary Group ID is a stealthy way for an attacker to escalate privileges without triggering member attribute auditing for group membership changes.	Informational	MITRE: Privilege Escalation ANSSI: vuln1_ primary_group_id_ 1000 ANSSI: vuln3_ primary_group_id_ nochange	Pre-attack Post-attack

Table 1: Security Indicators: Account Security (continued)

INDICATOR OF EXPOSURE (IOE)	DESCRIPTION	SEVERITY	FRAMEWORK	PRE- / POST-ATTACK
Users with Kerberos pre-authentication disabled	Looks for users with Kerberos pre-authentication disabled. These users can be targeted for ASREP-Roasting attacks (like "Kerberoasting").	Warning	MITRE: Credential Access ANSSI: vuln1_ kerberos_ properties_ preauth_priv ANSSI: vuln2_ kerberos_ properties_ preauth	Pre-attack
Users with old passwords	Looks for user accounts whose password has not changed in over 180 days. These accounts could be ripe for password guessing attacks.	Warning	MITRE: Credential Access MITRE: Persistence	Pre-attack
Users with Password Never Expires flag set	Identifies user accounts where the "Password Never Expires" flag is set. These accounts can be potential targets for brute force password attacks.	Informational	MITRE: Credential Access ANSSI: vuln2_ dont_expire	Pre-attack

AD Delegation

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.

Table 2: Security Indicators: AD Delegation

INDICATOR OF EXPOSURE (IOE)	DESCRIPTION	SEVERITY	FRAMEWORK	PRE- / POST-ATTACK
Built-in guest account is enabled	Checks to ensure that the built-in AD "guest" account is disabled. An enabled guest account allows for passwordless access to the domain, which could present a security risk.	Informational	MITRE: Discovery MITRE: Reconnaissance	Pre-attack
*Changes to AD display specifiers in the past 7 days	Looks for recent changes made to the adminContextMenu attribute on AD display specifiers. Modifying this attribute can potentially allow attackers to utilize context menus to get users to run arbitrary code.	Informational	MITRE: Defense Evasion MITRE: Execution	Pre-attack Post-attack
*Changes to AD display specifiers in the past 90 days	Looks for recent changes made to the adminContextMenu attribute on AD display specifiers. Modifying this attribute can potentially allow attackers to utilize context menus to get users to run arbitrary code.	Informational	MITRE: Defense Evasion MITRE: Execution	Pre-attack Post-attack
Changes to default security descriptor schema in the last 90 days	Detects recent schema attribute changes made on the default security descriptor. If an attacker gets access to the schema instance in a forest, any changes made can propagate to newly created objects in AD, potentially weakening AD security posture.	Warning	MITRE: Defense Evasion MITRE: Privilege Escalation	Pre-attack Post-attack
Changes to MS LAPS read permissions	Looks for permissions on computer accounts that could allow inadvertent exposure of local administrator accounts in environments that use Microsoft LAPS. Attackers may use this capability to laterally move through a domain using compromised local administrator accounts.	Informational	MITRE: Credential Access MITRE: Lateral Movement	Pre-attack
Delegation changes to Domain NC head in the last 7 days	Shows recent delegation changes that have occurred on the domain NC head. Changes in the delegation to this special object could grant unprivileged users the ability to synchronize the AD database for offline cracking (i.e., DCSync attack).	Warning	MITRE: Credential Access MITRE: Privilege Escalation	Pre-attack Post-attack

Table 2: Security Indicators: AD Delegation (continued)

