10.200.1.107 GT-4Q22

Microsoft Windows 10 22H2

88.99 Compliant

1 Scanned Policies with 336 Rules

299 of 336 Rules Passed

CIS Microsoft Windows 10 Enterprise Release 20H2 Level One (L1) - Corporate/Enterprise Environment (general use) v1.10.1	299 Rules Passed	37 Rules Failed
Failed Rules		Compliance increase if remediated
1.1.2. (L1) Ensure 'Maximum password age' is set to '60 or fewer days, but not 0'		0.00 %

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637751: FAIL

Based on the following 1 results:

1.
   1. At least one specified Password Policy entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
FAIL
max_passwd_age: 31536000

2. oval-org.cisecurity.benchmarks.windows_10-def-1637752: PASS

Based on the following 1 results:

1.
   1. At least one specified Password Policy entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
max_passwd_age: 31536000

Remediation Steps

To establish the recommended configuration via GP, set the following UI path to 60 or fewer days, but not 0 : Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age Impact: If the Maximum password age setting is too low, users are required to change their passwords very often. Such a configuration can reduce security in the organization, because users might write their passwords in an insecure location or lose them. If the value for this policy setting is too high, the level of security within an organization is reduced because it allows potential attackers more time in which to discover user passwords or to use compromised accounts.

2.2.16. (L1) Ensure 'Deny access to this computer from the network' to include 'Guests, Local account'	0.00 %

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637788: FAIL

Based on the following 2 results:

1.
   1. At least one specified User Right entry must match the given criteria.

At least one evaluation must pass.
Entry 1 findings:
PASS
userright: SE_DENY_NETWORK_LOGON_NAME
trustee_sid: S-1-5-32-546

2.
1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
FAIL
userright: SE_DENY_NETWORK_LOGON_NAME
trustee_sid: S-1-5-32-546

Remediation Steps

To establish the recommended configuration via GP, set the following UI path to include Guests, Local account : Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny access to this computer from the network Impact: If you configure the Deny access to this computer from the network user right for other groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should verify that delegated tasks will not be negatively affected.

2.2.20. (L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account' 0.00 %

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637796: FAIL

Based on the following 2 results:

1.
1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
userright: SE_DENY_REMOTE_INTERACTIVE_LOGON_NAME
trustee_sid: S-1-5-32-546

2.
1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
FAIL
userright: SE_DENY_REMOTE_INTERACTIVE_LOGON_NAME
trustee_sid: S-1-5-32-546

Remediation Steps

To establish the recommended configuration via GP, set the following UI path to include Guests, Local account : Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on through Remote Desktop Services Impact: If you assign the Deny log on through Remote Desktop Services user right to other groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. Accounts that have this user right will be unable to connect to the computer through either Remote Desktop Services or Remote Assistance. You should confirm that delegated tasks will not be negatively impacted.

2.3.4.1. (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators and Interactive Users' 0.00 %

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637875: FAIL

Based on the following 1 results:

1.

1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: Software\Microsoft\Windows NT\CurrentVersion\Winlogon
name: AllocateDASD

Remediation Steps

To establish the recommended configuration via GP, set the following UI path to Administrators and Interactive Users : Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Allowed to format and eject removable media Impact: None - the default value is Administrators only. Administrators and Interactive Users will be able to format and eject removable NTFS media.

2.3.10.1. (L1) Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' 0.00 %

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638000: FAIL

Based on the following 1 results:

1.

1. At least one specified WMI Status entry must match the given criteria. At least one evaluation must pass.
The specified WMI Status entry was not found based on the given criteria:
namespace: root\rsop\computer
wql: SELECT Setting FROM RSOP_SecuritySettingBoolean WHERE KeyName='LSAAnonymousNameLookup' AND Precedence=1

Remediation Steps

To establish the recommended configuration via GP, set the following UI path to Disabled : Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Allow anonymous SID/Name translation Impact: None - this is the default behavior.

9.1.1. (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' 0.00 %

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637803: FAIL

Based on the following 1 results:

1.

1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\WindowsFirewall\DomainProfile
name: EnableFirewall

Remediation Steps

To establish the recommended configuration via GP, set the following UI path to On (recommended) : Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Firewall state Impact: None - this is the default behavior.

9.1.2. (L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' 0.00 %

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637808: FAIL

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\WindowsFirewall\DomainProfile
name: DefaultInboundAction

Remediation Steps

To establish the recommended configuration via GP, set the following UI path to Block (default) : Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Inbound connections Impact: None - this is the default behavior.

9.1.3. (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' 0.00 %

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637811: FAIL

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\WindowsFirewall\DomainProfile
name: DefaultOutboundAction

Remediation Steps

To establish the recommended configuration via GP, set the following UI path to Allow (default) : Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Outbound connections Impact: None - this is the default behavior.

9.1.4. (L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' 0.00 %

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637815: FAIL

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE

key: Software\Policies\Microsoft\WindowsFirewall\DomainProfile
name: DisableNotifications

Remediation Steps: To establish the recommended configuration via GP, set the following UI path to No : Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Settings Customize\Display a notification Impact: Windows Firewall will not display a notification when a program is blocked from receiving inbound connections.

9.1.5. (L1) Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\domainfw.log' 0.00 %

Proof: This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637819: FAIL

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging
name: LogFilePath

Remediation Steps: To establish the recommended configuration via GP, set the following UI path to %SystemRoot%\System32\logfiles\firewall\domainfw.log : Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Name Impact: The log file will be stored in the specified file.

9.1.6. (L1) Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater' 0.00 %

Proof: This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637822: FAIL

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging
name: LogFileSize

Remediation Steps: To establish the recommended configuration via GP, set the following UI path to 16,384 KB or greater : Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Size limit (KB) Impact: The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

9.1.7. (L1) Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes' 0.00 %

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637826: FAIL

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging
name: LogDroppedPackets

Remediation Steps To establish the recommended configuration via GP, set the following UI path to Yes : Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Log dropped packets Impact: Information about dropped packets will be recorded in the firewall log file.

9.1.8. (L1) Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' 0.00 %

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637829: FAIL

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging
name: LogSuccessfulConnections

Remediation Steps To establish the recommended configuration via GP, set the following UI path to Yes : Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Log successful connections Impact: Information about successful connections will be recorded in the firewall log file.

18.2.1. (L1) Ensure LAPS AdmPwd GPO Extension / CSE is installed 0.00 %

Proof This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1637928: FAIL

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\

{D76B9641-3288-4f75-942D-087DE603E3EA}
name: DllName
2. oval-org.cisecurity.benchmarks.windows_10-def-1637931: FAIL

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{D76B9641-3288-4f75-942D-087DE603E3EA}
name: DllName

Remediation Steps

In order to utilize LAPS, a minor Active Directory Schema update is required, and a Group Policy Client Side Extension (CSE) must be installed on each managed computer. When LAPS is installed, the file AdmPwd.dll must be present in the following location and registered in Windows (the LAPS AdmPwd GPO Extension / CSE installation does this for you): C:\Program Files\LAPS\CSE\AdmPwd.dll Impact: No impact. When installed and registered properly, AdmPwd.dll takes no action unless given appropriate GPO commands during Group Policy refresh. It is not a memory-resident agent or service. In a disaster recovery scenario where Active Directory is not available, the local Administrator password will not be retrievable and a local password reset using a tool (such as Microsoft's Disaster and Recovery Toolset (DaRT) Recovery Image) may be necessary.

