CHECKLIST REVIEW POLICY CONFIGURATION (RSoP)								
STT	**Criteria**	**Request**	**How to check**	**Describe**	**Default configuration**	**Recommendation**	**Severity**	**References**
1					Password Policy			
1.1	Enforce password history	>= 24 passwords	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Account Policy/Password Policy	Passwords are easier to guess/crack if you reuse the same password too many times.	Default: 24 on domain controllers. 0 on stand-alone servers.	By default, for stand-alone servers, this configuration is 0 (meaning that the user is not required to change the new password to a different password from the old one), and for domain controllers, the default configuration is 24 (meaning that the user is required to change the new password to a different password from the 24 most recent old passwords). As for Best practice, the configuration requirement is 24, so the default configuration of the Domain Controller has met the requirements. Check if the Window Server is a Domain Controller or not: Check the path in the registry HKLM\System\CurrentControlSet\Control\ProductOptions\ProductType, if the value of ProductType is LanmanNT, the Server is operating as a Domain Controller, and the value is ServerNT, meaning it is operating as a normal Server.	Medium	(CIS Control v7.1) 16.10 Ensure All Accounts Have An Expiration Date Microsoft:https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/enforce-password-history
1.2	Maximum password age	30 <= && <=90 days (!= 0)	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Account Policy/Password Policy	The longer a password is used, the greater the risk. Changing your password periodically will help prevent offline password cracking attacks. A value of 0 means the password never expires.	Default: 42	By default, this parameter is configured as 42, meaning the password expiration date is 42 days. As for Best practice, the configuration requirement is 30-90 days, so the default configuration meets the requirements.	Medium	(CIS Control v7.1) 16.10 Ensure All Accounts Have An Expiration Date Mixcrosoft:https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/maximum-password-age
1.3	Minimum password age	>= 01 day	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Account Policy/Password Policy	Users can perform password reset multiple times to bypass the Enforce password history policy.	Default: 1 on domain controllers. 0 on stand-alone servers.	By default, this parameter is configured as 1 for domain controllers, meaning that after changing the password, you must wait 1 day before you can continue changing the password, and for stand-alone servers it is 0. As for Best practice, the requirement is set to 1 day, to avoid users changing their passwords continuously, bypassing the password history policy. Thus, the default parameter of the Domain controller has met the requirements.	Medium	(CIS Control v7.1) 16.10 Ensure All Accounts Have An Expiration Date Microsoft:https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/minimum-password-age
1.4	Minimum password length	>= 14 characters	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Account Policy/Password Policy	Passwords that are long enough will make cracking more difficult. It is recommended to use passphrases instead of passwords.	Default: 7 on domain controllers. 0 on stand-alone servers.	By default, this parameter is configured as 7 for domain controllers (requiring a minimum password length of 7) and 0 for stand-alone servers (requiring no password). As for Best Practice, the minimum password length is set to 14 characters. Note that previously, Windows did not support setting the minimum password length to more than 14 characters, but only from Windows Server version 2016 onwards. If it is an older version of Windows, it is only required to set it to 14.	Medium	(CIS Control v8) 16.10 Unique Password Microsoft:https://learn.microsoft.com/en-us/answers/questions/663081/enforcing-minimum-password-length-longer-than-14-c
1.5	Password must meet complexity requirements	Enabled	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Account Policy/Password Policy	Complex passwords make cracking more difficult	Default: Enabled on domain controllers. Disabled on stand-alone servers.	By default, this parameter is configured as Enabled on domain controllers (meaning the password must contain uppercase, lowercase, numbers, special characters and must not contain the login name or any part of the Full Name, Display Name), but not required on stand-alone servers. As for Best practice, the requirement is set to Enabled, so the default parameter of the Domain controller has met the requirement.	Medium	(CIS Control v8) 16.10 Unique Password Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
1.6	Store passwords using reversible encryption	Disabled	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Account Policy/Password Policy	Storing passwords in decipherable encrypted forms is just as risky as storing them unencrypted.	Default: Disabled.	The default configuration for this feature is Disabled, which disables password encryption using key-based encryption methods (which are not as secure as non-reversible methods like hashing). Best practices also require a similar configuration, which requires setting Disabled for this setting, so the Domain controller defaults are sufficient.	Medium	(CIS Control v7.1) 16.4 Encrypt or Hash All Authentication Credentials Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
2					Account Lockout Policy			
2.1	Account lockout duration	>= 15 min	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Account Policy/Account Lockout Policy	Set temporary account lock time, used to prevent password brute-force attacks	Default: None, because this policy setting only has meaning when an Account lockout threshold is specified.	By default, this configuration does not apply, only when the Account lockout threshold configuration is defined, this configuration will be applied. According to Best Practice, this parameter needs to be configured at least 15 minutes, meaning the password lock time after a number of consecutive incorrect logins is 15 minutes. Note that if set to 0, the account will be locked and will need to be reopened by the admin. Setting it like that is not wrong but not necessary.	Medium	(CIS Control v7.1) 16.11 Lock Workstation Sessions After Inactivity Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
2.2	Account lockout threshold	<= 05 attemp(s) (>0)	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Account Policy/Account Lockout Policy	Set the allowed password failure value, used to prevent password brute-force attacks. Value 0 corresponds to setting unlimited number of password failure attempts.	Default: 0.	By default, this configuration is 0, which means the account will never be locked out no matter how many times you log in incorrectly. According to Best Practice, the configuration should be greater than 0, maximum 3, however, depending on the unit with different password policies, we should set the maximum to 5.	Medium	(CIS Control v7.1) 16.11 Lock Workstation Sessions After Inactivity Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
2.3	Reset account lockout counter after	>= 15 min	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Account Policy/Account Lockout Policy	Set the account unlock time. The lower the value, the higher the risk of bruteforce attack	Default: None, because this policy setting only has meaning when an Account lockout threshold is specified.	Similar to Account lockout duration, this parameter is only applied when Account lockout threshold is defined, by default it is not applied. According to Best practice, this parameter should be less than or equal to Account lockout duration, and configured at least 15 min.	Medium	(CIS Control v7.1) 16.11 Lock Workstation Sessions After Inactivity Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
3					User Rights Assignment			
3.1	Access this computer from the network	Administrators Authenticated Users	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/User Rights Assignment	Allows users to connect to network protocols such as SMB, NetBIOS, CIFS and COM+, and thus read data associated with these protocols.	Default on workstations and servers: Administrators Backup Operators Users Everyone Default on domain controllers: Administrators Authenticated Users Enterprise Domain Controllers Everyone Pre-Windows 2000 Compatible Access	By default, this parameter for both Server and Domain controller allows many default groups/users, especially Everyone, allowing all user accounts including accounts that do not require password authentication such as Guest. According to Best practice, there are only 3 groups/users that we need to allow: Administrators, Authenticated Users, Enterprise Domain Controllers.	Medium	(CIS Control v7.1) 9.2 Ensure Only Approved Ports, Protocols, and Services Are Running Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf

CHECKLIST REVIEW POLICY CONFIGURATION (RSoP)								
STT	**Criteria**	**Request**	**How to check**	**Describe**	**Default configuration**	**Recommendation**	**Severity**	**References**
3.2	Deny access to this computer from the network	Guest Administrators Local Account	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/User Rights Assignment	Prevent guest accounts from being able to query system information Prevent Administrator accounts from being used in unsafe environments	Default: Guest	By default, only Guest group/users will be denied, but to ensure safety, we should also deny other local accounts, only allow login using domain accounts to ensure MFA authentication (if any) and assign permissions to ensure the least privilege rule. According to Best practice, only Guest user/group is required to be denied, but combined with practical experience, we should deny other local accounts.	Medium	(CIS Control v7.1) 4.3 Ensure the Use of Dedicated Administrative Accounts Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
3.3	Deny log on as a batch job	Guest Domain Admins Enterprise Admins	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/User Rights Assignment	Prevent guest accounts from being able to query system information Prevent Administrator accounts from being used in unsafe environments	Default: None.	By default, the server does not deny any user, meaning that all accounts can run batch jobs (automated tasks, scripts similar to cron), these tasks are usually handled and managed by Local Administrator as well as other local accounts. According to Best practice, only Guest user/group is required to be denied, but combined with practical experience, it is recommended to deny Active Directory Administrator accounts (Domain/Enterprise Admins), do not use accounts with maximum rights in the entire system used to run batch jobs because of serious security risks.	Medium	(CIS Control v7.1) 4.3 Ensure the Use of Dedicated Administrative Accounts Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