INDICATOR OF EXPOSURE (IOE)	DESCRIPTION	SEVERITY	FRAMEWORK	PRE- / POST-ATTACK
Domain Controller owner is not an administrator	Looks for Domain Controller computer accounts whose owner is not a Domain Admins, Enterprise Admins, or built-in Administrator account. Gaining control of DC machine accounts allows for an easy path to compromising the domain.	Warning	MITRE: Credential Access MITRE: Privilege Escalation ANSSI: vuln1_ permissions_dc	Pre-attack
Enterprise Key Admins with full access to domain	Looks for evidence of a bug in certain versions of Windows Server 2016 Adprep that granted undue access to the Enterprise Key Admins group. This issue was corrected in a subsequent release of Windows 2016; however, if this fix has not been applied, this bug grants this group the ability to replicate all changes from AD (DCSync attack).	Warning	MITRE: Credential Access MITRE: Lateral Movement MITRE: Privilege Escalation ANSSI: vuln2_ adupdate_bad	Pre-attack
*Inheritance enabled on AdminSDHolder object	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 (for example, users or groups with adminCount=1). Changes to the AdminSDHolder object are very rate. Administrators should know that a change was made and be able to articulate the reason for the change. If the change was not intentional, the likehood of compromise is very high.	Critical	MITRE: Credential Access MITRE: Defense Evasion	Pre-attack
*Non-default access to DPAPI key	Checks domain controllers for non-default principals that are permitted to retrieve the domain DPAPI backup key. With these permissions, an attacker could recover all domain data encrypted via DPAPI.	Warning	MITRE: Credential Access ANSSI: vuln1_ permissions_dpapi	Pre-attack
Non-default principals with DC Sync rights on the domain	Looks for security principals with Replicating Changes All or Replicating Directory Changes permissions on the domain naming context object. Security principals with these permissions on the domain naming context object can potentially retrieve password hashes for users in an AD domain (DCSync attack).	Critical	MITRE: Credential Access	Pre-attack Post-attack

Table 2: Security Indicators: AD Delegation (continued)

INDICATOR OF EXPOSURE (IOE)	DESCRIPTION	SEVERITY	FRAMEWORK	PRE- / POST-ATTACK
			ANSSI: vuln1_ permissions_ naming_context	
Non-default value on ms-Mcs-AdmPwd SearchFlags	Looks for changes to the default searchFlags on the ms-Mcs-AdmPwd schema. Some flags may inadvertently cause the password to be visible to unintended users allowing an attacker to use it as a stealthy backdoor.	Warning	MITRE: Credential Access	Pre-attack
*Non-privileged users with access to gMSA passwords	Looks for principals listed within the MSDS-groupMSAmembership that are not in the built-in admin groups. An attacker that controls access to the gMSA account can retrieve passwords for resources managed with gMSA.	Warning	MITRE: Credential Access	Pre-attack
Objects in built-in protected groups without adminCount=1 (SDProp)	Looks for objects in built-in protected groups whose adminCount attribute is not set to 1. If an object within these groups has an adminCount not equal to 1, they could signify that the DACLs were manually set (no inheritance) or that there is an issue with SDProp.	Informational	MITRE: Defense Evasion MITRE: Persistence	Pre-attack Post-attack
Permission changes on AdminSDHolder object	Looks for Access Control List (ACL) changes on the AdminSDHolder object. Could indicate an attempt to modify permissions on privileged objects that are subject to AdminSDHolder.	Critical	MITRE: Defense Evasion MITRE: Privilege Escalation ANSSI: vuln1_ permissions_ adminsdholder ANSSI: vuln1_ priivileged_ members_prem	Pre-attack

Table 2: Security Indicators: AD Delegation (continued)

INDICATOR OF EXPOSURE (IOE)	DESCRIPTION	SEVERITY	FRAMEWORK	PRE- / POST-ATTACK
Privileged objects with unprivileged owners	Looks for privileged objects (adminCount =1) that are owned by an unprivileged account. Any compromise of an unprivileged account could result in a privileged object's delegation being modified.	Warning	MITRE: Privilege Escalation ANSSI: vuln1_ permissions_ adminsdholder	Pre-attack
Unprivileged users can add computer accounts to domain	Checks to see if unprivileged domain members are allowed to add computer accounts to a domain. Having the ability to add computer accounts to a domain can be abused by Kerberos-based attacks.	Informational	MITRE: Credential Access MITRE: Lateral Movement	Pre-attack