18.2.2. (L1) Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' 0.00 %

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637937: FAIL

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft Services\AdmPwd
name: PwdExpirationProtectionEnabled

Remediation Steps

To establish the recommended configuration via GP, set the following UI path to Enabled : Computer Configuration\Policies\Administrative Templates\LAPS\Do not allow password expiration time longer than required by policy Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adml) is required - it is included with Microsoft Local Administrator Password Solution (LAPS). Impact: Planned password expiration longer than password age dictated by "Password Settings" policy is NOT allowed.

18.2.3. (L1) Ensure 'Enable Local Admin Password Management' is set to 'Enabled' 0.00 %

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637944: FAIL

Based on the following 1 results:

1.

1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft Services\AdmPwd
name: AdmPwdEnabled

Remediation Steps

To establish the recommended configuration via GP, set the following UI path to Enabled : Computer Configuration\Policies\Administrative Templates\LAPS\Enable Local Admin Password Management Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adml) is required - it is included with Microsoft Local Administrator Password Solution (LAPS). Impact: The local administrator password is managed (provided that the LAPS AdmPwd GPO Extension / CSE is installed on the target computer (see Rule 18.2.1), the Active Directory domain schema and account permissions have been properly configured on the domain). In a disaster recovery scenario where Active Directory is not available, the local Administrator password will not be retrievable and a local password reset using a tool (such as Microsoft's Disaster and Recovery Toolset (DaRT) Recovery Image) may be necessary.

18.2.4. (L1) Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' 0.00 %

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637949: FAIL

Based on the following 1 results:

1.

1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft Services\AdmPwd
name: PasswordComplexity

Remediation Steps

To establish the recommended configuration via GP, set the following UI path to Enabled , and configure the Password Complexity option to Large letters + small letters + numbers + special characters : Computer Configuration\Policies\Administrative Templates\LAPS\Password Settings Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adml) is required - it is included with Microsoft Local Administrator Password Solution (LAPS). Impact: LAPS-generated passwords will be required to contain large letters + small letters + numbers + special characters.

18.2.5. (L1) Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' 0.00 %

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637954: FAIL

Based on the following 1 results:

1.

1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft Services\AdmPwd
name: PasswordLength

Remediation Steps

To establish the recommended configuration via GP, set the following UI path to Enabled , and configure the Password Length option to 15 or more : Computer Configuration\Policies\Administrative Templates\LAPS\Password Settings Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adml) is required - it is included with Microsoft Local Administrator Password Solution (LAPS). Impact: LAPS-generated passwords will be required to have a length of 15 characters (or more, if selected).

18.2.6. (L1) Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' 0.00 %

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637960: FAIL

Based on the following 1 results:

1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft Services\AdmPwd
name: PasswordAgeDays

Remediation Steps

To establish the recommended configuration via GP, set the following UI path to Enabled , and configure the Password Age (Days) option to 30 or fewer : Computer Configuration\Policies\Administrative Templates\LAPS\Password Settings Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adml) is required - it is included with Microsoft Local Administrator Password Solution (LAPS). Impact: LAPS-generated passwords will be required to have a maximum age of 30 days (or fewer, if selected).

18.3.1. (L1) Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' 0.00 %

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637965: FAIL

Based on the following 1 results:

1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
name: LocalAccountTokenFilterPolicy

Remediation Steps To establish the recommended configuration via GP, set the following UI path to Enabled : Computer Configuration\Policies\Administrative Templates\MS Security Guide\Apply UAC restrictions to local accounts on network logons Note: This Group Policy path does not exist by default. An additional Group Policy template (SecGuide.admx/adml) is required - it is available from Microsoft at this link . Impact: None - this is the default behavior.

18.5.11.4. (L1) Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled' 0.00 %

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638043: FAIL

Based on the following 1 results:

1.

1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\Network Connections
name: NC_StdDomainUserSetLocation

Remediation Steps To establish the recommended configuration via GP, set the following UI path to Enabled : Computer Configuration\Policies\Administrative Templates\Network\Network Connections\Require domain users to elevate when setting a network's location Note: This Group Policy path may not exist by default. It is provided by the Group Policy template NetworkConnections.admx/adml that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer). Impact: Domain users must elevate when setting a network's location.

18.5.21.2. (L1) Ensure 'Prohibit connection to non-domain networks when connected to domain authenticated network' is set to 'Enabled' 0.00 %

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638064: FAIL

Based on the following 1 results:

1.

1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\WcmSvc\GroupPolicy
name: fBlockNonDomain

Remediation Steps To establish the recommended configuration via GP, set the following UI path to Enabled : Computer Configuration\Policies\Administrative Templates\Network\Windows Connection Manager\Prohibit connection to non-domain networks when connected to domain authenticated network Note: This Group Policy path may not exist by default. It is provided by the Group Policy template WCM.admx/adml that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer). Impact: The computer responds to automatic and manual network connection attempts based on the following circumstances: Automatic connection attempts - When the computer is already connected to a domain based network, all automatic connection attempts to non-domain networks are blocked. - When the

computer is already connected to a non-domain based network, automatic connection attempts to domain based networks are blocked. Manual connection attempts - When the computer is already connected to either a non-domain based network or a domain based network over media other than Ethernet, and a user attempts to create a manual connection to an additional network in violation of this policy setting, the existing network connection is disconnected and the manual connection is allowed. - When the computer is already connected to either a non-domain based network or a domain based network over Ethernet, and a user attempts to create a manual connection to an additional network in violation of this policy setting, the existing Ethernet connection is maintained and the manual connection attempt is blocked.

18.8.3.1. (L1) Ensure 'Include command line in process creation events' is set to 'Disabled' 0.00 %

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638069: FAIL

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
FAIL
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Audit
name: ProcessCreationIncludeCmdLine_Enabled
type: reg_dword
value: 1

Remediation Steps

To establish the recommended configuration via GP, set the following UI path to Disabled : Computer Configuration\Policies\Administrative Templates\System\Audit Process Creation\Include command line in process creation events Note: This Group Policy path may not exist by default. It is provided by the Group Policy template AuditSettings.admx/adml that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer). Impact: None - this is the default behavior.

18.8.21.2. (L1) Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' 0.00 %

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638088: FAIL

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\Group Policy\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}
name: NoBackgroundPolicy

Remediation Steps

To establish the recommended configuration via GP, set the following UI path to Enabled , then set the Do not apply during periodic background processing option to FALSE (unchecked): Computer Configuration\Policies\Administrative Templates\System\Group Policy\Configure registry policy processing Note:

This Group Policy path may not exist by default. It is provided by the Group Policy template GroupPolicy.admx/adml that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer). Impact: Group Policies will be reapplied every time they are refreshed, which could have a slight impact on performance.