3.4	Deny log on as a service	Guest Domain Admins Enterprise Admins	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/User Rights Assignment	Prevent guest accounts from being able to query system information Prevent Administrator accounts from being used in unsafe environments	Default: None.	By default, the server does not deny any user, meaning all accounts can run or start services. According to Best Practice, this item should not be configured because of the risk of misconfiguration causing DoS service failure due to blocked users. However, combined with practical experience, it is necessary to deny additional accounts that are definitely never used to run services, which are Active Directory Administrator accounts (Domain/Enterprise Admins) and Guest accounts.	Medium	(CIS Control v7.1) 4.3 Ensure the Use of Dedicated Administrative Accounts Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
3.5	Deny log on through Remote Desktop Services	Guest Administrators Domain Admins Enterprise Admins Local Account	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/User Rights Assignment	Prevent guest accounts from being able to query system information Prevent Administrator accounts from being used in unsafe environments	Default: None.	By default, the server does not deny any user, meaning all accounts can use the RDP service to log in remotely. According to Best Practice, Active Directory Administrator accounts (Domain/Enterprise Admins), Local accounts (including Local Administrators) and Guest accounts need to be denied.	Medium	(CIS Control v7.1) 4.3 Ensure the Use of Dedicated Administrative Accounts Stig: https://www.stigviewer.com/stig/windows_server_2016/2019-12-12/finding/V-73775
3.6	Deny log on locally	Guest Domain Admins Enterprise Admins	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/User Rights Assignment	Prevent guest accounts from being able to query system information	Default: None.	By default, the server does not deny any user, meaning that all accounts can be used to log in directly locally or via RDP. According to Best Practice, only Guest accounts need to be denied, however, combined with practical experience, it is necessary to disable additional accounts that are definitely never allowed to be used to log in because of the risk of abuse of power, such as Active Directory Administrator accounts (Domain/Enterprise Admins).	Medium	(CIS Control v7.1) 4.3 Ensure the Use of Dedicated Administrative Accounts Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
3.7	Allow log on locally	Administrators	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/User Rights Assignment	Allows accounts to log into the computer via interactive login methods such as Console, Remote Desktop, etc. If not limited, unauthorized users can perform malicious tasks to elevate their rights on the system.	Default: • On workstations and servers: Administrators, Backup Operators, Power Users, Users, and Guests. • On domain controllers: Account Operators, Administrators, Backup Operators, and Print Operators.	By default, the server allows many accounts to be used to log in directly locally or via RDP. According to Best practice, only allow Administrators accounts to ensure access for only accounts with administrative purposes.	Medium	(CIS Control v7.1) 4.3 Ensure the Use of Dedicated Administrative Accounts Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
3.8	Allow log on through Remote Desktop Services	Administrator	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/User Rights Assignment	Allows accounts to log into computers via Remote Desktop. If not limited, unauthorized users can perform malicious tasks that elevate their privileges on the system.	Default: On workstation and servers: Administrators, Remote Desktop Users. On domain controllers: Administrators	By default, for stand-alone servers, this configuration allows the use of RDP service to log in with both Administrators accounts and Remote Desktop Users accounts, while for domain controllers, the default configuration only allows Administrators accounts. According to Best practice, only Administrator accounts will be allowed because this configuration will allow the use of RDP service to log in remotely even if the account is not allowed in Allow log on locally. Thus, the default configuration of Domain Controller has met the requirements.	Medium	(CIS Control v7.1) 4.3 Ensure the Use of Dedicated Administrative Accounts Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
3.9	Shut down the system	Administrators	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/User Rights Assignment	An attacker can abuse this right to shut down the server, causing a DoS attack.	Default on Workstations: Administrators, Backup Operators, Users. Default on Servers: Administrators, Backup Operators. Default on Domain controllers: Administrators, Backup Operators, Server Operators, Print Operators.	By default, this parameter for both Server and Domain controller allows many default groups/users, especially Print Operators, allowing these accounts to have the right to shutdown the system, causing the risk of DoS attack. According to Best practice, for stand-alone server, Administrators and Backup Operators accounts are allowed, while for Domain Controller, only Administrators accounts are allowed.	Medium	(CIS Control v7.1) 4.3 Ensure the Use of Dedicated Administrative Accounts Stig Benchmark: Microsoft:https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/shut-down-the-system
3.10	Act as part of the operating system	None	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/User Rights Assignment	Allows anyone assigned this permission to have full access to that machine.	Default: None.	By default, this parameter is configured as None, which means that no account is allowed to have "part of OS" rights, which means that it has the right to execute and impact the system under the name of all other accounts, and access resources that are specifically licensed to those accounts, or it can be said that it has the right to access and impact the entire system. According to Best practice, it is not allowed to allow any account, so the default configuration of the Domain Controller has met the requirements.	High	(CIS Control v7.1) 4.3 Ensure the Use of Dedicated Administrative Accounts Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
4	Security Options							
4.1	Accounts: Administrator account status	Disabled	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/Security Options/	Disable the local Administrator account. This is an account with high privileges in the system, but it is difficult to manage password changes. Therefore, to ensure safety, this account should be disabled.	Default: Disabled.	The default of this parameter is Disable, meaning that the local Administrator account is disabled by default due to security risks related to passwords (the account is not locked when the password is entered incorrectly continuously, the password change process must be done manually, which is not really necessary because even if disabled, when booting through safe mode, this local Administrator account will be automatically enabled and allowed access). According to Best Practice, this account should be Disabled, so for this parameter, the default value has met the requirements (this criterion does not apply to Domain Controllers because Domain Controllers do not have local accounts because the SAM database containing information about local accounts will be disabled, in case of booting into Safe Mode to fix errors, a special account, DSRM, will be used).	Low	(CIS Control v7.1) 16.8 Disable Any Unassociated Accounts Microsoft: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/accounts-administrator-account-status

CHECKLIST REVIEW POLICY CONFIGURATION (RSoP)								
STT	**Criteria**	**Request**	**How to check**	**Describe**	**Default configuration**	**Recommendation**	**Severity**	**References**
4.2	Domain member: Digitally encrypt or sign secure channel data (always)	Enabled	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/Security Options/	Secure channel protects domain account information as it is sent to the Domain Controller	Default: Enabled.	When a computer is joined to a domain, a computer account will be created on AD. Then the password of this account will be used to create a secure channel to connect to the domain controller. The default for this parameter is enabled, meaning that the configuration Digitally sign secure channel data (when possible) will be considered enabled regardless of its current configuration. This is to ensure at least the signing process for secure channel traffic. And for logon information, it is always encrypted regardless of whether the remaining traffic supports encryption or not. Thus, the default configuration has met the requirements.	Medium	(CIS Control v7.1) 5.1 Establish Secure Configurations Microsoft:https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/domain-member-digitally-encrypt-or- sign-secure-channel-data-always
4.3	Domain member: Digitally encrypt secure channel data (when possible)	Enabled	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/Security Options/	Secure channel protects domain account information as it is sent to the Domain Controller	Default: Enabled.	By default, this parameter is Enabled, which means it will encrypt all data sent in the connection between clients and Domain Controller, ensuring that information is encrypted and not leaked during communication. According to Best practice, this parameter needs to be configured as Enabled, so here the default parameter meets the requirements.	Medium	(CIS Control v7.1) 5.1 Establish Secure Configurations Windows:https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/domain-member-digitally-encrypt-or- sign-secure-channel-data-always
4.4	Domain member: Digitally sign secure channel data (when possible)	Enabled	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/Security Options/	Secure channel protects domain account information as it is sent to the Domain Controller	Default: Enabled.	By default, this parameter is Enabled, which means it will sign all data sent in the connection between clients and Domain Controller, ensuring that information is not changed or forged. According to Best practice, this parameter needs to be configured as Enabled, so here the default parameter meets the requirements.	Medium	(CIS Control v7.1) 5.1 Establish Secure Configurations Microsoft:https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/domain-member-digitally-encrypt-or- sign-secure-channel-data-always
4.5	Domain member: Disable machine account password changes	Disabled	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/Security Options/	If the computer does not automatically change the computer account password, there is a risk that an attacker can obtain the computer account password.	Default: Disabled.	Machine account password is used to create secure channel with connections authenticated by AD. Password is handled automatically by AD, computer authenticate and request to change password, AD will automatically update the new password. By default, this parameter is configured as Disable, which means that this password must be changed periodically, and according to Best practice, this parameter is also required to be Disabled, so the default parameter has met the requirements.	Medium	(CIS Control v7.1) 5.1 Establish Secure Configurations Microsoft:https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/domain-member-disable-machine-account- password-changes