AD Infrastructure Security

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

Table 3: Security Indicators: AD Infrastructure Security

INDICATOR OF EXPOSURE (IOE)	DESCRIPTION	SEVERITY	FRAMEWORK	PRE- / POST-ATTACK
*AD Certificate Authority with Web Enrollment - PetitPotam and ESC8	Identifies AD CS servers in the domain that accept NTLM authentication to Web Enrollment. Attackers may abuse a flaw in AD CS Web Enrollment that enables NTLM relay attacks to authenticate as a privileged user.	Critical	MITRE: Credential Access MITRE: Privilege Escalation	Pre-attack
Anonymous access to Active Directory enabled	Looks for the presence of the flag that enables anonymous access. Anonymous access would allow unauthenticated users to query AD.	Critical	MITRE: Defense Evasion MITRE: Initial Access MITRE: Persistence MITRE: Privilege Escalation ANSSI: vuln2_ compatible_2000_ anonymous	Pre-attack
Anonymous NSPI access to AD enabled	Detects when anonymous name service provider interface (NSPI) access is enabled. Allows anonymous RPC-based binds to AD. NSPI is rarely enabled, so if it is found to be enabled it should be a cause for concern.	Warning	MITRE: Initial Access ANSSI: vuln1_ dsheuristics_bad	Pre-attack
Changes to nTSecurityDescriptor on MicrosoftDNS container in the last 30 days	Shows any changes made to SACL, DACL, or ownership of the MicrosoftDNS container object, which provides permissions and ownership of Microsoft DNS management services. The DNS infrastructure is a critical component of any IP network that can be abused by attackers to subvert network traffic.	Informational	MITRE: Execution	Pre-attack Post-attack

Table 3: Security Indicators: AD Infrastructure Security (continued)

INDICATOR OF EXPOSURE (IOE)	DESCRIPTION	SEVERITY	FRAMEWORK	PRE- / POST-ATTACK
Computers with older OS versions	Looks for machine accounts that are running versions of Windows older than Windows Server 2012 R2 and Windows 8.1. Computers running older and unsupported OS versions could be targeted with known or unpatched exploits.	Informational	MITRE: Lateral Movement MITRE: Persistence	Pre-attack
Computers with password last set over 90 days ago	Looks for computer accounts that have not automatically rotated their passwords. Computer accounts should automatically rotate their passwords every 30 days; objects that are not doing this could show evidence of tampering.	Warning	MITRE: Credential Access ANSSI: vuln2_password_change_server_no_change_90	Pre-attack
*Dangerous control paths expose certificate containers	Looks for non-default principals with permissions on the NTAuthCertificates container, which holds the intermediate CA certificates used to authenticate to Active Directory. Unprivileged users with permissions on the NTAuthCerticates container have the ability to escalate their access and make the domain trust a rogue CA.	Warning	MITRE: Credential Access ANSSI: vuln1_adcs_control	Pre-attack
*Dangerous control paths expose certificate templates	Looks for non-default principals with the ability to write properties on a certificate template. Unprivileged users with write properties on certificate templates have the ability to escalate their access and create vulnerable certificates to enroll.	Warning	MITRE: Credential Access ANSSI: vuln1_adcs_template_control	Pre-attack
Domain controllers in an inconsistent state	Looks for domain controllers that may be in an inconsistent state, indicating a possible rogue or otherwise non-functional DC. Illegitimate machines acting as DCs could indicate someone has compromised the environment (e.g., using DCShadow or similar DC spoofing attack).	Informational	MITRE: Privilege Escalation MITRE: Resource Development ANSSI: vuln1_dc_inconsistent_uac	Pre-attack Post-attack

Table 3: Security Indicators: AD Infrastructure Security (continued)

INDICATOR OF EXPOSURE (IOE)	DESCRIPTION	SEVERITY	FRAMEWORK	PRE- / POST-ATTACK
Domain controllers that have not authenticated to the domain for more than 45 days	Looks for domain controllers that have not authenticated to the domain in over 45 days. Lack of domain authentication reveals out-of-sync machines. If an attacker compromises an offline DC and cracks the credentials or re-connects to the domain, they may be able to introduce unwanted changes to Active Directory.	Warning	MITRE: Credential Access MITRE: Privilege Escalation ANSSI: vuln1_ password_change_ inactive_dc	Pre-attack
Domain controllers with old passwords	Looks for domain controller machine accounts whose password has not been reset in over 45 days. Machine accounts with older passwords could indicate a DC that is no longer functioning in the domain. In addition, DCs with older machine account passwords could be more easily taken over.	Informational	MITRE: Privilege Escalation MITRE: Resource Development ANSSI: vuln1_ password_change_ dc_no_change	Pre-attack
*Domain trust to a third-party domain without quarantine	Looks for outbound forest trusts that have the Quarantine flag set to false. An attacker that has compromised the remote domain can create a "spoofable" account to gain access to every resource on the local domain. If a dangerous control path is exposed, any "spoofable" account could also escalate his privileges up to Domain Admins and compromise the entire forest.	Warning	MITRE: Lateral Movement ANSSI: vuln1_ trusts_domain_ notfiltered	Pre-attack
Domains with obsolete functional levels	Looks for AD domains that have a domain functional level set to Windows Server 2012 or lower. Lower functional levels mean that newer security features available in AD cannot be leveraged.	Informational	MITRE: Reconnaissance	Pre-attack
Evidence of Mimikatz DCShadow attack	Looks for evidence that a machine has been used to inject arbitrary changes into AD using a "fake" domain controller. These changes bypass the security event log and cannot be spotted using standard monitoring tools.	Critical	MITRE: Defense Evasion	Post-attack