18.8.21.3. (L1) Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' 0.00 %

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638089: FAIL

Based on the following 1 results:

1.

1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\Group Policy\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}
name: NoGPOListChanges

Remediation Steps

To establish the recommended configuration via GP, set the following UI path to Enabled , then set the Process even if the Group Policy objects have not changed option to TRUE (checked): Computer Configuration\Policies\Administrative Templates\System\Group Policy\Configure registry policy processing Note: This Group Policy path may not exist by default. It is provided by the Group Policy template GroupPolicy.admx/adml that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer). Impact: Group Policies will be reapplied even if they have not been changed, which could have a slight impact on performance.

18.8.28.3. (L1) Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled' 0.00 %

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638113: FAIL

Based on the following 1 results:

1.

1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\System
name: DontEnumerateConnectedUsers

Remediation Steps

To establish the recommended configuration via GP, set the following UI path to Enabled : Computer Configuration\Policies\Administrative Templates\System\Logon\Do not enumerate connected users on domain-joined computers Note: This Group Policy path may not exist by default. It is provided by the Group Policy template Logon.admx/adml that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer). Impact: The Logon UI will not enumerate any connected users on domain-joined computers.

18.8.28.4. (L1) Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' 0.00 %

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638114: FAIL

Based on the following 1 results:

1.
   1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\System
name: EnumerateLocalUsers

Remediation Steps

To establish the recommended configuration via GP, set the following UI path to Disabled : Computer Configuration\Policies\Administrative Templates\System\Logon\Enumerate local users on domain-joined computers Note: This Group Policy path may not exist by default. It is provided by the Group Policy template Logon.admx/adml that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer). Impact: None - this is the default behavior.

18.8.28.6. (L1) Ensure 'Turn off picture password sign-in' is set to 'Enabled' 0.00 %

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638116: FAIL

Based on the following 1 results:

1.
   1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\System
name: BlockDomainPicturePassword

Remediation Steps

To establish the recommended configuration via GP, set the following UI path to Enabled : Computer Configuration\Policies\Administrative Templates\System\Logon\Turn off picture password sign-in Note: This Group Policy path may not exist by default. It is provided by the Group Policy template CredentialProviders.admx/adml that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer). Impact: Users will not be able to set up or sign in with a picture password.

18.9.48.4. (L1) Ensure 'Allow Sideloading of extension' is set to 'Disabled' 0.00 %

Proof

Based on the following 1 results:

1.
   1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
The specified Windows registry information entry was not found based on the given criteria:

hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\MicrosoftEdge\Extensions
name: AllowSideloadingOfExtensions

Remediation Steps

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Allow Sideloading of extension Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MicrosoftEdge.admx/adml that is included with the Microsoft Windows 10 Release 1809 & Server 2019 Administrative Templates (or newer). Impact: Sideloading of unverified extensions in Microsoft Edge is not allowed.

18.9.48.5. (L1) Ensure 'Configure cookies' is set to 'Enabled: Block only 3rd-party cookies' or higher 0.00 %

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638261: FAIL

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\MicrosoftEdge\Main
name: Cookies

Remediation Steps

To establish the recommended configuration via GP, set the following UI path to Enabled: Block only 3rd-party cookies (or, if applicable for your environment, Enabled: Block all cookies): Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Configure cookies Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MicrosoftEdge.admx/adml that is included with the Microsoft Windows 10 Release 1507 Administrative Templates (or newer). Note #2: In the Microsoft Windows 10 Release 1507 Administrative Templates, this setting was named Configure how Microsoft Edge treats cookies , but it was renamed starting with the Windows 10 Release 1511 Administrative Templates. Impact: If you select "Block only 3rd-party cookies", cookies from 3rd-party websites will be blocked, but 1st-party website cookies will still be permitted. If you select "Block all cookies", cookies from all websites will be blocked. Note: Blocking all cookies may interfere with functionality on some websites that depend on them for session tracking and/or login credentials.

18.9.48.6. (L1) Ensure 'Configure Password Manager' is set to 'Disabled' 0.00 %

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638262: FAIL

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\MicrosoftEdge\Main
name: FormSuggest Passwords

Remediation Steps To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Configure Password Manager Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MicrosoftEdge.admx/adml that is included with the Microsoft Windows 10 Release 1507 Administrative Templates (or newer). Note #2: In the Microsoft Windows 10 Release 1507 Administrative Templates, this setting was initially named Allows you to configure password manager . In the Microsoft Windows 10 Release 1511 Administrative Templates, this setting was renamed to Turn off Password Manager , but it was finally renamed to Configure Password Manager starting with the Windows 10 Release 1607 & Server 2016 Administrative Templates. Impact: Employees will not be able to use Password Manager.

18.9.48.9. (L1) Ensure 'Configure the Adobe Flash Click-to-Run setting' is set to 'Enabled' 0.00 %

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638265: FAIL

Based on the following 1 results:

1.

1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\MicrosoftEdge\Security
name: FlashClickToRunMode

Remediation Steps To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Configure the Adobe Flash Click-to-Run setting Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MicrosoftEdge.admx/adml that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer). Impact: None - this is the default behavior.

18.9.48.11. (L1) Ensure 'Prevent bypassing Windows Defender SmartScreen prompts for files' is set to 'Enabled' 0.00 %

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638267: FAIL

Based on the following 1 results:

1.

1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\MicrosoftEdge\PhishingFilter
name: PreventOverrideAppRepUnknown

Remediation Steps To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Prevent bypassing Windows Defender SmartScreen prompts for files Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MicrosoftEdge.admx/adml that is

included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer). Note #2: In the Microsoft Windows 10 Release 1511 Administrative Templates, this setting was initially named Don't allow SmartScreen Filter warning overrides for unverified files . In the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates, this setting was renamed to Prevent bypassing SmartScreen prompts for files . Finally, it was given its current name of Prevent bypassing Windows Defender SmartScreen prompts for files starting with the Windows 10 Release 1703 Administrative Templates. Impact: Employees will not be able to ignore SmartScreen Filter warnings on files, and they will be blocked from downloading unverified files (that are potentially malicious) that SmartScreen detects.

18.9.48.12. (L1) Ensure 'Prevent certificate error overrides' is set to 'Enabled' 0.00 %

Proof

Based on the following 1 results:

1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\MicrosoftEdge\Internet Settings
name: PreventCertErrorOverrides

Remediation Steps

To establish the recommended configuration via GP, set the following UI path to Enabled : Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Prevent certificate error overrides Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MicrosoftEdge.admx/adml that is included with the Microsoft Windows 10 Release 1809 & Server 2019 Administrative Templates (or newer). Impact: Overriding certificate errors is not allowed. Internal websites at an organization may not load if they use self-signed SSL certificates that are not issued from a trusted PKI source.