4.6	Domain member: Maximum machine account password age	<= 30 day(s) (>0)	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/Security Options/	If the password change period for computer accounts is longer than 30 days or the value is 0 (no password change), it will increase the risk that attackers can perform attacks to successfully obtain passwords.	Default: 30 days.	The default for this parameter is 30 days, meaning the maximum time limit for a machine account password before it must be changed is 30 days. According to Best Practice, this parameter is also required to be configured for about 30 days, so this parameter has met the requirements by default.	Medium	(CIS Control v7.1) 16.10 Ensure All Accounts Have An Expiration Date Microsoft:https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/domain-member-maximum-machine-account- password-age
4.7	Domain member: Require strong (Windows 2000 or later) session key	Enabled	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/Security Options/	Session keys are used to establish a secure communication channel between the Domain Controller and member computers. Complex session keys provide increased protection against eavesdropping attacks.	Default: Enabled.	By default, this value is configured as Enabled, which means checking if the session key is strong enough (128-bit) before creating a secure channel connection. According to Best Practice, this parameter is also required to be Enabled, so by default this parameter meets the requirements.	Medium	Microsoft:https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/domain-member-require-strong-windows- 2000-or-later-session-key
4.8	Interactive logon: Machine inactivity limit	<= 900 second(s) (>0)	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/Security Options/	If the user forgets to lock the screen after use, it is a risk for attackers to gain unauthorized access. A value of 0 means that the screen is not automatically locked.	Default: not enforce.	By default, this parameter is not configured, which means that the system does not ensure that the screen saver will automatically lock the screen after a period of inactivity. According to Best Practice, it should be set to a maximum of 15 minutes (900s), or less, but not to 0 because it means disabling automatic screen locking.	Medium	(CIS Control v7.1) 16.11 Lock Workstation Sessions After Inactivity Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
4.9	Interactive logon: Number of previous logons to cache (in case domain controller is not available)	<= 4 logon(s)	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/Security Options/	In case the Domain Controller service is interrupted, member servers can still log in.	Default: Windows Server 2008: 25 All Other Versions: 10	The default for Windows Server is 10, except for version 2008 which is 25. This is the login information of domain accounts that is cached on the server, allowing users to continue logging into the server in case of problems connecting to the Domain Controller. The default value is 10, allowing the 10 most recent users with valid login information to continue accessing the system even if authentication to the Domain Controller is unavailable. As for Best Practice, the limit is only 2, however, combined with practical experience, this item should be limited to a maximum of 4 to store information for more administrative accounts, supporting tracing and troubleshooting.	Low	Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
4.10	Interactive logon: Prompt user to change password before expiration	5-14 days	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/Security Options/	Users need to be notified that their password is about to expire, they need to change their password or their account will be locked when the password expires	Default: 5 days.	By default, this parameter is configured to 5 days, that is, 5 days before the password expires. Every time the user logs in, there will be a warning asking to change the password; in case of a long-running logon session, there will be a warning on the day the password expires. If not changed, when the password expires, the user will be automatically locked out of the system. According to Best Practice combined with practical experience, this parameter is at least 5 and is best configured within 5-14 days. Note that if the value is 0, there will be no warning of password expiration.	Low	Microsoft:https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/jj852243(v=ws.11) Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
4.11	Microsoft network client: Digitally sign communications (always)	Enabled	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/Security Options/	Prevent packet spoofing when using communication protocols such as SMB or NetBIOS	Default: Disabled.	The default configuration is Disabled, which means that SMB signing is not required when connecting. This parameter manages whether the client-side SMB component requires SMB signing or not. According to Best Practice, this configuration should be Enabled to prevent MITM attacks, by determining that SMB signing is established between the client and server before the connection is created.	Medium	(CIS Control v7.1) 5.1 Establish Secure Configurations Microsoft:https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/microsoft-network-client-digitally-sign- communications-always

CHECKLIST REVIEW POLICY CONFIGURATION (RSoP)								
STT	**Criteria**	**Request**	**How to check**	**Describe**	**Default configuration**	**Recommendation**	**Severity**	**References**
4.12	Microsoft network client: Digitally sign communications (if server agrees)	Enabled	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/Security Options/	Prevent packet spoofing when using communication protocols such as SMB or NetBIOS	Default: Enabled.	By default, this parameter is Enabled, meaning that if the other device supports it, it will establish an SMB connection with SMB signing, but if the device does not support it, it will still allow the connection to be created. This parameter controls whether the client-side SMB component needs to use the SMB signing feature or not (only used when the server supports it). According to Best Practice, this feature needs to be configured as Enabled. So the default parameter has been configured correctly.	Medium	(CIS Control v7.1) 5.1 Establish Secure Configurations Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
4.13	Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/Security Options/	If this policy is enabled, the server may send passwords in unencrypted form over the network, posing a high risk of password disclosure.	Default: Disabled.	The default configuration is Disabled, which means it does not allow sending plaintext passwords to non-Microsoft SMB servers, only allows sending encrypted passwords. If the non-Microsoft SMB server does not support encryption, the connection will not be created. According to Best Practice, this feature should be configured as Disabled. So the default parameter has been configured correctly.	High	(CIS Control v7.1) 5.1 Establish Secure Configurations Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
4.14	Microsoft network server: Amount of idle time required before suspending session	<= 15 minute(s)	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/Security Options/	With each SMB session consuming server resources, an attacker can open multiple empty sessions to DoS the server.	Default: This policy is not defined, which means that the system treats it as 15 minutes for servers and undefined for workstations.	By default, this parameter is not configured, meaning that for servers, the maximum idle time is 15 minutes before canceling the SMB session, and for workstations, it is not required. As for Best practice, the requirement for this configuration is 15 minutes or less, so the default configuration of this parameter has met the requirements.	Medium	(CIS Control v7.1) 16.11 Lock Workstation Sessions After Inactivity Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
4.15	Microsoft network server: Digitally sign communications (always)	Enabled	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/Security Options/	Prevent packet spoofing when using communication protocols such as SMB or NetBIOS	Default: Disabled for member servers. Enabled for domain controllers.	By default, this parameter is configured as Disabled for stand-alone servers, meaning that SMB signing is not required to create a connection; but for Domain Controllers, it is required. This parameter manages whether the client-side SMB component is required to use the SMB signing feature or not. According to Best Practice, this parameter should be configured as Enabled. Thus, the default parameter for Domain Controllers meets the requirements.	Medium	(CIS Control v7.1) 5.1 Establish Secure Configurations Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
4.16	Microsoft network server: Digitally sign communications (if client agrees)	Enabled	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/Security Options/	Prevent packet spoofing when using communication protocols such as SMB or NetBIOS	Default: Enabled on domain controllers only.	By default, this parameter is configured as Enabled for only Domain Controllers, which requires SMB signing to be set up before creating a connection. This parameter controls whether the client-side SMB component needs to use the SMB signing feature or not (only used when the client supports it). According to Best Practice, this parameter is required to be configured as Enabled. Thus, the default parameter for Domain Controllers meets the requirements.	Medium	(CIS Control v7.1) 5.1 Establish Secure Configurations Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
4.17	Microsoft network server: Disconnect clients when logon hours expire	Enabled	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/Security Options/	This policy is only effective for businesses that limit user login times. If this policy is not enabled, users can keep their sessions even after the allowed time has passed.	Default on Windows Vista and above: Enabled. Default on Windows XP: Disabled	By default, this parameter is configured as Enabled except for Windows XP which is disabled. Enabled means that when the user's logon hours end and the user is still connected, the server will automatically disconnect the session, ensuring that the user can only access resources during the allowed time. According to Best Practice, this parameter should be configured as Enabled. Thus, the default parameter for modern Windows versions meets the requirements.	Low	(CIS Control v7.1) 16.11 Lock Workstation Sessions After Inactivity Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
4.18	Microsoft network server: Server SPN target name validation level	Accept if provided by client or higher	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/Security Options/	Computer identities can be spoofed to gain unauthorized access to network resources.	Default: Off	By default, this parameter is off, meaning that SPn is not required from the client request. SPN is a way to manage the service name, which exists only for a service, and is often used in Kerberos authentication. When the client wants to access the service, it will use SPN to request a service ticket from KDC (Key Distribution Center). If SPN is incorrect or does not exist, the user's authentication process will fail and the service will not be accessible. According to Best Practice, it is necessary to configure "Accept if provided by client" to prevent SMB relay attack, requiring the client to enter the SPN parameter, otherwise the connection will be denied.	Medium	Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
