semperis

Uncover weaknesses in Active Directory before attackers do.

DATA SHEET INDICATORS OF EXPOSURE

Uncover weaknesses in Active Directory before attackers do.

Semperis Directory Services Protector (DSP) continuously scans Active Directory (AD) to uncover security vulnerabilities and risky configurations. Users receive prioritized, action-oriented guidance to fix existing and new weak spots. Semperis DSP proactively hardens AD against adversary tactics and techniques with built-in threat intelligence from a community of researchers. Powerful reporting enables organizations to reduce their attack surface and track improvement over time.

INDICATOR OF EXPOSURE (IOE)	IOE DESCRIPTION	MITRE ATT&CK MATRIX™
Active Directory Delegation		
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.	Privilege Escalation Defense Evasion
Normal Users Can Add Computer Accounts to Domain	Checks to see if regular users are allowed to add machine accounts to a domain. Having the ability to add machine accounts to a domain can be abused by Kerberos-based attacks.	Credential Access Lateral Movement
Default Security Descriptor Changes in Schema in the Last 7 Days	Detects schema attribute changes 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.	Persistence Defense Evasion Lateral Movement
Delegation Changes to Domain NC Head in the Last 7 Days	Shows 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).	Privilege Escalation Credential Access Lateral Movement Defense Evasion
Changes to LAPS Read Permissions	Looks for changes to the security descriptor on computer accounts. Allows you to spot ACL changes that could allow an attacker to view the Microsoft LAPS local administrator account password attribute.	Credential Access Lateral Movement

INDICATOR OF EXPOSURE (IOE)	IOE DESCRIPTION	MITRE ATT&CK MATRIX™
Account Security		
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.	Credential Access
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 AD, which could present a security risk.	Discovery
Protected Users Group in Use	Detects when users are added to the Protected Users group.	Credential Access
Security Principals Marked with AdminCount Equals 1	Checks for changes that have happened to the AdminCount attribute. Could indicate someone is trying to use an account as a back door for other activities.	Defense Evasion
Users with Risky User Account Control	Identifies user accounts where the Password Not Required, Trusted for Delegation, Passwords Encrypted with DES, Passwords with Reversible Encryption, Trusted to Authenticate for Delegation, or Don't Require Pre-Authentication flags are set. These flags all represent potential weaknesses in user accounts, which make them targets of takeover attacks.	Privilege Escalation Credential Access Lateral Movement Defense Evasion
Security Principals with Built-in Privileged Groups in SidHistory	Looks for security principals (users or groups) that have a privileged built-in group in their sidHistory attribute. Could indicate that an attacker is attempting to use the account as a back door for privileged access.	Privilege Escalation Persistence
Active Directory Infrastructure Security		
Mimikatz DCShadow in Use	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 normal AD tools.	Persistence Defense Evasion
Anonymous Access to Active Directory Enabled	Looks for the presence of the flag that enables anonymous access to AD.	Initial Access Discovery

INDICATOR OF EXPOSURE (IOE)	IOE DESCRIPTION	MITRE ATT&CK MATRIX™
Group Policy		
Changes to Default Domain Policy or Default Domain Controllers Policy in the Last 7 Days	Looks for 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.	Privilege Escalation Execution
Changes to GPO Linking at the AD Site Level in the Last Day	Detects any GPOs linked or unlinked at the AD Site level. These types of changes can affect the security and privileged access of AD and your domain controllers.	Privilege Escalation Execution
Changes to GPO Linking at the Domain Level in the Last Day	Detects any GPOs linked or unlinked at the Domain level. These are considered high security risk changes because these GPOs can affect all domain controllers, computers, and users in the domain.	Privilege Escalation Execution
Kerberos Security		
Computer Account Takeover through Kerberos Resource-based Constrained Delegation (RBCD)	Looks for changes to the msDS-Allowed-ToActOnBehalfOfOtherIdentity attribute on computer objects to discover if a takeover activity is happening. Could indicate resources are compromised using RBCD.	Privilege Escalation Credential Access Lateral Movement
Computer or User Accounts with Unconstrained Delegation	Looks for computer or user accounts that have unconstrained Kerberos delegation defined. Accounts with unconstrained delegation are easily targeted for Kerberos-based attacks.	Privilege Escalation Credential Access Lateral Movement
Kerberos Golden Ticket Susceptibility	Looks for a Krbtgt user account whose password hasn't changed in the past 180 days. If the Krbtgt account's password is compromised, so-called Golden Ticket attacks can be performed to obtain access to any resource in an AD domain.	Privilege Escalation Credential Access Lateral Movement
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.	Privilege Escalation Credential Access

+1-703-918-4884
info@semperis.com
www.semperis.com

7 World Trade Center at
250 Greenwich Street, 10th floor
New York NY 10007

Semperis is the pioneer of identity-driven cyber resilience for cross-cloud and hybrid environments. The company provides cyber preparedness, incident response, and disaster recovery solutions for enterprise directory services—the keys to the kingdom. Semperis' patented technology for Microsoft Active Directory protects over 40 million identities from cyberattacks, data breaches, and operational errors. Semperis is headquartered in New York City and operates internationally, with its research and development team distributed between San Francisco and Tel Aviv.

Semperis hosts the award-winning Hybrid Identity Protection conference. The company has received the highest level of industry accolades; most recently being named Best Business Continuity / Disaster Recovery Solution by SC Magazine's 2020 Trust Awards. Semperis is accredited by Microsoft and recognized by Gartner.

semperis