18.9.95.1. (L1) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled' 0.00 %

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638312: FAIL

Based on the following 1 results:

1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
FAIL
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging
name: EnableScriptBlockLogging
type: reg_dword
value: 1

Remediation Steps

To establish the recommended configuration via GP, set the following UI path to Disabled : Computer Configuration\Policies\Administrative Templates\Windows Components\Windows PowerShell\Turn on PowerShell Script Block Logging Note: This Group Policy path may not exist by default. It is provided by the Group Policy template PowerShellExecutionPolicy.admx/adml that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer). Impact: Logging of PowerShell script input is disabled.

18.9.102.1.1. (L1) Ensure 'Manage preview builds' is set to 'Enabled: Disable preview builds' 0.00 %

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638323: PASS

Based on the following 1 results:

1.
   1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate
name: ManagePreviewBuilds
type: reg_dword
value: 1

2. oval-org.cisecurity.benchmarks.windows_10-def-1638324: FAIL

Based on the following 1 results:

1.
   1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
FAIL
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate
name: ManagePreviewBuildsPolicyValue
type: reg_dword
value: 1

Remediation Steps

To establish the recommended configuration via GP, set the following UI path to Enabled: Disable preview builds : Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Windows Update for Business\Manage preview builds Note: This Group Policy path may not exist by default. It is provided by the Group Policy template WindowsUpdate.admx/adml that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer). Impact: Preview builds are prevented from installing on the device.

18.9.102.1.2. (L1) Ensure 'Select when Preview Builds and Feature Updates are received' is set to 'Enabled: Semi-Annual Channel, 180 or more days' 0.00 %

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638326: PASS

Based on the following 1 results:

1.
   1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate
name: DeferFeatureUpdatesPeriodInDays
type: reg_dword
value: 180

2.

This is a complex check. Operator = AND
1. oval-org.cisecurity.benchmarks.windows_10-def-1638325: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate
name: DeferFeatureUpdates
type: reg_dword
value: 1
2. oval-org.cisecurity.benchmarks.windows_10-def-1638327: FAIL

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate
name: BranchReadinessLevel

Remediation Steps

To establish the recommended configuration via GP, set the following UI path to Enabled: Semi-Annual Channel, 180 or more days : Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Windows Update for Business\Select when Preview Builds and Feature Updates are received Note: This Group Policy path may not exist by default. It is provided by the Group Policy template WindowsUpdate.admx/adml that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer). Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named Select when Feature Updates are received , but it was renamed to Select when Preview Builds and Feature Updates are received starting with the Windows 10 Release 1709 Administrative Templates. Impact: Feature Updates will be delayed until 180 or more days after they are declared to have a Windows readiness level of "Semi-Annual Channel".

Passed Rules

1.1.1. (L1) Ensure 'Enforce password history' is set to '24 or more password(s)'

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637750: PASS

Based on the following 1 results:
1.
1. At least one specified Password Policy entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS

Proof password_hist_len: 24

1.1.3. (L1) Ensure 'Minimum password age' is set to '1 or more day(s)'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637753: PASS

Based on the following 1 results:

1.
    1. At least one specified Password Policy entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
min_passwd_age: 86400

1.1.4. (L1) Ensure 'Minimum password length' is set to '14 or more character(s)'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637754: PASS

Based on the following 1 results:

1.
    1. At least one specified Password Policy entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
min_passwd_len: 14

1.1.5. (L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637755: PASS

Based on the following 1 results:

1.
    1. At least one specified Password Policy entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
password_complexity: true

1.1.6. (L1) Ensure 'Relax minimum password length limits' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637756: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the

given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Control\SAM
name: relaxminimumpasswordlengthlimits
type: reg_dword
value: 1

1.1.7. (L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637757: PASS

Based on the following 1 results:
1.
1. At least one specified Password Policy entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
reversible_encryption: false

1.2.1. (L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637758: PASS

Based on the following 1 results:
1.
1. At least one specified Lockout Policy entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
lockout_duration: 900

1.2.2. (L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637759: PASS

Based on the following 1 results:
1.
1. At least one specified Lockout Policy entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
lockout_threshold: 5
2. oval-org.cisecurity.benchmarks.windows_10-def-1637760: PASS

Based on the following 1 results:
1.
1. At least one specified Lockout Policy entry must match the given criteria. At

least one evaluation must pass.
Entry 1 findings:
PASS
lockout_threshold: 5

1.2.3. (L1) Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)'

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637761: PASS

Based on the following 1 results:

1.
    1. At least one specified Lockout Policy entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
lockout_observation_window: 900

2.2.1. (L1) Ensure 'Access Credential Manager as a trusted caller' is set to 'No One'

Proof

Based on the following 1 results:

1.
    1. The specified User Right entry must not match the given criteria.

The specified User Right entry was not found based on the given criteria:
userright: SE_TRUSTED_CREDMAN_ACCESS_NAME

2.2.2. (L1) Ensure 'Access this computer from the network' is set to 'Administrators, Remote Desktop Users'

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637763: PASS

Based on the following 1 results:

1.
    1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
userright: SE_NETWORK_LOGON_NAME
trustee_sid: S-1-5-32-555
trustee_sid: S-1-5-32-544

2.2.3. (L1) Ensure 'Act as part of the operating system' is set to 'No One'

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637765: PASS

Based on the following 1 results:

1.
    1. The specified User Right entry must not match the given criteria.

The specified User Right entry was not found based on the given criteria:
userright: SE_TCB_NAME

2.2.4. (L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637767: PASS

Based on the following 1 results:

1.
    1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
userright: SE_INCREASE_QUOTA_NAME
trustee_sid: S-1-5-32-544
trustee_sid: S-1-5-20
trustee_sid: S-1-5-19

2.2.5. (L1) Ensure 'Allow log on locally' is set to 'Administrators, Users'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637768: PASS

Based on the following 1 results:

1.
    1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
userright: SE_INTERACTIVE_LOGON_NAME
trustee_sid: S-1-5-32-545
trustee_sid: S-1-5-32-544

2.2.6. (L1) Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637770: PASS

Based on the following 1 results:

1.
    1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
userright: SE_REMOTE_INTERACTIVE_LOGON_NAME
trustee_sid: S-1-5-32-555
trustee_sid: S-1-5-32-544

2.2.7. (L1) Ensure 'Back up files and directories' is set to 'Administrators'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637772: PASS

Based on the following 1 results:

1.
    1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
userright: SE_BACKUP_NAME
trustee_sid: S-1-5-32-544

2.2.8. (L1) Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637774: PASS

Based on the following 1 results:

1.
    1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
userright: SE_SYSTEMTIME_NAME
trustee_sid: S-1-5-32-544
trustee_sid: S-1-5-19

2.2.9. (L1) Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE, Users'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637775: PASS

Based on the following 1 results:

1.
    1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
userright: SE_TIME_ZONE_NAME
trustee_sid: S-1-5-32-545
trustee_sid: S-1-5-32-544
trustee_sid: S-1-5-19

2.2.10. (L1) Ensure 'Create a pagefile' is set to 'Administrators'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637777: PASS

Based on the following 1 results:

1.
    1. At least one specified User Right entry must match the given criteria. At least

one evaluation must pass.
Entry 1 findings:
PASS
userright: SE_CREATE_PAGEFILE_NAME
trustee_sid: S-1-5-32-544