Table 3: Security Indicators: AD Infrastructure Security (continued)

INDICATOR OF EXPOSURE (IOE)	DESCRIPTION	SEVERITY	FRAMEWORK	PRE- / POST-ATTACK
gMSA objects with old passwords	Looks for group managed service accounts (gMSA) that have not automatically rotated their passwords. Objects that are not rotating their passwords regularly could show evidence of tampering.	Warning	MITRE: Credential Access	Pre-attack Post-attack
*Non-default access to gMSA root key	Looks for non-default principals with permissions to read the msKds-RootKeyData attribute on the KDS root key. Users with read permissions to this property could compromise every gMSA account in the forest.	Warning	MITRE: Credential Access ANSSI: vuln1_ permissions_gmsa_ keys ANSSI: vuln2_ permissions_gmsa_ keys	Pre-attack
*Non-standard schema permissions	Looks for additional principals with any permissions beyond generic Read to the schema partitions. By default, modification permissions on the schema are limited to Schema Admins. These permissions grant the trusted principal complete control over the Active Directory.	Warning	MITRE: Privilege Escalation ANSSI: vuln1_ permissions_ schema	Pre-attack
*NTFRS SYSVOL replication	Looks for indication of usage of FRS for SYSVOL replication. 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.	Warning	MITRE: Collection ANSSI: vuln2_ sysvol_ntfrs	Pre-attack
Operator groups no longer protected by AdminSDHolder and SDProp	Checks if dwAdminSDExMask on dsHeurstics has been set, which indicates a change to the SDProp behavior that could compromise security. A change to the AdminSDHolder SDProp behavior could indicate an attempt at defense evasion.	Warning	MITRE: Defense Evasion	Pre-attack Post-attack

Table 3: Security Indicators: AD Infrastructure Security (continued)

INDICATOR OF EXPOSURE (IOE)	DESCRIPTION	SEVERITY	FRAMEWORK	PRE- / POST-ATTACK
*Outbound forest trust with SID History enabled	Looks for outbound forest trusts that have the TRUST_ATTRIBUTE_TREAT_AS_EXTERNAL flag set to true. If this flag is set, a cross-forest trust to a domain is treated as an external trust for the purposes of SID filtering. This attribute relaxes the more stringent filtering performed on cross-forest trusts.	Warning	MITRE: Lateral Movement ANSSI: vuln1_ trusts_forest_ sidhistory	Pre-attack
*Print spooler service is enabled on a DC	Looks for domain controllers that have the print spooler service running, which is enabled by default. Several critical flaws were found in Windows Print Spooler services, which directly affect Print spoolers installed on domain controllers, enabling remote code execution.	Critical	MITRE: Execution MITRE: Lateral Movement MITRE: Privilege Escalation	Pre-attack
Risky RODC credential caching	Looks for a Password Replication Policy that allows privileged objects. If privileged users are in the allow list, they can be exposed to credential theft on an RODC.	Warning	MITRE: Credential Access ANSSI: vuln2_rodc_ priv_revealed	Pre-attack
*Unsecured DNS configuration	Looks for DNS zones configure with ZONE_UPDATE_UNSECURE, which allows updating a DSN record anonymously. An attacker could leverage this exposure to add a new DSN record or replace an existing DNS record to spoof a management interface, then wait for incoming connections in order to steal credentials.	Warning	MITRE: Privilege Escalation ANSSI: vuln1_ dnszone_bad_prop	Pre-attack
*Weak certificate encryption	Looks for certificates stored in Active Directory with keysize smaller than 1024 bits or using DSA encryption. Weak certificates can be abused by attackers to gain access to systems who use certificate authentication.	Critical	MITRE: Privilege Escalation ANSSI: vuln1_ certificates_vuln	Pre-attack
Well-known privileged SIDs in sIDHistory	Looks for security principals that contain specific SIDs of accounts from built-in privileged groups within the sIDHistory attribute. Allows 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).	Warning	MITRE: Defense Evasion MITRE: Privilege Escalation	Pre-attack Post-attack