4.19	Network security: Allow Local System to use computer identity for NTLM	Enabled	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/Security Options/	Local System accounts during negotiation for NTLM authentication if using anonymous authentication pose a risk of unauthorized access	By default, this policy is enabled on Windows 7 and above. By default, this policy is disabled on Windows Vista.	By default, modern Windows versions from Windows 7 will enable this feature except for Windows Vista which is disabled. Enabled means it will use computer identity for authentication, ensuring authentication with computer identity, supporting both signing and encryption to ensure data protection.	Medium	Microsoft:https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/network-security-allow-local-system- to-use-computer-identity-for-ntlm
4.20	Network security: Configure encryption types allowed for Kerberos	AES128_HMAC_SHA1 AES256_HMAC_SHA1 Future encryption types	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/Security Options/	Using weak encryption algorithms in Kerberos authentication poses a risk of credential theft, allowing attackers unrestricted access to the system.	Default domain policy Not defined Default domain controller policy Not defined Stand-alone server default settings Not defined	By default, it is not configured, meaning it does not specify the encryption types that Kerberos is allowed to use. According to Best practice, it is necessary to configure to only allow the following encryption types: AES128_HMAC_SHA1 AES256_HMAC_SHA1 Future encryption types	High	(CIS Control v7.1) 14.4 Encrypt All Sensitive Information in Transit (CIS Control v7.1) 18.5 Use Only Standardized and Extensively Reviewed Encryption Algorithms Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
4.21	Network security: Do not store LAN Manager hash value on next password change	Enabled	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/Security Options/	The SAM file can be hacked, allowing an attacker to access the hashed values of the account and password. The attacker can then use tools to crack the password, allowing him to impersonate the user and access network resources. This policy does not completely prevent the attack, it only makes it more complicated to exploit.	Default on Windows Vista and above: Enabled Default on Windows XP: Disabled.	The default on Windows Vista and newer versions is Enabled, except for Windows XP which is Disabled. Enable means that LAN Manager hash will not be used because this is the old hashing method used to store passwords, which is weak and can be cracked. According to Best Practice, this configuration should be Enabled, so the default value of this parameter meets the requirements.	High	(CIS Control v7.1) 16.4 Encrypt or Hash all Authentication Credentials Microsoft: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/network-security-do-not-store-lan-manager-hash-value-on-next-password-change
4.22	Network security: Force logoff when logon hours expire	Enabled	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/Security Options/	If this policy is disabled, users can continue to access their current session on their computer even after the configured working hours have passed.	Default: Enabled.	The default configuration is Enabled, which means the user must be disconnected when the allowed logon time has expired. According to Best practice, this parameter is also required to be configured as Enabled, so by default this parameter is configured correctly.	Medium	(CIS Control v7.1) 16.11 Lock Workstation Sessions After Inactivity Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf

CHECKLIST REVIEW POLICY CONFIGURATION (RSoP)								
STT	**Criteria**	**Request**	**How to check**	**Describe**	**Default configuration**	**Recommendation**	**Severity**	**References**
4.23	Network security: LAN Manager authentication level	Send NTLMv2 response only. Refuse LM & NTLM	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/Security Options/	LM and NTLMv1 contain multiple critical vulnerabilities that attackers can exploit to gain access to the system.	Default: Windows 2000 and windows XP: send LM & NTLM responses Windows Server 2003: Send NTLM response only Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2: Send NTLMv2 response only	By default, the configuration still allows the use of LM and NTLM, which are old protocols and are not secure. According to Best Practice, the configuration "Send NTLMv2 response only. Refuse LM & NTLM" means only allowing the NTLMv2 authentication protocol, refusing the LM and NTLM protocols.	High	(CIS Control v7.1) 18.5 Use Only Standardized and Extensively Reviewed Encryption Algorithms Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
4.24	Network security: LDAP client signing requirements	Negotiate signing or higher	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/Security Options/	This policy is used to prevent man-in-the-middle attacks in the LDAP protocol. If not used, an attacker can forge packets exchanged between a client and an LDAP server, leading to unwanted results.	Default: Negotiate signing.	The default configuration is Negotiate signing, which means that if the TLS/SSL protocol is not used, the client will create an LDAP BIND request to set LDAP data signing. If TLS/SSL is already used, data signing is not required. According to Best Practice, at least the Negotiating requirement needs to be enabled. So by default, this parameter meets the requirements.	Medium	(CIS Control v7.1) 18.5 Use Only Standardized and Extensively Reviewed Encryption Algorithms Microsoft: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/network-security-ldap-client-signing- requirements. requirements
4.25	Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Require NTLMv2 session security Require 128-bit encryption	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/Security Options/	Protection features for RPC	Default: Windows XP, Windows Vista, Windows 2000 Server, Windows Server 2003, and Windows Server 2008: No requirements. Windows 7 and Windows Server 2008 R2: Require 128-bit encryption	The default configuration for older Windows versions is not required or does not require both criteria: using NTLMv2 authentication protocol and 128-bit encryption method. As for Best practice, both of these parameters are required to be configured, ensuring that data between client and server is encrypted, otherwise the connection will fail.	Medium	(CIS Control v7.1) 18.5 Use Only Standardized and Extensively Reviewed Encryption Algorithms Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
4.26	Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require NTLMv2 session security Require 128-bit encryption	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policy/Security Options/	Protection features for RPC	Default: Windows XP, Windows Vista, Windows 2000 Server, Windows Server 2003, and Windows Server 2008: No requirements. Windows 7 and Windows Server 2008 R2: Require 128-bit encryption	The default configuration for older Windows versions is not required or does not require both criteria: using NTLMv2 authentication protocol and 128-bit encryption method. As for Best practice, both of these parameters are required to be configured, ensuring that data between client and server is encrypted, otherwise the connection will fail.	Medium	(CIS Control v7.1) 18.5 Use Only Standardized and Extensively Reviewed Encryption Algorithms Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
5	Windows Defender Firewall with Advanced Security							
5.1	Firewall state	On	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Windows Defender Firewall with Advanced Security/	Maintain default firewall configuration	Default: Domain: on Private: on Public: on	The default firewall status on all profiles is on. Thus, this parameter default meets the requirements.	Medium	(CIS Control v7.1) 9.4 - Apply Host-Based Firewalls or Port-Filtering
5.2	Inbound connections	Block (Default)	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Windows Defender Firewall with Advanced Security/	Maintain default firewall configuration	Default: Domain: Block Private: Block Public: Block	By default, all firewall profiles have an implicit deny rule that blocks all inbound connections. So, by default, this parameter meets the requirements.	Medium	(CIS Control v7.1) 9.4 - Apply Host-Based Firewalls or Port-Filtering
5.3	Log file maximum size (KB)	>= 16,384 KB	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Windows Defender Firewall with Advanced Security/	Maintain default firewall configuration	Default: Domain: 4MB Private: 4MB Public: 4MB	The default firewall log file size for domains is only 4MB, but according to best practice, the total log file size should be configured to 20MB (maximum 32MB).	Medium	(CIS Control v7.1) 6.3 - Enable Detailed Logging Windows:https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/configure-logging?tabs=intune
5.4	Log dropped packets	Yes	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Windows Defender Firewall with Advanced Security/	Maintain default firewall configuration	Default: Domain: No Private: No Public: No	By default, this parameter is configured as No, meaning it does not return invalid packets blocked by the firewall. According to Best Practice, the profiles should be configured as Yes: Domain: Yes Private: Yes Public: Yes	Medium	(CIS Control v7.1) 6.3 - Enable Detailed Logging Windows:https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/configure-logging?tabs=intune
5.5	Log successful connections	Yes	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Windows Defender Firewall with Advanced Security/	Maintain default firewall configuration	Default: Domain: No Private: No Public: No	By default, this parameter is configured as No, meaning it does not record valid packets allowed by the firewall. According to Best Practice, the profiles should be configured as Yes: Domain: Yes Private: Yes Public: Yes (recording successful connections through the firewall. Recording successful connections helps monitor network traffic and detect unusual behavior.)	Medium	(CIS Control v7.1) 6.3 - Enable Detailed Logging Windows:https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/configure-logging?tabs=intune
6	Audit Policy							
6.1	Audit account logon event	Success Failure	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policies/Audit Policy	Logging Logging includes Event IDs: 672-678, 681-683 (Account Logon Events)	Default values on Server editions: Credential Validation: Success Kerberos Service Ticket Operations: Success Other Account Logon Events: No Auditing Kerberos Authentication Service: Success	By default, the parameter is configured to audit only successful user login events (Success) and not audit (No Auditing) login events without password authentication or Kerberos (via AD), currently there is no authentication method in this group. According to Best practice, audit Success and Failure for Credential Validation and 2 Kerberos authentication events are required.	Medium	(CIS Control v7.1) 6.3 - Enable Detailed Logging Stig BenchMark (for AD's own events): https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