2.2.11. (L1) Ensure 'Create a token object' is set to 'No One'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637779: PASS

Based on the following 1 results:
1.
1. The specified User Right entry must not match the given criteria.
The specified User Right entry was not found based on the given criteria:
userright: SE_CREATE_TOKEN_NAME

2.2.12. (L1) Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637781: PASS

Based on the following 1 results:
1.
1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
userright: SE_CREATE_GLOBAL_NAME
trustee_sid: S-1-5-6
trustee_sid: S-1-5-32-544
trustee_sid: S-1-5-20
trustee_sid: S-1-5-19

2.2.13. (L1) Ensure 'Create permanent shared objects' is set to 'No One'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637783: PASS

Based on the following 1 results:
1.
1. The specified User Right entry must not match the given criteria.
The specified User Right entry was not found based on the given criteria:
userright: SE_CREATE_PERMANENT_NAME

2.2.14. (L1) Configure 'Create symbolic links' is set to 'Administrators, NT VIRTUAL MACHINE\Virtual Machines'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637785: PASS

Based on the following 1 results:

1.
    1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
userright: SE_CREATE_SYMBOLIC_LINK_NAME
trustee_sid: S-1-5-32-544

2.2.15. (L1) Ensure 'Debug programs' is set to 'Administrators'

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637786: PASS

Based on the following 1 results:

1.
    1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
userright: SE_DEBUG_NAME
trustee_sid: S-1-5-32-544

2.2.17. (L1) Ensure 'Deny log on as a batch job' to include 'Guests'

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637790: PASS

Based on the following 1 results:

1.
    1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
userright: SE_DENY_BATCH_LOGON_NAME
trustee_sid: S-1-5-32-546

2.2.18. (L1) Ensure 'Deny log on as a service' to include 'Guests'

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637792: PASS

Based on the following 1 results:

1.
    1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
userright: SE_DENY_SERVICE_LOGON_NAME
trustee_sid: S-1-5-32-546

2.2.19. (L1) Ensure 'Deny log on locally' to include 'Guests'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637794: PASS

Based on the following 1 results:

1.
    1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
userright: SE_DENY_INTERACTIVE_LOGON_NAME
trustee_sid: S-1-5-32-546

2.2.21. (L1) Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637798: PASS

Based on the following 1 results:

1.
    1. The specified User Right entry must not match the given criteria.

The specified User Right entry was not found based on the given criteria:
userright: SE_ENABLE_DELEGATION_NAME

2.2.22. (L1) Ensure 'Force shutdown from a remote system' is set to 'Administrators'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637800: PASS

Based on the following 1 results:

1.
    1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
userright: SE_REMOTE_SHUTDOWN_NAME
trustee_sid: S-1-5-32-544

2.2.23. (L1) Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637801: PASS

Based on the following 1 results:

1.
    1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:

PASS
userright: SE_AUDIT_NAME
trustee_sid: S-1-5-20
trustee_sid: S-1-5-19

2.2.24. (L1) Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637804: PASS

Based on the following 1 results:
1.
1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
userright: SE_IMPERSONATE_NAME
trustee_sid: S-1-5-6
trustee_sid: S-1-5-32-544
trustee_sid: S-1-5-20
trustee_sid: S-1-5-19

2.2.25. (L1) Ensure 'Increase scheduling priority' is set to 'Administrators, Window Manager\Window Manager Group'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637806: PASS

Based on the following 1 results:
1.
1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
userright: SE_INC_BASE_PRIORITY_NAME
trustee_sid: S-1-5-32-544

2.2.26. (L1) Ensure 'Load and unload device drivers' is set to 'Administrators'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637809: PASS

Based on the following 1 results:
1.
1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
userright: SE_LOAD_DRIVER_NAME
trustee_sid: S-1-5-32-544

2.2.27. (L1) Ensure 'Lock pages in memory' is set to 'No One'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637812: PASS

Based on the following 1 results:

1.
    1. The specified User Right entry must not match the given criteria.

The specified User Right entry was not found based on the given criteria:
userright: SE_LOCK_MEMORY_NAME

2.2.30. (L1) Ensure 'Manage auditing and security log' is set to 'Administrators'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637820: PASS

Based on the following 1 results:

1.
    1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
userright: SE_SECURITY_NAME
trustee_sid: S-1-5-32-544

2.2.31. (L1) Ensure 'Modify an object label' is set to 'No One'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637823: PASS

Based on the following 1 results:

1.
    1. The specified User Right entry must not match the given criteria.

The specified User Right entry was not found based on the given criteria:
userright: SE_RELABEL_NAME

2.2.32. (L1) Ensure 'Modify firmware environment values' is set to 'Administrators'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637825: PASS

Based on the following 1 results:

1.
    1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
userright: SE_SYSTEM_ENVIRONMENT_NAME
trustee_sid: S-1-5-32-544

2.2.33. (L1) Ensure 'Perform volume maintenance tasks' is set to 'Administrators'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637827: PASS

Based on the following 1 results:

1.
    1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
userright: SE_MANAGE_VOLUME_NAME
trustee_sid: S-1-5-32-544

2.2.34. (L1) Ensure 'Profile single process' is set to 'Administrators'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637830: PASS

Based on the following 1 results:

1.
    1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
userright: SE_PROF_SINGLE_PROCESS_NAME
trustee_sid: S-1-5-32-544

2.2.35. (L1) Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637833: PASS

Based on the following 1 results:

1.
    1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
userright: SE_SYSTEM_PROFILE_NAME
trustee_sid: S-1-5-32-544

2.2.36. (L1) Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637834: PASS

Based on the following 1 results:

1.
    1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:

PASS
userright: SE_ASSIGNPRIMARYTOKEN_NAME
trustee_sid: S-1-5-20
trustee_sid: S-1-5-19

2.2.37. (L1) Ensure 'Restore files and directories' is set to 'Administrators'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637837: PASS

Based on the following 1 results:
1.
1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
userright: SE_RESTORE_NAME
trustee_sid: S-1-5-32-544

2.2.38. (L1) Ensure 'Shut down the system' is set to 'Administrators, Users'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637840: PASS

Based on the following 1 results:
1.
1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
userright: SE_SHUTDOWN_NAME
trustee_sid: S-1-5-32-545
trustee_sid: S-1-5-32-544

2.2.39. (L1) Ensure 'Take ownership of files or other objects' is set to 'Administrators'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637841: PASS

Based on the following 1 results:
1.
1. At least one specified User Right entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
userright: SE_TAKE_OWNERSHIP_NAME
trustee_sid: S-1-5-32-544

2.3.1.1. (L1) Ensure 'Accounts: Administrator account status' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637844: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows User SID entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
user_sid: S-1-5-21-3293848366-2354669173-3456164447-500
enabled: false

2.3.1.2. (L1) Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637847: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Microsoft\Windows\CurrentVersion\Policies\System
name: noconnecteduser
type: reg_dword
value: 3

2.3.1.3. (L1) Ensure 'Accounts: Guest account status' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637850: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows User SID entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
user_sid: S-1-5-21-3293848366-2354669173-3456164447-501
enabled: false

2.3.1.4. (L1) Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637853: PASS

Based on the following 1 results:

1.