Table 3: Security Indicators: AD Infrastructure Security (continued)

INDICATOR OF EXPOSURE (IOE)	DESCRIPTION	SEVERITY	FRAMEWORK	PRE- / POST-ATTACK
			ANSSI: vuln2_ sidhistory_ dangerous ANSSI: vul3_ sidhistory_present	
Zerologon vulnerability	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.	Critical	MITRE: Privilege Escalation	Pre-attack

Group Policy Security

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

Table 4: Security Indicators: Group Policy Security

INDICATOR OF EXPOSURE (IOE)	DESCRIPTION	SEVERITY	FRAMEWORK	PRE- / POST-ATTACK
Changes to Default Domain Policy or Default Domain Controllers Policy in the last 7 days	Looks for recent changes to the Default Domain Policy and Default Domain Controllers Policy GPOs. These GPOs control domain-wide and domain controller-wide security settings and can be misused to gain privileged access to AD.	Informational	MITRE: Defense Evasion MITRE: Privilege Escalation	Pre-attack Post-attack
Changes to GPO linking at the AD Site level in the last 7 days	Detects recent changes to AD Site GPO links. These types of changes can affect the security and privileged access of AD and your domain controllers.	Warning	MITRE: Credential Access MITRE: Execution MITRE: Privilege Escalation	Pre-attack Post-attack
Changes to GPO linking at the Domain level in the last 7 days	Detects recent changes to domain level GPO links. These are considered high security risk changes because these GPOs can affect all domain controllers, computers, and users in the domain.	Warning	MITRE: Credential Access MITRE: Execution MITRE: Privilege Escalation	Pre-attack Post-attack
GPO linking delegation at the AD Site level	Looks for non-privileged principals who have write permissions on the GPLink attribute or Write DACL/Write Owner on the object. When non-privileged users can link GPOs at the AD Site level, they have the ability to effect change on domain controllers. They can potentially elevate access and change domain-wide security posture.	Warning	MITRE: Execution MITRE: Privilege Escalation ANSSI: vuln1_ permissions_gpo_ priv	Pre-attack
GPO linking delegation at the domain controller OU level	Looks for non-privileged principals who have write permissions on the GPLink attribute or Write DAC/Write Owner on the object.	Warning	MITRE: Execution	Pre-attack

Table 4: Security Indicators: Group Policy Security (continued)

INDICATOR OF EXPOSURE (IOE)	DESCRIPTION	SEVERITY	FRAMEWORK	PRE- / POST-ATTACK
	When non-privileged users can link GPOs at the domain controller OU level, they have the ability to effect change on domain controllers. They can potentially elevate access and change domain-wide security posture.		MITRE: Privilege Escalation ANSSI: vuln1_ permissions_gpo_ priv	
GPO linking delegation at the domain level	Looks for non-privileged principals who have write permissions on the GPLink attribute or Write DACL/Write Owner on the object. 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. They can potentially elevate access and change domain-wide security posture.	Warning	MITRE: Defense Evasion MITRE: Privilege Escalation ANSSI: vuln1_ permissions_gpo_ priv	Pre-attack
Reversible passwords found in GPOs	Looks in the SYSVOL for GPOs that contain passwords that can be easily decrypted by an attacker (so called "Cpassword" entries). This area is one of the first things attackers look for when they've gained access to an AD environment.	Critical	MITRE: Credential Access	Pre-attack