6.2	Audit account management	Success and Failure	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policies/Audit Policy	Logging Logging includes Event IDs: 4720, 4723, 4724, 4726-4735, 4737-4764, 4780, 685 (Account management events)	Default values on Server editions: User Account Management: Success Computer Account Management: Success Security Group Management: Success Distribution Group Management: No Auditing Application Group Management: No Auditing Other Account Management Events: No Auditing	By default, the parameter is configured to audit only account management events, including successful account creation, deletion, and change (Success) and not audit (No Auditing) events for Distribution and Application Group or other account management events. According to Best practice, Audit Success for Distribution Group Management, Other Account Management Events, Audit Success and Failure for Application Group Management, User account management are required, while the remaining parameters are defaulted to meet the requirements.	Medium	(CIS Control v7.1) 6.3 - Enable Detailed Logging Stig BenchMark (for AD-specific events):https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
6.3	Audit process tracking	Success	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policies/Audit Policy	Logging Logging includes Event IDs: 592-602 (Process tracking event)	Default: No auditing	The default configuration parameter is No auditing, which means the system will not monitor or record the status of process creation/destruction events, special events such as Handle duplication that allows the shared handle process to access resources illegally or Indirect Object Access that allows indirect access to resources through the rights of another object (inheriting rights from the parent folder) or rights delegated from others. According to Best practice and practical experience, this parameter should be configured as Success.	Medium	(CIS Control v7.1) 6.3 - Enable Detailed Logging Windows:https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protectiouditing/basic-audit-process-tracking

CHECKLIST REVIEW POLICY CONFIGURATION (RSoP)								
STT	**Criteria**	**Request**	**How to check**	**Describe**	**Default configuration**	**Recommendation**	**Severity**	**References**
6.4	Audit Directory Service Access	Success Failure	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policies/Audit Policy	Logs include Event ID: 566 (Directory service access events)	Default values on Server editions: Directory Service Access: Success Directory Service Changes: No Auditing Directory Service Replication: No Auditing Detailed Directory Service Replication: No Auditing	By default, the configuration parameter is only Audit Success Directory Service Access, the rest of the events are not audited (No auditing), meaning the system will not monitor or record events created when an object in Active Directory Domain Services (AD DS) accesses the system. Note that only AD DS objects with matching system access control lists (SACL) (configuration in file/folder -> auditing -> set permissions for auditing such as write, access, read,...) will be recorded in the log. According to Best practice, both Success and Failure are required for some events. This section requires configuring Success and Failure.	Medium	(CIS Control v7.1) 6.3 - Enable Detailed Logging Stig BenchMark (for AD-specific events):https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
6.5	Audit logon events	Success Failure	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policies/Audit Policy	Logs include Event IDs: 4624, 4625, 4634, 4647, 4648, 4779 (Logon events)	Default values on Server editions: Logon: Success, Failure Logoff: Success Account Lockout: Success IPsec Main Mode: No Auditing IPsec Quick Mode: No Auditing IPsec Extended Mode: No Auditing Special Logon: Success Other Logon/Logoff Events: No Auditing Network Policy Server: Success, Failure	By default this parameter has Audit configuration for some events but not all, events related to login and logout, including both success and failure. Auditing these events helps to track and analyze login activities, but according to Best practice the configuration requirement is Success and Failure.	Medium	(CIS Control v7.1) 6.3 - Enable Detailed Logging Stig BenchMark (for AD-specific events):https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
6.6	Audit Policy Change	Success	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policies/Audit Policy	Logs include Event IDs: 608-623, 625, 768-771, 805	Default: Audit Policy Change: Success Authentication Policy Change: Success Authorization Policy Change: No Auditing MPSSVC Rule-Level Policy Change: No Auditing Filtering Platform Policy Change: No Auditing Other Policy Change Events: No Auditing	By default, this parameter configures Audit success for 2 events: Audit Policy Change and Authentication Policy Change, recording successful changes related to security policy configuration, but not for the remaining events. According to Best Practice, Audit success is required for all events, in addition, Success and Failure are required for Audit Policy Change, MPSSVC Rule-Level Policy Change and Other Policy Change Events.	Medium	(CIS Control v7.1) 6.3 - Enable Detailed Logging Stig BenchMark (for AD-specific events):https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
6.7	Audit Privilege Use	Success Failure	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Local Policies/Audit Policy	Logs include Event IDs: 576-578	Default: No auditing.	The default for this parameter is not Audit, which means it does not record events or processes that use privileges to execute, including both success and failure. According to Best Practice, this parameter must be configured as Success and Failure, especially the Audit Sensitive Privilege Use feature must be configured as Audit Success and Failure.	Medium	(CIS Control v7.1) 6.3 - Enable Detailed Logging Stig BenchMark (for AD-specific events):https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf Windows: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protectiouditing/basic-audit-privilege-use
7	MS Security Guide							
7.1	Configure this SMB v1 client Polcy driver requires installing additional custom SecGuide: "SecGuide.admx" and "SecGuide.adml", then copied to \Windows\PolicyDefinitions and \Windows\PolicyDefinitions\en-US respectively. Link:https://www.microsoft.com/en-us/download/details.aspx?id=55319	Enabled: Disable driver	Check the path: Computer Configuration/Policies/Administrative Templates/MS Security Guide If the path does not exist, do not evaluate, the reason is that the server has not configured additional Microsoft Policy Definitions.	SMBv1 is an outdated protocol that uses the MD5 algorithm, which has many vulnerabilities.	Default: * "Manual start" for Windows 7 and Windows Servers 2008, 2008R2, and 2012; * "Automatic start" for Windows 8.1 and Windows Server 2012R2 and newer.	By default, this SMBv1 protocol will automatically start for new Windows server versions, but for Best practice, it is required to disable the driver and not load this protocol.	High	(CIS Control v7.1) 9.2 Ensure Only Approved Ports, Protocols and Services Are Running Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
7.2	Configuring this SMB v1 Polcy server requires installing additional custom SecGuide: "SecGuide.admx" and "SecGuide.adml", then copied to \Windows\PolicyDefinitions and \Windows\PolicyDefinitions\en-US respectively. Link:https://www.microsoft.com/en-us/download/details.aspx?id=55319	Disabled	Check the path: Computer Configuration/Policies/Administrative Templates/MS Security Guide If the path does not exist, do not evaluate, the reason is that the server has not configured additional Microsoft Policy Definitions.	SMBv1 is an outdated protocol that uses the MD5 algorithm, which has many vulnerabilities.	Default: Enabling this setting enables server-side processing of the SMBv1 protocol.	Disabling this setting disables server-side processing of the SMBv1 protocol. (Recommended.) Enabling this setting enables server-side processing of the SMBv1 protocol. (Default.)	High	(CIS Control v7.1) 9.2 Ensure Only Approved Ports, Protocols and Services Are Running Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
7.3	This WDigest Authentication Polcy requires installing additional custom SecGuide: "SecGuide.admx" and "SecGuide.adml", then copied to \Windows\PolicyDefinitions and \Windows\PolicyDefinitions\en-US respectively. Link:https://www.microsoft.com/en-us/download/details.aspx?id=55319	Disabled	Check the path: Computer Configuration/Policies/Administrative Templates/MS Security Guide If the path does not exist, do not evaluate, the reason is that the server has not configured additional Microsoft Policy Definitions.	Preventing account information from being stored in unencrypted form in RAM can reduce the likelihood of account theft.	When WDigest authentication is enabled, Lsass.exe retains a copy of the user's plaintext password in memory, where it can be at risk of theft. Microsoft recommends disabling WDigest authentication unless it is needed. If this setting is not configured, WDigest authentication is disabled in Windows 8.1 and in Windows Server 2012 R2; it is enabled by default in earlier versions of Windows and Windows Server. Update KB2871997 must first be installed to disable WDigest authentication using this setting in Windows 7, Windows 8, Windows Server 2008 R2 and Windows Server 2012. Enabled: Enables WDigest authentication. Disabled (recommended): Disables WDigest authentication. For this setting to work on Windows 7, Windows 8, Windows Server 2008 R2 or Windows Server 2012, KB2871997 must first be installed.	When WDigest authentication is enabled, Lsass.exe retains a copy of the user's plaintext password in memory, where it can be at risk of theft. Microsoft recommends disabling WDigest authentication unless it is needed. If this setting is not configured, WDigest authentication is disabled in Windows 8.1 and in Windows Server 2012 R2; it is enabled by default in earlier versions of Windows and Windows Server. Update KB2871997 must first be installed to disable WDigest authentication using this setting in Windows 7, Windows 8, Windows Server 2008 R2 and Windows Server 2012. Enabled: Enables WDigest authentication. Disabled (recommended): Disables WDigest authentication. For this setting to work on Windows 7, Windows 8, Windows Server 2008 R2 or Windows Server 2012, KB2871997 must first be installed.	Medium	(CIS Control v7.1) 16.4 Encrypt or Hash all Authentication Credentials
8	Network Provider							