1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Control\Lsa
name: LimitBlankPasswordUse
type: reg_dword
value: 1

2.3.1.5. (L1) Configure 'Accounts: Rename administrator account'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637856: PASS

Based on the following 1 results:
1.
1. At least one specified SID entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
trustee_sid: S-1-5-21-3293848366-2354669173-3456164447-500
trustee_name: CISADMIN

2.3.1.6. (L1) Configure 'Accounts: Rename guest account'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637859: PASS

Based on the following 1 results:
1.
1. At least one specified SID entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
trustee_sid: S-1-5-21-3293848366-2354669173-3456164447-501
trustee_name: CISGUEST

2.3.2.1. (L1) Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637864: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Control\Lsa
name: scenoapplylegacyauditpolicy
type: reg_dword

value: 1

2.3.2.2. (L1) Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637869: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Control\Lsa
name: crashonauditfail
type: reg_dword
value: 0

2.3.6.1. (L1) Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637885: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Services\Netlogon\Parameters
name: RequireSignOrSeal
type: reg_dword
value: 1

2.3.6.2. (L1) Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637891: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Services\Netlogon\Parameters
name: SealSecureChannel
type: reg_dword
value: 1

2.3.6.3. (L1) Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637894: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Services\Netlogon\Parameters
name: SignSecureChannel
type: reg_dword
value: 1

2.3.6.4. (L1) Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637899: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Services\Netlogon\Parameters
name: DisablePasswordChange
type: reg_dword
value: 0

2.3.6.5. (L1) Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637903: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Services\Netlogon\Parameters
name: MaximumPasswordAge
type: reg_dword
value: 30

2. oval-org.cisecurity.benchmarks.windows_10-def-1637906: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Services\Netlogon\Parameters
name: MaximumPasswordAge
type: reg_dword
value: 30

2.3.6.6. (L1) Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637911: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Services\Netlogon\Parameters
name: RequireStrongKey
type: reg_dword
value: 1

2.3.7.1. (L1) Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637916: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Microsoft\Windows\CurrentVersion\Policies\System
name: disablecad
type: reg_dword
value: 0

2.3.7.2. (L1) Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637921: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Microsoft\Windows\CurrentVersion\Policies\System
name: dontdisplaylastusername
type: reg_dword
value: 1

2.3.7.4. (L1) Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0'

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637938: PASS

Based on the following 1 results:
1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Microsoft\Windows\CurrentVersion\Policies\System
name: inactivitytimeoutsecs
type: reg_dword
value: 900

2. oval-org.cisecurity.benchmarks.windows_10-def-1637942: PASS

Based on the following 1 results:
1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Microsoft\Windows\CurrentVersion\Policies\System
name: inactivitytimeoutsecs
type: reg_dword
value: 900

2.3.7.5. (L1) Configure 'Interactive logon: Message text for users attempting to log on'

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637947: PASS

Based on the following 1 results:
1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Microsoft\Windows\CurrentVersion\Policies\System
name: legalnoticetext

type: reg_sz
value: ADD TEXT HERE

2.3.7.6. (L1) Configure 'Interactive logon: Message title for users attempting to log on'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637953: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Microsoft\Windows\CurrentVersion\Policies\System
name: legalnoticecaption
type: reg_sz
value: ADD TEXT HERE

2.3.7.8. (L1) Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637964: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Microsoft\Windows NT\CurrentVersion\Winlogon
name: PasswordExpiryWarning
type: reg_dword
value: 14
2. oval-org.cisecurity.benchmarks.windows_10-def-1637967: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Microsoft\Windows NT\CurrentVersion\Winlogon
name: PasswordExpiryWarning
type: reg_dword
value: 14

2.3.7.9. (L1) Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637973: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Microsoft\Windows NT\CurrentVersion\Winlogon
name: scremoveoption
type: reg_sz
value: 1

2.3.8.1. (L1) Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637980: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Services\LanmanWorkstation\Parameters
name: RequireSecuritySignature
type: reg_dword
value: 1

2.3.8.2. (L1) Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637983: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Services\LanmanWorkstation\Parameters
name: EnableSecuritySignature
type: reg_dword
value: 1

2.3.8.3. (L1) Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637985: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Services\LanmanWorkstation\Parameters
name: EnablePlainTextPassword
type: reg_dword
value: 0

2.3.9.1. (L1) Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s)'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637987: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Services\LanManServer\Parameters
name: autodisconnect
type: reg_dword
value: 15

2.3.9.2. (L1) Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637990: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Services\LanManServer\Parameters
name: requiresecuritysignature
type: reg_dword
value: 1

2.3.9.3. (L1) Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637992: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Services\LanManServer\Parameters
name: enablesecuritysignature
type: reg_dword
value: 1

2.3.9.4. (L1) Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637995: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Services\LanManServer\Parameters
name: enableforcedlogoff
type: reg_dword
value: 1

2.3.9.5. (L1) Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637998: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Services\LanManServer\Parameters
name: smbservernamehardeninglevel
type: reg_dword
value: 1

2.3.10.2. (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638002: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Control\Lsa
name: restrictanonymoussam
type: reg_dword
value: 1

2.3.10.3. (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638004: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Control\Lsa
name: restrictanonymous
type: reg_dword
value: 1

2.3.10.4. (L1) Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638006: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Control\Lsa
name: disabledomaincreds
type: reg_dword
value: 1

2.3.10.5. (L1) Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638008: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Control\Lsa
name: everyoneincludesanonymous
type: reg_dword
value: 0

2.3.10.6. (L1) Ensure 'Network access: Named Pipes that can be accessed anonymously' is set to 'None'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638010: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\LanManServer\Parameters
name: NullSessionPipes
type: reg_multi_sz
value:

2.3.10.7. (L1) Ensure 'Network access: Remotely accessible registry paths' is configured

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638012: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedExactPaths
name: Machine
type: reg_multi_sz
value: System\CurrentControlSet\Control\ProductOptions
value: System\CurrentControlSet\Control\Server Applications
value: Software\Microsoft\Windows NT\CurrentVersion

2.3.10.8. (L1) Ensure 'Network access: Remotely accessible registry paths and sub-paths'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638014: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedPaths
name: Machine
type: reg_multi_sz
value: Software\Microsoft\Windows NT\CurrentVersion\Print
value: Software\Microsoft\Windows NT\CurrentVersion\Windows
value: System\CurrentControlSet\Control\Print\Printers
value: System\CurrentControlSet\Services\Eventlog
value: Software\Microsoft\OLAP Server
value: System\CurrentControlSet\Control\ContentIndex
value: System\CurrentControlSet\Control\Terminal Server
value: System\CurrentControlSet\Control\Terminal Server\UserConfig
value: System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration
value: Software\Microsoft\Windows NT\CurrentVersion\Perflib
value: System\CurrentControlSet\Services\SysmonLog

2.3.10.9. (L1) Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638016: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\LanManServer\Parameters
name: restrictnullsessaccess
type: reg_dword
value: 1