Kerberos Security

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

Table 5: Security Indicators: Kerberos Security

INDICATOR OF EXPOSURE (IOE)	DESCRIPTION	SEVERITY	FRAMEWORK	PRE- / POST-ATTACK
Computer account takeover through Kerberos Resource-Based Constrained Delegation (RBCD)	Looks for the msDS-Allowed-ToActOnBehalfOfOtherIdentity attribute on computer objects. Attackers could use Kerberos RBCD configuration to escalate privileges through a computer they control if that computer has delegation to the target system.	Informational	MITRE: Credential Access MITRE: Lateral Movement MITRE: Privilege Escalation	Pre-attack
Computer or user accounts with unconstrained delegation	Looks for computer or user accounts that are trusted for unconstrained Kerberos delegation. Accounts with unconstrained delegation are easily targeted for Kerberos-based attacks.	Warning	MITRE: Defense Evasion MITRE: Lateral Movement ANSSI: vuln2_ delegation_t4d	Pre-attack
Domain controllers with Resource-Based Constrained Delegation (RBCD) enabled	Detects a configuration that grants certain accounts with complete delegation to domain controllers.	Warning	MITRE: Defense Evasion MITRE: Lateral Movement MITRE: Privilege Escalation ANSSI: vuln1_ delegation_ sourcedeleg	Pre-attack

Table 5: Security Indicators: Kerberos Security (continued)

INDICATOR OF EXPOSURE (IOE)	DESCRIPTION	SEVERITY	FRAMEWORK	PRE- / POST-ATTACK
Kerberos krbtgt account with old password	Looks for a krbtgt user account whose password has not changed in the past 180 days. If the krbtgt account's password is compromised, Golden Ticket attacks can be performed to obtain access to any resource in an AD domain.	Warning	MITRE: Credential Access ANSSI: vuln2_krbtgt	Pre-attack
Kerberos protocol transition delegation configured	Looks for services that have been configured to allow Kerberos protocol transition, which basically says that a delegated service can use any available authentication protocol. Compromised services can reduce the quality of their authentication protocol that is more easily compromised (e.g., NTLM).	Warning	MITRE: Credential Access MITRE: Lateral Movement MITRE: Privilege Escalation	Pre-attack
krbtgt account with Resource-Based Constrained Delegation (RBCD) enabled	Looks for a krbtgt account that has Resource-Based Constrained Delegation (RBCD) defined. Normally, delegations should not be created on the krbtgt account; if found, they could represent significant risk and should be mitigated quickly.	Warning	MITRE: Privilege Escalation ANSSI: vuln1_ delegation_a2d2	Pre-attack Post-attack
Objects with constrained delegation configured	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. Attackers may use delegations to move laterally or escalate privileges if they compromise a service that is trusted to delegate.	Informational	MITRE: Lateral Movement MITRE: Privilege Escalation	Pre-attack
Principals with constrained authentication delegation enabled for a DC service	Looks for computers and 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.	Warning	MITRE: Privilege Escalation	Pre-attack
Principals with constrained delegation using protocol transition enabled for a DC service	Looks for computers and users that have constrained delegation using protocol transition defined against a service running on a DC. If an attacker can create such a delegation for a service that they can control or compromise an existing service, they can effectively gain a TGS for any user with privileges to the DC.	Warning	MITRE: Privilege Escalation ANSSI: vuln1_ delegation_t2a4d	Pre-attack

Table 5: Security Indicators: Kerberos Security (continued)

INDICATOR OF EXPOSURE (IOE)	DESCRIPTION	SEVERITY	FRAMEWORK	PRE- / POST-ATTACK
Privileged users with ServicePrincipalNames defined	Looks for accounts with the adminCount attribute set to 1 AND ServicePrincipalNames (SPNs) defined on the account. Privileged accounts that have an SPN defined are targets for Kerberos-based attacks that can elevate privileges to those accounts.	Warning	MITRE: Credential Access MITRE: Privilege Escalation ANSSI: vuln1_spn_priv	Pre-attack
Users with ServicePrincipalName defined	Provides a way to visually inventory all user accounts that have ServicePrincipalNames (SPNs) defined. Generally, SPNs are only defined for "Kerberized" services; other accounts with an SPN may be cause for concern.	Informational	MITRE: Privilege Escalation	Pre-attack