8.1	Hardened UNC Paths - NETLOGON, SYSVOL	"Require Mutual Authentication" "Require Integrity"	Check the path: Computer Configuration/Policies/Administrative Templates/Network/Network Provider	Additional security requirements are applied to UNC paths specified in hard UNC paths before allowing access to them. This assists in preventing spoofing or tampering of connections to these paths.	Default: Not configured This means that by default this parameter isDisabled,No UNC paths are hardened. Stig Benchmark page 618:https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf	According to Best practice, it is necessary to configure 2 parameters RequireMutualAuthentication=1, RequireIntegrity=1 for 2 UNC PATH *\SYSVOL, *\NETLOGON. Select Enabled. In the Options section, click Show and add: *\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1 *\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1 Click OK, then Apply and OK. Update Group Policy: On Domain Controllers, run gpupdate /force to apply the new policy.	Medium	Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
9	Credentials Delegation							

CHECKLIST REVIEW POLICY CONFIGURATION (RSoP)								
STT	**Criteria**	**Request**	**How to check**	**Describe**	**Default configuration**	**Recommendation**	**Severity**	**References**
9.1	Encryption Oracle Remediation	Enabled: Force Updated Clients	Check the path: Computer Configuration/Policies/Administrative Templates/System/Credentials Delegation	Mitigation of Oracle's CredSSP cryptographic vulnerability (CVE-2018-0886). This vulnerability allows an attacker, if successfully exploited, to execute remote code.	Default: Not configured This means the default parameter is: 1. If the security update 5/2018 has not been applied, this parameter isEnabled: VulnerableThis means that the client application can switch back to using an insecure version of CredSSP, and the services supporting CredSSP can still accept clients that have not been updated. 2. If the 5/2018 security update has been applied, this parameter isEnabled: MitigatedThat is, it does not allow clients to switch back to an insecure version, but the service still accepts clients that have not been updated.	According to Best practice, the configuration requirement is Force Updated Clients The Force Updated Clients option requires client applications to be updated to the required CredSSP version before they can access the service.	High	(CIS Control v7.1) 3.4 Deploy Automated Operating System Patch Management Tools Stig BenchMark (for AD-specific events):https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
10	Windows Defender							
10.1	Turn off Windows Defender	Disabled	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Windows Defender	If this policy is enabled, Microsoft Defender Antivirus (MDA) will be disabled. Configure this policy to disable to ensure MDA always works.	Default: Not configured/Disable	According to Best practice, similar configuration is required so by default the parameters are configured as required.	Medium	(CIS Control v7.1) 8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies
10.2	Turn off real-time protection	Disabled	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Windows Defender/Real-time protection	Enable real-time protection	Default: Not configured/Disable	According to Best practice, similar configuration is required so by default the parameters are configured as required.	Medium	(CIS Control v7.1) 8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies
10.3	Turn on behavior monitoring	Enabled	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Windows Defender/Real-time protection	Enable behavior tracking, analyze to warn or block malicious software and behavior	Default: Not configured/Enable	According to Best practice, similar configuration is required so by default the parameters are configured as required.	Medium	(CIS Control v7.1) 8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies
10.4	Scan all downloaded files and attachments	Enabled	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Windows Defender/Real-time protection	Trigger scanning as soon as files are downloaded or attached (by email) to ensure system safety	Default: Not configured/Enable	According to Best practice, similar configuration is required so by default the parameters are configured as required.	Medium	(CIS Control v7.1) 8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies
10.5	Turn on process scanning whenever real-time protection is enabled	Enabled	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Windows Defender/Real-time protection	Enable process scanning when real-time protection is enabled	Default: Not configured/Enable	According to Best practice, similar configuration is required so by default the parameters are configured as required.	Medium	(CIS Control v7.1) 8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies
10.6	Monitor file and program activity on your computer	Enabled	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Windows Defender/Real-time protection	Enable monitoring of file and program activity running on the system	Default: Not configured/Enable	According to Best practice, similar configuration is required so by default the parameters are configured as required.	Medium	(CIS Control v7.1) 8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies
10.7	Scan archive files	Enabled	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Windows Defender/Scan	Enable scanning of compressed files to ensure system safety	Default: Not configured/Enable	According to Best practice, similar configuration is required so by default the parameters are configured as required.	Medium	(CIS Control v7.1) 8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies
10.8	Scan packed executables	Enabled	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Windows Defender/Scan	Enable scanning of launch files to ensure system safety	Default: Not configured/Enable	According to Best practice, similar configuration is required so by default the parameters are configured as required.	Medium	(CIS Control v7.1) 8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies
10.9	Scan removable drives	Enabled	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Windows Defender/Scan	Enable scanning of removable storage drives such as USB, portable hard drives, etc. to ensure system safety.	Default: Not configured/Disable	According to Best practice, it is also required to configure Enabled to ensure scanning of removable drives, ensuring system safety.	Medium	(CIS Control v7.1) 8.4 Configure Anti-Malware Scanning of Removable Media
11	Remote Desktop Services							
11.1	Restrict Remote Desktop Services users to a single Remote Desktop Services session	Enabled	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Remote Desktop Services/Remote Desktop Session Host/Connections	The access administrator will only use a single session, avoiding creating multiple sessions that affect server performance.	Default: Not configured / Enabled	According to Best practice, this parameter is also required to be Enabled to limit each user to only be able to connect to a single Remote Desktop session on a server, so by default the parameter is configured as required.	Medium	(CIS Control 7.1) 9.2 Ensure Only Approved Ports, Protocols and Services Are Running Stig Benchmark page 886: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
11.2	Do not allow Clipboard redirection	Enabled	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Remote Desktop Services/Remote Desktop Session Host/Device and Resource Redirection	Block copy/paste feature via Remote Desktop	Default: Not configured/ Disabled	According to Best practice, this parameter is also required to be Enabled to prevent users from copying data on Remote Desktop Server to their personal computers.	Medium	(CIS Control 7.1) 13.3 Monitor and Block Unauthorized Network Traffic Microsoft: https://learn.microsoft.com/en-us/azure/virtual-desktop/redirection-configure-clipboard?tabs=intune&pivots=azure-virtual-desktop
11.3	Do not allow drive redirection	Enabled	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Remote Desktop Services/Remote Desktop Session Host/Device and Resource Redirection	Block navigation of storage devices via Remote Desktop	Default: Not configured/ Disabled	According to Best practice, this parameter is also required to be Enabled to prevent users from sharing local drives from their personal computers to the Remote Desktop Server.	Medium	(CIS Control 7.1) 13.3 Monitor and Block Unauthorized Network Traffic Microsoft: https://learn.microsoft.com/en-us/azure/virtual-desktop/redirection-configure-drives-storage?tabs=intune&pivots=azure-virtual-desktop
11.4	Set client connection encryption level	High Level	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Remote Desktop Services/Remote Desktop Session Host/Security	Ensure connections from clients use strong encryption algorithms, preventing MITM attacks, attackers can decrypt if using weak encryption algorithms	Default: Not configured/High Level By default this parameter is configured as High level, which requires all communication between the client and the RD server to use RDP encryption with 128-bit strength	According to Best practice, this parameter is also required to be configured as High Level to ensure that RD services traffic will not be decrypted, so by default this parameter meets the requirements.	Medium	(CIS Control 7.1) 14.4 Encrypt All Sensitive Information in Transit Stig Benchmark page 906:https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf

CHECKLIST REVIEW POLICY CONFIGURATION (RSoP)								
STT	**Criteria**	**Request**	**How to check**	**Describe**	**Default configuration**	**Recommendation**	**Severity**	**References**
11.5	Always prompt for password upon connection	Enabled	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Remote Desktop Services/Remote Desktop Session Host/Security	Ensure users always enter credentials when making RDP connections	Default: Not configured/ Disabled. The default of this parameter is Disabled, which means that users who have saved their login information on the RDP client will not have to re-enter their password every time they create an RDP connection, which is risky when there is a possibility that an attacker can physically access the victim's computer.	As per Best practice, this parameter should also be configured as Enable to ensure that a password will always be required every time a user creates an RDP session.	Medium	(CIS Control 7.1) 14.4 Encrypt All Sensitive Information in Transit Stig Benchmark page 898:https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
11.6	Require secure RPC communication	Enabled	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Remote Desktop Services/Remote Desktop Session Host/Security	RPC is used to manage and configure Remote Desktop Services, it is recommended to use secure connections for this protocol.	Default: Not configured/Disabled By default this parameter is Disabled which means that RD services will always request security for all traffic but will still allow clients that do not respond to this request, do not support,...	According to Best practice, this parameter is also required to be configured as Enable to ensure the security of RPC connections.	Medium	(CIS Control 7.1) 14.4 Encrypt All Sensitive Information in Transit Stig Benchmark page 900:https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