2.3.10.10. (L1) Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638018: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE

key: SYSTEM\CurrentControlSet\Control\Lsa
name: restrictremotesam
type: reg_sz
value: O:BAG:BAD:(A;;RC;;;BA)

2.3.10.11. (L1) Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None'

Proof This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1638022: FAIL

Based on the following 1 results:
1.
1. The specified Windows registry information entry must not match the given criteria.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Services\LanManServer\Parameters
name: nullsessionshares
last_write_time: 0
type: reg_multi_sz
value:
windows_view: 64_bit
2. oval-org.cisecurity.benchmarks.windows_10-def-1638020: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Services\LanManServer\Parameters
name: nullsessionshares
type: reg_multi_sz
value:

2.3.10.12. (L1) Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638023: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Control\Lsa
name: forceguest
type: reg_dword
value: 0

2.3.11.1. (L1) Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638026: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Control\Lsa
name: usemachineid
type: reg_dword
value: 1

2.3.11.2. (L1) Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638028: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Control\Lsa\MSV1_0
name: allownullsessionfallback
type: reg_dword
value: 0

2.3.11.3. (L1) Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638030: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Control\Lsa\pku2u
name: allowonlineid
type: reg_dword
value: 0

2.3.11.4. (L1) Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types'

Proof

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters
name: supportedencryptiontypes
type: reg_dword
value: 2147483640

2.3.11.5. (L1) Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638035: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Control\Lsa
name: NoLmHash
type: reg_dword
value: 1

2.3.11.6. (L1) Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled'

Proof

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Services\LanManServer\Parameters
name: enableforcedlogoff
type: reg_dword
value: 1

2.3.11.7. (L1) Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM&NTLM'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638038: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Control\Lsa
name: lmcompatibilitylevel
type: reg_dword
value: 5

2.3.11.8. (L1) Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638040: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Services\LDAP
name: ldapclientintegrity
type: reg_dword
value: 1

2.3.11.9. (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638042: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Control\Lsa\MSV1_0
name: NtlmMinClientSec
type: reg_dword
value: 537395200

2.3.11.10. (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638044: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Control\Lsa\MSV1_0
name: NtlmMinServerSec
type: reg_dword
value: 537395200

2.3.15.1. (L1) Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638048: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Control\Session Manager\Kernel
name: obcaseinsensitive
type: reg_dword
value: 1

2.3.15.2. (L1) Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638050: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Control\Session Manager
name: ProtectionMode
type: reg_dword
value: 1

2.3.17.1. (L1) Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638052: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Microsoft\Windows\CurrentVersion\Policies\System
name: filteradministratortoken
type: reg_dword
value: 1

2.3.17.2. (L1) Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638054: PASS

Based on the following 1 results:
1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Microsoft\Windows\CurrentVersion\Policies\System
name: ConsentPromptBehaviorAdmin
type: reg_dword
value: 2

2.3.17.3. (L1) Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638057: PASS

Based on the following 1 results:
1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Microsoft\Windows\CurrentVersion\Policies\System
name: ConsentPromptBehaviorUser
type: reg_dword
value: 0

2.3.17.4. (L1) Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638059: PASS

Based on the following 1 results:
1.

1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Microsoft\Windows\CurrentVersion\Policies\System
name: EnableInstallerDetection
type: reg_dword
value: 1

2.3.17.5. (L1) Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638061: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Microsoft\Windows\CurrentVersion\Policies\System
name: EnableSecureUIAPaths
type: reg_dword
value: 1

2.3.17.6. (L1) Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638063: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Microsoft\Windows\CurrentVersion\Policies\System
name: EnableLUA
type: reg_dword
value: 1

2.3.17.7. (L1) Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638065: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the

given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Microsoft\Windows\CurrentVersion\Policies\System
name: PromptOnSecureDesktop
type: reg_dword
value: 1

2.3.17.8. (L1) Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638067: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Microsoft\Windows\CurrentVersion\Policies\System
name: EnableVirtualization
type: reg_dword
value: 1

5.3. (L1) Ensure 'Computer Browser (Browser)' is set to 'Disabled' or 'Not Installed'

Proof This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1637769: FAIL

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\Browser
name: Start
2. oval-org.cisecurity.benchmarks.windows_10-def-1637771: PASS

Based on the following 1 results:
1.
1. The specified Windows registry information entry must not match the given criteria.
The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\Browser
name: Start

5.6. (L1) Ensure 'IIS Admin Service (IISADMIN)' is set to 'Disabled' or 'Not Installed'

Proof This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1637778: FAIL

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\IISADMIN
name: Start

2. oval-org.cisecurity.benchmarks.windows_10-def-1637780: PASS

Based on the following 1 results:

1.
    1. The specified Windows registry information entry must not match the given criteria.
The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\IISADMIN
name: Start

5.7. (L1) Ensure 'Infrared monitor service (irmon)' is set to 'Disabled' or 'Not Installed'

Proof This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1637782: FAIL

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\irmon
name: Start

2. oval-org.cisecurity.benchmarks.windows_10-def-1637784: PASS

Based on the following 1 results:

1.
    1. The specified Windows registry information entry must not match the given criteria.
The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\irmon
name: Start

5.8. (L1) Ensure 'Internet Connection Sharing (ICS) (SharedAccess)' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637787: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\SharedAccess
name: Start
type: reg_dword
value: 4

5.10. (L1) Ensure 'LxssManager (LxssManager)' is set to 'Disabled' or 'Not Installed'

Proof This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1637791: FAIL

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\LxssManager
name: Start

2. oval-org.cisecurity.benchmarks.windows_10-def-1637793: PASS

Based on the following 1 results:

1.
    1. The specified Windows registry information entry must not match the given criteria.

The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\LxssManager
name: Start

5.11. (L1) Ensure 'Microsoft FTP Service (FTPSVC)' is set to 'Disabled' or 'Not Installed'

Proof This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1637795: FAIL

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\FTPSVC
name: Start

2. oval-org.cisecurity.benchmarks.windows_10-def-1637797: PASS

Based on the following 1 results:

1.
    1. The specified Windows registry information entry must not match the given criteria.

The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\FTPSVC
name: Start

5.13. (L1) Ensure 'OpenSSH SSH Server (sshd)' is set to 'Disabled' or 'Not Installed'

Proof This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1637802: FAIL

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\sshd
name: Start

2. oval-org.cisecurity.benchmarks.windows_10-def-1637805: PASS

Based on the following 1 results:

1.
    1. The specified Windows registry information entry must not match the given criteria.

The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\sshd
name: Start

5.23. (L1) Ensure 'Remote Procedure Call (RPC) Locator (RpcLocator)' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637838: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\RpcLocator
name: Start
type: reg_dword
value: 4

5.25. (L1) Ensure 'Routing and Remote Access (RemoteAccess)' is set to 'Disabled'

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637845: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\RemoteAccess
name: Start
type: reg_dword
value: 4

5.27. (L1) Ensure 'Simple TCP/IP Services (simptcp)' is set to 'Disabled' or 'Not Installed'

Proof

This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1637851: FAIL

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\simptcp
name: Start

2. oval-org.cisecurity.benchmarks.windows_10-def-1637854: PASS

Based on the following 1 results:

1.
    1. The specified Windows registry information entry must not match the given criteria.

