Purple Knight 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.

Purple Knight is a security assessment tool that provides valuable insight into the security posture of your hybrid identity evironment. It runs as a stand alone utility that queries your Active Directory environment and performs a comprehensive set of tests against many aspects of Active Directory's security posture, including AD Delegation, Account security, AD Infrastructure security, Group Policy security, and Kerberos security. In this latest version, Purple Knight can also query your Azure Active Directory (Azure AD) environment focusing on some of the most common attack vectors that threat actors use to gain access to the Azure AD environment.

This document provides a list of security indicators included in Purple Knight. 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 indicator is aligned. It lists the MITRE ATT&CK® tactic categories, MITRE D3FEND™ cybersecurity countermeasures, and the French National Agency for the Security of Information Systems (ANSSI) rules that correlate to each security indicator.
- IOE / IOC: Indicates the type of security incident that can be detected to help you defend your Active Directory environment across the full attack continuum—before, during, and after an attack:
    - Indicators of Exposure (IOEs): Test against IOEs to uncover risky Active Directory configurations that could be exploited by an attacker. IOEs help you understand your current security posture to assist in closing attack paths and spotting modifications that suggest nefarious behavior.
    - Indicators of Compromise (IOCs): Scan for IOCs to identify evidence of actual compromise of Active Directory. IOCs help you understand how your Active Directory was breached, revealing information such as evidence of backdoor accounts and suspicious recent changes.

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

Published: July 2022

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 NAME	DESCRIPTION	SEVERITY	FRAMEWORK	IOE / IOC
Abnormal Password Refresh	Looks for user accounts with a recent pwdLastSet change without a corresponding password replication. If the "User must change password at next logon" option is set and then later cleared, could indicate an administrative error or an attempt to bypass the organization's password policy.	Warning	MITRE ATT&CK: Credential Access Persistence	IOE IOC
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 ATT&CK: Lateral Movement Persistence MITRE D3FEND: Detect - Domain Account Monitoring	IOE IOC
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 ATT&CK: Discovery MITRE D3FEND: Harden - Strong Password Policy ANSSI: vuln1_password_change_priv	IOE
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 ATT&CK: Defense Evasion MITRE D3FEND: Detect - Credential Compromise Scope Analysis Harden - Strong Password Policy	IOE IOC
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 ATT&CK: Credential Access MITRE D3FEND: Harden - Strong Password Policy	IOE

Table 1: Security Indicators: Account Security (continued)

INDICATOR NAME	DESCRIPTION	SEVERITY	FRAMEWORK	IOE / IOC
Changes to Pre-Windows 2000 Compatible Access Group membership	Looks for changes to the built-in "Pre-Windows 2000 Compatible Access" group. It is best to ensure this group does not contain the "Anonymous Logon" or "Everyone" groups.	Warning	MITRE ATT&CK: Privilege Escalation	IOE IOC
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 ATT&CK: Persistence Privilege Escalation	IOE IOC
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 ATT&CK: Privilege Escalation	IOE
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 ATT&CK: Credential Access Privilege Escalation MITRE D3FEND: Evict - Account Locking ANSSI: vuln1_user_accounts_dormant	IOE
Ephemeral Admins	Looks for users that were added and removed from an Admin group within a 48 hour period. Such short-lived accounts may indicate malicious activity.	Informational	MITRE ATT&CK: Persistence MITRE D3FEND: Harden - User Account Permissions	IOE IOC
* FGPP not applied to Group	Looks for fine-grained password policy (FGPP) targeted to a Universal or Domain Local group. Changing a group's scope setting from Global to Universal or Domain Local, results in FGPP settings no longer applying to that group, thus decreasing its password security controls.	Warning	MITRE ATT&CK: Credential Access Persistence MITRE D3FEND: Harden - Strong Password Policy	IOE
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.	Warning	MITRE ATT&CK: Privilege Escalation Reconnaissance ANSSI: vuln1_privileged_members	IOE

Table 1: Security Indicators: Account Security (continued)