11.7	Require use of specific security layer for remote (RDP) connections	SSL	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Remote Desktop Services/Remote Desktop Session Host/Security	Native Remote Desktop Services encryption is currently considered weak, so enforcing the use of stronger Transport Layer Security (TLS) encryption for all RDP communications between clients and RD Session Server servers is preferred.	Default: Not configured /Negotiate By default this parameter is Negotiate which means that the most secure authentication method supported by the client will be used. If TLS is supported, it will be used to authenticate with the RDP server, otherwise RDP's own encryption method will be used.	According to Best practice, this parameter is also required to be configured as Enabled => Select SSL in the security layer section to ensure that the Remote Desktop connection uses a specific security layer, SSL (Secure Sockets Layer).	Medium	(CIS Control 7.1) 14.4 Encrypt All Sensitive Information in Transit Stig Benchmark page 902:https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
11.8	Require user authentication for remote connections by using Network Level Authentication	Enabled	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Remote Desktop Services/Remote Desktop Session Host/Security	Requiring user authentication before remote connections enhances security.	Default: Enabled / High Level. The default parameter is Enabled: High Level, meaning that Remote Desktop connections between the client and the server must use 128-bit encryption. If the client does not support it, it will not be possible to create a Remote Desktop Server connection session.	As per Best practice, this parameter is also required to be configured as Enabled to ensure that users must authenticate before creating an RDP session.	Medium	Available in CIS Control v8 Stig Benchmark page 905:https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
11.9	Set time limit for disconnected sessions	Enabled: 1 minute	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Remote Desktop Services/Remote Desktop Session Host/Session Time Limits	The server will delete disconnected sessions after the specified configured time.	Default: Not configured/Disabled By default, this parameter is Disabled, meaning that disconnected Remote Desktop sessions will still be maintained on the server indefinitely. Existing unused old sessions can cause unnecessary use of system resources, or the inability to create new connection sessions in case the system limits the number of simultaneous access sessions, causing a Denial Of Services (DoS) situation.	According to Best practice, this parameter is also required to be configured as Enabled => Select 1 minute in the End a disconnected session section (set a time limit for disconnected Remote Desktop sessions. After the specified time, the disconnected session will automatically end)	Medium	(CIS Control 7.1) 16.11 Lock Workstation Sessions After Inactivity Stig Benchmark page 909:https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
11.10.	Set time limit for active but idle Remote Desktop Services sessions	<= 15 minute(s) (>0)	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Remote Desktop Services/Remote Desktop Session Host/Session Time Limits	Disconnect unused login sessions that exceed the specified time	Default: Not configured /Disabled By default this parameter is Disabled, meaning Remote Desktop Services will never timeout users, and inactive sessions will never timeout.	According to Best practice, this parameter is also required to be configured as Enabled => Select 15 minutes in the Idle session limit section (set the time limit for Remote Desktop sessions that are active but have no user activity. After the specified time, the session will be automatically disconnected)	Medium	(CIS Control 7.1) 16.11 Lock Workstation Sessions After Inactivity Stig Benchmark page 908:https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
11.11	Do not delete temp folders upon exit	Disabled	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Remote Desktop Services/Remote Desktop Session Host/Temporary folders	Delete data in Temp folder to avoid data leakage	Default: Not configured/Disabled By default, this parameter is Disabled, which means that users' temporary folders will not be saved after the RDP session ends. If not deleted, there is a possibility that sensitive information will be saved on the system and the administrator can read this information.	As per Best practice, it is also required to configure this parameter as Disabled to ensure temporary folders are deleted when the Remote Desktop session ends.	Medium	Stig Benchmark page 911:https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
11.12	Do not use temporary folders per session	Disabled	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Remote Desktop Services/Remote Desktop Session Host/Temporary folders	Block the use of temporary folders during sessions to avoid data leakage	Default: Not configured/Disabled By default, this parameter is Disabled, meaning that each connection session will create a separate temp folder, ensuring that each session's data is separate, reducing the risk that cached sensitive information can be shared between sessions, and limiting sensitive information to separate user sessions.	According to Best practice, it is also required to configure this parameter as Disabled to ensure that temporary folders will be used separately for each session, helping to better manage system resources)	Medium	Stig Benchmark page 913:https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
12	Windows PowerShell							
12.1	Turn on PowerShell Script Block Logging	Enabled	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Windows Powershell	Configure logging of script blocks executed on Powershell and its output on console	Default: Not configured/Enabled Enabled. (PowerShell will log script blocks the first time they are used.) The way PowerShell Script Block Logging works is that by default it will only save suspicious logs, and suspicious logs will be saved even if the script block has been run. However, other scripts, such as running normal commands, will not be saved. If you enable this configuration, it will ensure that 100% of the logs will be saved for all users.	According to Best practice, this feature is also required to be Enabled, so by default this parameter meets the requirements.	Medium	(CIS Control 7.1) 8.8 Enable Command-line Audit Logging Stig Benchmark page 951:https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
12.2	Turn on PowerShell Transcription	Disabled	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Windows Powershell	If this setting is enabled, there is a risk that passwords may be stored unencrypted in the PowerShell_transcript file.	Default: Not configured/Disabled By default, this parameter is Disabled, which means that the input/output of commands and results in Powershell will not be saved as text. This limits the possibility that sensitive user/password information can be saved in the Powershell output transcript file.	According to Best practice, this feature is also required to be Disabled, so by default this parameter is required.	High	Stig Benchmark page 953:https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf

CHECKLIST REVIEW POLICY CONFIGURATION (RSoP)								
STT	**Criteria**	**Request**	**How to check**	**Describe**	**Default configuration**	**Recommendation**	**Severity**	**References**
12.3	Turn on Script Execution	Enabled: Allow only signed scripts or higher	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Windows Powershell	Settings that prevent the launch of unknown scripts that may be harmful to the system	Default: Not configured /disable By default this parameter is Disabled, meaning there is no limit to the type of scripts that can be executed.	According to Best practice, Enabled => Select Allow only signed scripts in Execution Policy to ensure that only authenticated scripts are allowed to execute, helping to enhance security by preventing untrusted or malicious scripts from running on the system.	Medium	(CIS Control 7.1) 2.9 Implement ApplicationWhitelisting of Scripts Cis Windows 2022: https://www.calcomsoftware.com/cis-benchmark-for-windows-server-2022/
13	WinRM							
13.1	Allow Basic authentication	Disabled	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Windows Remote Management (WinRM)/WinRM Client	Basic authentication is a weak authentication method that uses authentication by transmitting authentication information (including passwords) in unencrypted form over the network. Attackers can perform packet capture and extract login information for malicious purposes.	Default: Not configured / Disabled. (The WinRM client does not use Basic authentication.)	According to Best practice, this feature is also required to be Disabled, so by default this parameter is required.	High	(CIS Control 7.1) 9.2 Ensure Only Approved Ports, Protocols and Services Are Running Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
13.2	Allow unencrypted traffic	Disabled	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Windows Remote Management (WinRM)/WinRM Client	WinRM network traffic encryption reduces the risk of attackers viewing or modifying WinRM messages as they travel through the network.	Default: Not configured Disabled. (The WinRM client sends or receives only encrypted messages over the network.)	According to Best practice, this feature is also required to be Disabled, so by default this parameter is required.	High	(CIS Control 7.1) 14.4 Encrypt All Sensitive Information in Transit Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
13.3	Disallow Digest authentication	Enabled	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Windows Remote Management (WinRM)/WinRM Client	Digest authentication is a weak authentication method. Attackers can perform packet capture and extract login information for malicious purposes.	Default: Not configured Disabled. (The WinRM client will use Digest authentication.)	Change to Enabled (prevents the use of Digest authentication via WinRM. Digest authentication can provide a higher level of security than Basic authentication, but may not provide enough protection if not configured properly. By disabling Digest authentication, you can reduce security risks)	High	(CIS Control 7.1) 9.2 Ensure Only Approved Ports, Protocols and Services Are Running Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
13.4	Allow Basic authentication	Disabled	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Windows Remote Management (WinRM)/WinRM Service	Basic authentication is a weak authentication method that uses authentication by transmitting authentication information (including passwords) in unencrypted form over the network. Attackers can perform packet capture and extract login information for malicious purposes.	Default: Not configured / Disabled. (The WinRM service will not accept Basic authentication from a remote client.)	Change to Disabled (Same as 13.1)	High	(CIS Control 7.1) 9.2 Ensure Only Approved Ports, Protocols and Services Are Running Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