INDICATOR NAME	DESCRIPTION	SEVERITY	FRAMEWORK	IOE / IOC
* Operator Groups that are not empty	Looks for operator groups (Account Operators, Server Operators, Backup Operators, Print Operators) that contain members. These groups have write access to critical resources on the domain; attackers that are members of these groups can take indirect control of the domain.	Warning	MITRE ATT&CK: Credential Access Privilege Escalation MITRE D3FEND: Harden - User Account Permissions	IOE
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 ATT&CK: Credential Access Privilege Escalation MITRE D3FEND: Harden - Strong Password Policy ANSSI: vuln1_dont_expire_priv	IOE
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 ATT&CK: Privilege Escalation MITRE D3FEND: Harden - User Account Permissions	IOE
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. 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.	Critical	MITRE ATT&CK: Discovery MITRE D3FEND: Harden - Strong Password Policy ANSSI: vuln2_privileged_members_password	IOE IOC
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 ATT&CK: Credential Access ANSSI: vuln3_protected_users	IOE

Table 1: Security Indicators: Account Security (continued)

INDICATOR NAME	DESCRIPTION	SEVERITY	FRAMEWORK	IOE / IOC
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 ATT&CK: Persistence MITRE D3FEND: Detect - Domain Account Monitoring	IOE IOC
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 ATT&CK: Privilege Escalation	IOE IOC
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 ATT&CK: Initial Access MITRE D3FEND: Harden - Strong Password Policy ANSSI: vuln2_trusts_accounts	IOE
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 ATT&CK: Execution Privilege Escalation ANSSI: vuln1_permissions_msdn vuln1_dnsadmins	IOE
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 ATT&CK: Privilege Escalation	IOE IOC
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 ATT&CK: Credential Access MITRE D3FEND: Harden - Strong Password Policy ANSSI: vuln3_reversible_password	IOE

Table 1: Security Indicators: Account Security (continued)

INDICATOR NAME	DESCRIPTION	SEVERITY	FRAMEWORK	IOE / IOC
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 ATT&CK: Credential Access ANSSI: vuln2_kerberos_properties_deskey	IOE
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 ATT&CK: Lateral Movement MITRE D3FEND: Harden - Strong Password Policy	IOE
Users and computers with non-default Primary Group IDs	Returns a list of all users and computers whose Primary Group IDs (PGIDs) 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 ATT&CK: Privilege Escalation ANSSI: vuln1_primary_group_id_1000 vuln3_primary_group_id_nochange	IOE IOC
Users and computers without readable PGID	Finds users and computers that can not read the Primary Group ID (PGID). May be caused by removing the default Read permission, which could indicate an attempt to hide the user (in combination with removal of the memberOf attribute).	Warning	MITRE ATT&CK: Defense Evasion	IOE IOC
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 ATT&CK: Credential Access ANSSI: vuln1_kerberos_properties_preauth_priv vuln2_kerberos_properties_preauth	IOE

Table 1: Security Indicators: Account Security (continued)

INDICATOR NAME	DESCRIPTION	SEVERITY	FRAMEWORK	IOE / IOC
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 ATT&CK: Credential Access Persistence MITRE D3FEND: Harden - Strong Password Policy	IOE
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 ATT&CK: Credential Access ANSSI: vuln2_dont_expire	IOE

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 NAME	DESCRIPTION	SEVERITY	FRAMEWORK	IOE / IOC
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 ATT&CK: Discovery Reconnaissance MITRE D3FEND: Evict - Account Locking	IOE
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 ATT&CK: Defense Evasion Execution	IOE IOC
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 ATT&CK: Defense Evasion Privilege Escalation MITRE D3FEND: Detect - Domain Account Monitoring	IOE IOC
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 ATT&CK: Credential Access Lateral Movement MITRE D3FEND: Harden - User Account Permissions	IOE
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 ATT&CK: Credential Access Privilege Escalation MITRE D3FEND: Harden - System Configuration Permissions ANSSI: vuln1_permissions_dc	IOE

Table 2: Security Indicators: AD Delegation (continued)

INDICATOR NAME	DESCRIPTION	SEVERITY	FRAMEWORK	IOE / IOC
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 ATT&CK: Credential Access Lateral Movement Privilege Escalation MITRE D3FEND: Harden - User Account Permissions ANSSI: vuln2_adupdate_bad	IOE
Foreign Security Principals in Privileged Group	Looks for members of built-in protected groups which are Foreign Security Principals. Special care should be taken when including accounts from other domains as members of privileged groups. Foreign Security Principals do not have the adminCount attribute and therefore may not be detected by some security auditing tools. Additionally, an attacker may add a privileged account and attempt to hide it using this method.	Warning	MITRE ATT&CK: Defense Evasion Persistence MITRE D3FEND: Detect - Domain Account Monitoring	IOE
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 likelihood of compromise is very high.	Critical	MITRE ATT&CK: Credential Access Defense Evasion	IOE IOC
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 ATT&CK: Credential Access MITRE D3FEND: Harden - User Account Permissions ANSSI: vuln1_permissions_dpapi	IOE
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 ATT&CK: Credential Access ANSSI: vuln1_permissions_naming_context	IOE

Table 2: Security Indicators: AD Delegation (continued)

INDICATOR NAME	DESCRIPTION	SEVERITY	FRAMEWORK	IOE / IOC
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 ATT&CK: Credential Access	IOE IOC
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 ATT&CK: Credential Access	IOE IOC
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 ATT&CK: Defense Evasion Persistence	IOE IOC
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 ATT&CK: Defense Evasion Privilege Escalation ANSSI: vuln1_permissions_adminsdholder vuln1_privileged_members_perm	IOE IOC
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 ATT&CK: Privilege Escalation ANSSI: vuln1_permissions_adminsdholder	IOE

Table 2: Security Indicators: AD Delegation (continued)

INDICATOR NAME	DESCRIPTION	SEVERITY	FRAMEWORK	IOE / IOC
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 ATT&CK: Credential Access Lateral Movement	IOE
Users with permissions to set Server Trust Account	Checks the domain NC head permissions to see if the Server_Trust_Account flag is set on computer objects. An attacker that can seed authenticated users with these permissions can utilize their access 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.	Critical	MITRE ATT&CK: Privilege Escalation	IOE

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 NAME	DESCRIPTION	SEVERITY	FRAMEWORK	IOE / IOC
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 ATT&CK: Credential Access Privilege Escalation	IOE
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 ATT&CK: Defense Evasion Initial Access Persistence Privilege Escalation MITRE D3FEND: Harden - User Account Permissions ANSSI: vuln2_compatible_2000_anonymous	IOE
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 ATT&CK: Initial Access MITRE D3FEND: Harden - User Account Permissions ANSSI: vuln1_dsheuristics_bad	IOE
* Certificate templates that allow requesters to specify a subjectAltName	Checks if certificate templates are enabling requesters to specify a subjectAltName in the CSR. 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.	Critical	MITRE ATT&CK: Credential Access Privilege Escalation MITRE D3FEND: Detect - Certificate Analysis	IOE

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

INDICATOR NAME	DESCRIPTION	SEVERITY	FRAMEWORK	IOE / IOC
* Certificate templates with three or more insecure configurations	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. Each of these configurations can be exploited by adversaries to gain access.	Warning	MITRE ATT&CK: Credential Access Privilege Escalation MITRE D3FEND: Detect - Certificate Analysis	IOE
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 ATT&CK: Lateral Movement Persistence MITRE D3FEND: Harden - Software Update	IOE
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 ATT&CK: Credential Access MITRE D3FEND: Harden - Strong Password Policy ANSSI: vuln2_password_change_server_no_change_90	IOE
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 ATT&CK: Credential Access MITRE D3FEND: Harden - Credential Transmission Scoping ANSSI: vuln1_adcs_control	IOE IOC
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 ATT&CK: Credential Access MITRE D3FEND: Detect - Certificate Analysis ANSSI: vuln1_adcs_template_control	IOE IOC