13.5	Allow unencrypted traffic	Disabled	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Windows Remote Management (WinRM)/WinRM Service	WinRM network traffic encryption reduces the risk of attackers viewing or modifying WinRM messages as they travel through the network.	Default: Not configured / Disabled. (The WinRM client sends or receives only encrypted messages over the network.)	Change to Disabled (Same as 13.2)	High	(CIS Control 7.1) 14.4 Encrypt All Sensitive Information in Transit Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
13.6	Disallow WinRM from storing RunAs credentials	Enabled	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Windows Remote Management (WinRM)/WinRM Service	Storing RunAs credentials is a convenient feature, however it increases the risk of account compromise.	Default: Not configured / Disabled. (The WinRM service will allow the RunAsUser and RunAsPassword configuration values to be set for plug-ins and the RunAsPassword value will be stored securely.)	Change to Enabled (prevents WinRM from storing credentials when using the RunAs function. This helps protect credentials from being leaked or accessed by unauthorized parties)	Medium	(CIS Control 7.1) 14.3 Disable Workstation to Workstation Communication Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
13.7	Allow remote server management through WinRM	Disabled	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Windows Remote Management (WinRM)/WinRM Service	Any feature is a potential attack vector, features that allow inbound network connections are especially risky. Only allow use of the Windows Remote Management (WinRM) service on trusted networks	Default: Not configured Disabled. (The WinRM service will not respond to requests from a remote computer, regardless of whether or not any WinRM listeners are configured.)	Change to Disabled (controls whether remote server management via WinRM is allowed. By disabling this option, you can prevent remote management, minimizing security risks from untrusted connections)	Medium	(CIS Control 7.1) 9.2 Ensure Only Approved Ports, Protocols and Services Are Running Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
14	Windows Remote Shell							
14.1	Allow Remote Shell Access	Disabled	Check the path: Computer Configuration/Policies/Administrative Templates/Windows Components/Windows Remote Shell	Any feature is a potential attack vector, features that allow inbound network connections are especially risky. Only allow Windows Remote Shell on trusted networks	Default: Not configured / Enabled. (New Remote Shell connections are allowed.)	Change to Disabled (manages whether Remote Shell (remote command) access is allowed via Windows Remote Management (WinRM). When disabled, users cannot use Remote Shell to execute remote commands on the computer. This helps prevent potential security threats from remote shell access, protecting the system from malicious or unwanted commands.)	Medium	(CIS Control 7.1) 9.2 Ensure Only Approved Ports, Protocols and Services Are Running Stig Benchmark: https://www.itsecure.hu/wp-content/uploads/2023/12/CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.0.0.pdf
15	System Services							
15.1	Print Spooler (Spooler)	Disabled	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/System Services	Mitigating Remote Attacks against PrintNightmare Vulnerability (CVE-2021-34527) and Other Remote Print Spooler Attacks	Default: Not configured Not configured will prevent Print Spooler from accepting connections from clients. However, sharing a printer or opening a print queue will automatically trigger Print Spooler to accept connections from clients without configuring this policy.	Go to Computer Configuration/Policies/Windows Settings/Security Settings/System Services. Select Print Spooler, in Print Spooler Properties click Define this policy setting. In Select service startup mode select Disabled (manages print requests and processes print jobs when you send documents to the printer. When this policy is set to Disabled, the Print Spooler service will be disabled, preventing print requests and helping to reduce the security risks associated with Print Spooler vulnerabilities, such as the "PrintNightmare" vulnerability. Disabling this service may be necessary in environments with high security requirements or when no printers are used on the system)	Medium	(CIS Control 7.1) 9.2 Ensure Only Approved Ports, Protocols and Services Are Running Cis: CIS Microsoft Windows Server 2022 STIG v1.0.0 L2 MS
16	Group Policy							

CHECKLIST REVIEW POLICY CONFIGURATION (RSoP)								
STT	**Criteria**	**Request**	**How to check**	**Describe**	**Default configuration**	**Recommendation**	**Severity**	**References**
16.1	Turn off local group policy processing	Enabled	Check the path: Computer Configuration/Policies/Windows Settings/Security Settings/Administrattive Templates/System/Group Policy	Prevent the use of Local group policy, policies must be handled according to Group policy managed on the Domain Controller	Default: Not configured /enable Group Policy Objects (GPO) are processed in the following order: The local GPO is applied. GPOs linked to sites are applied. GPOs linked to domains are applied. GPOs linked to organizational units are applied. For nested organizational units (OUs), GPOs linked to parent organizational units are applied before GPOs linked to child organizational units are applied.	Change to Enabled (prevents processing and application of local group policies on the computer. This means that settings from locally configured Group Policy Objects (GPOs) will not be applied, and only policies from Active Directory or other sources will be used)	Medium	(CIS Control v7.1) 5.4 Deploy System Configuration Management Tools Microsoft: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-processing
17	AD User Account							
17.1	Password configuration	Accounts in active state must have passwords configured.	How to check: - Access Powershell - Enter command: Get-ADUser -Filter * -Properties Passwordnotrequired |FT Name, Passwordnotrequired, Enabled	If an account in the domain does not require a password, it is a serious vulnerability. Attackers can exploit it to penetrate the system. The test command can be run by any account in the system.		##Require password setting for accounts that do not require passwords: Method 1: Access Active Directory Users and Computers and go to the Users folder, right-click on the USER$ account, select Reset Password, change the new password -> OK Method 2: Configure account requirements for users. Use PowerShell to run the command: > Set-ADUser -Identity 'USER$' -PasswordNotRequired $false ##Accounts that do not have expired passwords: Access Active Directory Users and Computers and go to the Users folder, select the BVSCHCM$ account, select Account, in the Account options section, uncheck Password never expires -> Apply -> OK	High	(CIS Control v7.1) 4.4 Use Unique Passwords
17.2	Check for unused accounts	Accounts with last login time >= 45 days must be disabled	How to check: - Access Powershell - Enter command: Get-ADUser -Filter * -Properties LastLogonTimestamp | FT Name, LastLogonTimestamp, Enabled	Unused accounts are vulnerable to attacks due to not changing passwords periodically, and having incorrect permission configurations can be exploited to attack and gain unauthorized access to the system.		##For accounts that do not have LastLogonTimestamp information, exclude accounts that use Non-Interactive Logon Types such as Service Accounts or accounts that run Schedule Tasks. For accounts that have been created but have never been logged in, consider disabling or deleting those redundant accounts from the system. ##For accounts that have not been used in the last 45 days, consider disabling or deleting those accounts from the system.	Medium	(CIS Control v7.1) 16.9 Disable Dormant Accounts
17.3	Check accounts for passwords that have not been changed periodically	No active accounts with last password change >= 365 days	How to check: - Access Powershell - Enter command: Get-ADUser -Filter * -Properties pwdLastSet | FT Name, pwdLastSet, Enabled Alt: Get-ADUser -Filter {Enabled -eq $true} -Properties pwdLastSet \| Select-Object Name, @{Name='pwdLastSetReadable'; Expression={[datetime]::FromFileTime ($_.pwdLastSet).ToString ('dd/MM/yyyy')}}	Passwords that are not changed periodically are at high risk of being hacked/guessed, allowing attackers to take over your account.		##For accounts that do not have information in the PasswordLastSet field, the user must be asked to log in and change the password immediately. In case the account is no longer in use, consider disabling or deleting the redundant accounts from the system. ##For accounts that have not had their passwords changed in the last 365 days, the password must be changed immediately. #Access Active Directory Users and Computers and go to the Users folder, select the user account that needs to change the password, select Account, in the Account options section, select User must change password at nextlogon -> Apply -> OK	Medium	(CIS Control v7.1) 16.10 Ensure All Accounts Have An Expiration Date
17.4	Check the accounts used for the service	Do not use privileged accounts for services	How to check: - Access Powershell - Enter command: Get-ADUser -Filter "AdminCount -eq 1" -Properties servicePrincipalName | FT Name, servicePrincipalName, Enabled	Using a privileged account for a service poses a risk that an attacker could crack the service account password, thereby gaining unauthorized access to the system with the privileged account.		##It is necessary to create a separate service account with appropriate permissions because using a domain admin account to run a service is a serious risk. If exploited, the attacker will have access to the entire domain.	High	(CIS Control v7.1) 4.3 Ensure the Use of Dedicated Administrative Accounts
17.5	Change krbtgt account password	<= 180 days	How to check: - Access Powershell - Enter command: Get-ADUser krbtgt -Property PasswordLastSet	##krbtgt is a system default account, always inactive. This account is used to identify the TGS key in Kerberos authentication. Change the krbtgt password periodically to prevent/mitigate fake ticket attacks (Silver/Golden ticket attacks). ##Changing the password of this account needs to be done twice in a row to ensure that old sessions expire.		##The krbtgt account needs to change its password twice, each time about 10 hours apart to ensure that the old tickers have expired. Change the password twice to ensure that no ticket can use the old password for authentication.	Medium	(CIS Control v7.1) 16.10 Ensure All Accounts Have An Expiration Date
17.6	Configure NTFS permission of AdminSDHolder folder	No strange accounts configured	How to check: - Access Active Directory Users and Computers - Select View > Enabled Advanced Feature - Right click on System > AdminSDHolder select Properties - Check the configuration in the Security tab	AdminSDHolder is used as a template for privileged accounts in privileged groups. Privileged accounts that deviate from this template are updated every 60 minutes via the SDProp process. An attacker can exploit this feature to maintain malicious privileged accounts on the system by adding them to the NTFS permission configuration of this OU.		##Make sure NTFS permission of AdminSDHolder folder is only for default Users, do not configure other users.	Medium	(CIS Control v7.1) 4.1 Maintain Inventory of Administrative Accounts