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

INDICATOR NAME	DESCRIPTION	SEVERITY	FRAMEWORK	IOE / IOC
Dangerous Trust Attribute Set	Identifies trusts with either of the following attributes set: TRUST_ATTRIBUTE_CROSS_ORGANIZATION_ENABLE_TGT_DELEGATION or TRUST_ATTRIBUTE_PIM_TRUST. Setting these attributes will either allow a kerberos ticket to be delegated or reduce the protection that SID filtering provides.	Warning	MITRE ATT&CK: Privilege Escalation MITRE D3FEND: Harden - Domain Trust Policy	IOE IOC
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 ATT&CK: Privilege Escalation Resource Development ANSSI: vuln1_dc_inconsistent_uac	IOE
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 ATT&CK: Credential Access Privilege Escalation MITRE D3FEND: Isolate - Execution Isolation ANSSI: vuln1_password_change_inactive_dc	IOE
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 ATT&CK: Privilege Escalation Resource Development MITRE D3FEND: Harden - Strong Password Policy ANSSI: vuln1_password_change_dc_no_change	IOE

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

INDICATOR NAME	DESCRIPTION	SEVERITY	FRAMEWORK	IOE / IOC
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 ATT&CK: Lateral Movement MITRE D3FEND: Harden - Domain Trust Policy ANSSI: vuln1_trusts_domain_notfiltered	IOE
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 ATT&CK: Reconnaissance MITRE D3FEND: Harden - Software Update	IOE
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 ATT&CK: Defense Evasion MITRE D3FEND: Detect - Domain Account Monitoring Isolate - Execution Isolation	IOE IOC
gMSA not used	Checks for enabled group Managed Service Accounts (gMSA) objects in the domain. The gMSA feature in Windows Server 2016 allows automatic rotation of passwords for service accounts, making them much more difficult for attackers to compromise.	Informational	MITRE ATT&CK: Credential Access	IOE
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 ATT&CK: Credential Access	IOE
* LDAP signing is not required on Domain Controllers	Looks for domain controllers where LDAP signing is not required. Unsigned network traffic is exposed to MITM (Man-in-the-Middle) 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.	Warning	MITRE ATT&CK: Credential Access Privilege Escalation	IOE

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

INDICATOR NAME	DESCRIPTION	SEVERITY	FRAMEWORK	IOE / IOC
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 ATT&CK: Credential Access ANSSI: vuln1_permissions_gmsa_keys vuln2_permissions_gmsa_keys	IOE IOC
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 ATT&CK: Privilege Escalation MITRE D3FEND: Harden - System Configuration Permissions ANSSI: vuln1_permissions_schema	IOE IOC
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 ATT&CK: Collection ANSSI: vuln2_sysvol_ntfrs	IOE
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 ATT&CK: Defense Evasion MITRE D3FEND: Harden - User Account Permissions	IOE
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 ATT&CK: Lateral Movement MITRE D3FEND: Harden - Domain Trust Policy ANSSI: vuln1_trusts_forest_sid-history	IOE

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

INDICATOR NAME	DESCRIPTION	SEVERITY	FRAMEWORK	IOE / IOC
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 ATT&CK: Execution Lateral Movement Privilege Escalation MITRE D3FEND: Harden - Software Update	IOE
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 ATT&CK: Credential Access MITRE D3FEND: Harden - User Account Permissions ANSSI: vuln2_rodc_priv_revealed	IOE
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 ATT&CK: Privilege Escalation ANSSI: vuln1_dnszone_bad_prop	IOE
Weak certificate encryption	Looks for certificates stored in Active Directory with keysize smaller than 2048 bits or using DSA encryption. Weak certificates can be abused by attackers to gain access to systems who use certificate authentication.	Critical	MITRE ATT&CK: Privilege Escalation MITRE D3FEND: Harden - Certificate-based Authentication ANSSI: vuln1_certificates_vuln	IOE

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

INDICATOR NAME	DESCRIPTION	SEVERITY	FRAMEWORK	IOE / IOC
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 ATT&CK: Defense Evasion Privilege Escalation ANSSI: vuln2_sidhistory_dangerous vuln3_sidhistory_present	IOE IOC
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 ATT&CK: Privilege Escalation	IOE

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 NAME	DESCRIPTION	SEVERITY	FRAMEWORK	IOE / IOC
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 ATT&CK: Defense Evasion Privilege Escalation	IOE IOC
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 ATT&CK: Execution Privilege Escalation ANSSI: vuln1_permissions_gpo_priv	IOE
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. 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.	Warning	MITRE ATT&CK: Execution Privilege Escalation ANSSI: vuln1_permissions_gpo_priv	IOE
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 ATT&CK: Defense Evasion Privilege Escalation ANSSI: vuln1_permissions_gpo_priv	IOE

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

INDICATOR NAME	DESCRIPTION	SEVERITY	FRAMEWORK	IOE / IOC
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 ATT&CK: Credential Access MITRE D3FEND: Detect - Emulated File Analysis	IOE
SYSVOL Executable Changes	Looks for modifications to executable files within SYSVOL. Changes to the executable files within SYSVOL should be accounted for or investigated to look for potential security posture weakening.	Informational	MITRE ATT&CK: Execution Persistence Privilege Escalation MITRE D3FEND: Detect - File Analysis	IOE IOC

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 NAME	DESCRIPTION	SEVERITY	FRAMEWORK	IOE / IOC
* Accounts with Constrained Delegation configured to krbtgt	Looks for accounts that have Constrained Delegation configured to the krbtgt service. Creating a Kerberos delegation to the krbtgt account itself allows that principal (user or computer) 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.	Critical	MITRE ATT&CK: Privilege Escalation MITRE D3FEND: Detect - Domain Account Monitoring	IOE
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 ATT&CK: Credential Access Lateral Movement Privilege Escalation	IOE IOC
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 ATT&CK: Defense Evasion Lateral Movement MITRE D3FEND: Detect - Domain Account Monitoring ANSSI: vuln2_delegation_t4d	IOE
Domain controllers with Resource-Based Constrained Delegation (RBCD) enabled	Detects a configuration that grants certain accounts with complete delegation to domain controllers.	Warning	MITRE ATT&CK: Defense Evasion Lateral Movement Privilege Escalation ANSSI: vuln1_delegation_sour-cedeleg	IOE IOC

Table 5: Security Indicators: Kerberos Security (continued)

INDICATOR NAME	DESCRIPTION	SEVERITY	FRAMEWORK	IOE / IOC
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 ATT&CK: Credential Access MITRE D3FEND: Harden - Strong Password Policy ANSSI: vuln2_krbtgt	IOE
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 ATT&CK: Credential Access Lateral Movement Privilege Escalation	IOE IOC
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.	Critical	MITRE ATT&CK: Privilege Escalation ANSSI: vuln1_delegation_a2d2	IOE IOC
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 ATT&CK: Lateral Movement Privilege Escalation MITRE D3FEND: Detect - Domain Account Monitoring	IOE IOC
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 ATT&CK: Privilege Escalation MITRE D3FEND: Detect - Domain Account Monitoring	IOE IOC
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 ATT&CK: Privilege Escalation ANSSI: vuln1_delegation_t2a4d	IOE IOC

Table 5: Security Indicators: Kerberos Security (continued)

INDICATOR NAME	DESCRIPTION	SEVERITY	FRAMEWORK	IOE / IOC
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 ATT&CK: Credential Access Privilege Escalation ANSSI: vuln1_spn_priv	IOE IOC
* RC4 encryption type is supported by Domain Controllers	Checks if RC4 encryption is supported by domain controllers. RC4 is considered an insecure form of encryption, susceptible to various cryptographic attacks. Multiple vulnerabilities in the RC4 algorithm allow MITM (Man-in-the-Middle) and deciphering attacks.	Warning	MITRE ATT&CK: Credential Access Privilege Escalation	IOE
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 ATT&CK: Privilege Escalation MITRE D3FEND: Detect - Domain Account Monitoring	IOE IOC
Write access to RBCD on DC	Looks for users who are not in Domain Admins, Enterprise Admins, or Built-in Admins groups that have write access on Resource-Based Constrained Delegation (RBCD) for domain controllers. Attackers that can gain write access to RBCD for a resource can cause the resource to impersonate any user (except where delegation is explicitly disallowed).	Warning	MITRE ATT&CK: Credential Access	IOE
Write access to RBCD on krbtgt account	Looks for users who are not in Domain Admins, Enterprise Admins, or Built-in Admins groups that have write access on Resource-Based Constrained Delegation (RBCD) for the krbtgt account. Attackers that can gain write access to RBCD for a resource can cause the resource to impersonate any user (except where delegation is explicitly disallowed).	Warning	MITRE ATT&CK: Credential Access	IOE

Azure AD

Azure AD indicators help you understand and mitigate the risks associates with a hybrid identity environment.

***NOTE**: Purple Knight: These indicators require Purple Knight v1.5 or later.*

Table 6: Security Indicators: Azure AD

INDICATOR NAME	DESCRIPTION	SEVERITY	FRAMEWORK	IOE / IOC
* AAD privileged users that are also privileged in AD	Checks for Azure AD privileged users that are also privileged users in on-premises AD. A compromise of an account that is privileged in both AD and AAD can result in both environments being compromised.	Warning	MITRE ATT&CK: Credential Access Privilege Escalation	IOE
* Administrative units are not being used	Checks for the existence of administrative units. Administrative units help limit the scope of a security principle's authority. Attackers that compromise an administrative account could have wide-ranging access across resources. By utilizing administrative units, it is possible to limit the scope of specific admins and ensure that a single compromise of credentials is constrained and does not affect the entire environment.	Informational	MITRE ATT&CK: Lateral Movement	IOE
* Check for guests having permission to invite other guests	Checks for guest invite permissions. It is not recommended to allow guests to send guest invitations.	Warning	MITRE ATT&CK: Lateral Movement	IOE
* Check for risky API permissions granted to application service principals	Checks for API permissions that could be risky if not properly planned and approved. A malicious application administrator could use these permissions to grant administrative privileges to themself or others.	Warning	MITRE ATT&CK: Privilege Escalation	IOE
* Check if legacy authentication is allowed	Check whether legacy authentication is blocked, either using conditional access policies or security defaults. Allowing legacy authentication increases the risk that an attacker will logon using previously compromised credentials.	Warning	MITRE ATT&CK: Credential Access	IOE

Table 6: Security Indicators: Azure AD (continued)

INDICATOR NAME	DESCRIPTION	SEVERITY	FRAMEWORK	IOE / IOC
* MFA not configured for privileged accounts	Checks whether Multi-Factor Authentication (MFA) is enabled for users with administrative rights. Accounts with privileged access are more vulnerable targets to attackers. A compromise of a privileged user represents a significant risk and therefore requires extra protection.	Warning	MITRE ATT&CK: Credential Access	IOE
* Non-admin users can register custom applications	Checks for an authorization policy that enables non-admin users to register custom applications. If non-admin users are allowed to register custom-developed enterprise applications, attackers might use that loophole to register nefarious applications, which they can then leverage to gain additional permissions.	Warning	MITRE ATT&CK: Persistence Privilege Escalation	IOE
* Privileged group contains guest account	Checks whether any privileged roles have been assigned to guest accounts. External attackers covet privileged accounts, as they provide a fast track to an organization's most critical systems. Guest accounts represent an external entity that does not undergo the same security as users in your tenant; therefore, assigning privileged roles to them poses a heightened risk.	Warning	MITRE ATT&CK: Privilege Escalation	IOE
* Security defaults not enabled	When there are no conditional access policies configured, this indicator checks whether security defaults are enabled. It is recommended that security defaults be used for tenants that have no conditional access policies configured. Security defaults will require MFA, block legacy authentication, and require additional authentication when accessing the Azure portal, Azure PowerShell, and the Azure CLI.	Warning	MITRE ATT&CK: Credential Access Initial Access	IOE
* Unrestricted user consent allowed	Checks is users are allowed to add application from unverified publishers. When users are allowed to consent to any third party applications, there is considerable risk that an allowed application will take intrusive or risky actions.	Warning	MITRE ATT&CK: Lateral Movement Persistence	IOE