The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\simptcp
name: Start

5.29. (L1) Ensure 'Special Administration Console Helper (sacsvr)' is set to 'Disabled' or 'Not Installed'

Proof

This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1637865: FAIL

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\sacsvr
name: Start

2. oval-org.cisecurity.benchmarks.windows_10-def-1637872: PASS

Based on the following 1 results:

1.
    1. The specified Windows registry information entry must not match the given criteria.

The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\sacsvr
name: Start

5.30. (L1) Ensure 'SSDP Discovery (SSDPSRV)' is set to 'Disabled'

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637877: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\SSDPSRV
name: Start
type: reg_dword
value: 4

5.31. (L1) Ensure 'UPnP Device Host (upnphost)' is set to 'Disabled'

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637881: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\upnphost
name: Start
type: reg_dword
value: 4

5.32. (L1) Ensure 'Web Management Service (WMSvc)' is set to 'Disabled' or 'Not Installed'

Proof This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1637886: FAIL

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\WMSvc
name: Start

2. oval-org.cisecurity.benchmarks.windows_10-def-1637890: PASS

Based on the following 1 results:

1.
    1. The specified Windows registry information entry must not match the given criteria.

The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\WMSvc
name: Start

5.35. (L1) Ensure 'Windows Media Player Network Sharing Service (WMPNetworkSvc)' is set to 'Disabled' or 'Not Installed'

Proof This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1637905: FAIL

Based on the following 1 results:

1.
    1. The specified Windows registry information entry must not match the given criteria.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\WMPNetworkSvc
name: Start
last_write_time: 0
type: reg_dword
value: 4
windows_view: 64_bit

2. oval-org.cisecurity.benchmarks.windows_10-def-1637902: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\WMPNetworkSvc
name: Start
type: reg_dword
value: 4

5.36. (L1) Ensure 'Windows Mobile Hotspot Service (icssvc)' is set to 'Disabled'

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637909: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\icssvc
name: Start
type: reg_dword
value: 4

5.40. (L1) Ensure 'World Wide Web Publishing Service (W3SVC)' is set to 'Disabled' or 'Not Installed'

Proof

This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1637935: FAIL

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\W3SVC
name: Start

2. oval-org.cisecurity.benchmarks.windows_10-def-1637940: PASS

Based on the following 1 results:

1.
    1. The specified Windows registry information entry must not match the given criteria.

The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\W3SVC
name: Start

5.41. (L1) Ensure 'Xbox Accessory Management Service (XboxGipSvc)' is set to 'Disabled'

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637945: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\XboxGipSvc
name: Start
type: reg_dword
value: 4

5.42. (L1) Ensure 'Xbox Live Auth Manager (XblAuthManager)' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637950: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\XblAuthManager
name: Start
type: reg_dword
value: 4

5.43. (L1) Ensure 'Xbox Live Game Save (XblGameSave)' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637956: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\XblGameSave
name: Start
type: reg_dword
value: 4

5.44. (L1) Ensure 'Xbox Live Networking Service (XboxNetApiSvc)' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637961: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS

hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\XboxNetApiSvc
name: Start
type: reg_dword
value: 4

9.2.1. (L1) Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637832: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\WindowsFirewall\PrivateProfile
name: EnableFirewall
type: reg_dword
value: 1

9.2.2. (L1) Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637836: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\WindowsFirewall\PrivateProfile
name: DefaultInboundAction
type: reg_dword
value: 1

9.2.3. (L1) Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637839: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\WindowsFirewall\PrivateProfile

name: DefaultOutboundAction
type: reg_dword
value: 0

9.2.4. (L1) Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637843: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\WindowsFirewall\PrivateProfile
name: DisableNotifications
type: reg_dword
value: 1

9.2.5. (L1) Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\privatefw.log'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637846: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging
name: LogFilePath
type: reg_sz
value: %systemroot%\system32\logfiles\firewall\privatefw.log

9.2.6. (L1) Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637849: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging
name: LogFileSize

type: reg_dword
value: 16384

9.2.7. (L1) Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637852: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging
name: LogDroppedPackets
type: reg_dword
value: 1

9.2.8. (L1) Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637855: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging
name: LogSuccessfulConnections
type: reg_dword
value: 1

9.3.1. (L1) Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637861: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\WindowsFirewall\PublicProfile
name: EnableFirewall
type: reg_dword
value: 1

9.3.2. (L1) Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637866: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\WindowsFirewall\PublicProfile
name: DefaultInboundAction
type: reg_dword
value: 1

9.3.3. (L1) Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637870: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\WindowsFirewall\PublicProfile
name: DefaultOutboundAction
type: reg_dword
value: 0

9.3.4. (L1) Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637874: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\WindowsFirewall\PublicProfile
name: DisableNotifications
type: reg_dword
value: 1

9.3.5. (L1) Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637879: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\WindowsFirewall\PublicProfile
name: AllowLocalPolicyMerge
type: reg_dword
value: 0

9.3.6. (L1) Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637883: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\WindowsFirewall\PublicProfile
name: AllowLocalIPsecPolicyMerge
type: reg_dword
value: 0

9.3.7. (L1) Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\publicfw.log'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637888: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging
name: LogFilePath
type: reg_sz
value: %systemroot%\system32\logfiles\firewall\publicfw.log

9.3.8. (L1) Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637892: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging
name: LogFileSize
type: reg_dword
value: 16384

9.3.9. (L1) Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637895: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging
name: LogDroppedPackets
type: reg_dword
value: 1

9.3.10. (L1) Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637900: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging
name: LogSuccessfulConnections
type: reg_dword
value: 1

17.1.1. (L1) Ensure 'Audit Credential Validation' is set to 'Success and Failure'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637857: PASS

Based on the following 1 results:

1.
    1. At least one specified Audit Event Policy Subcategories entry must match the given criteria.

At least one evaluation must pass.
Entry 1 findings:
PASS
credential_validation: AUDIT_SUCCESS_FAILURE

17.2.1. (L1) Ensure 'Audit Application Group Management' is set to 'Success and Failure'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637860: PASS

Based on the following 1 results:

1.
    1. At least one specified Audit Event Policy Subcategories entry must match the given criteria.

At least one evaluation must pass.
Entry 1 findings:
PASS
application_group_management: AUDIT_SUCCESS_FAILURE

17.2.2. (L1) Ensure 'Audit Security Group Management' is set to include 'Success'

Proof This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1637863: PASS

Based on the following 1 results:

1.
    1. At least one specified Audit Event Policy Subcategories entry must match the given criteria.

At least one evaluation must pass.
Entry 1 findings:
PASS
security_group_management: AUDIT_SUCCESS
2. oval-org.cisecurity.benchmarks.windows_10-def-1637867: FAIL

Based on the following 1 results:

1.
    1. At least one specified Audit Event Policy Subcategories entry must match the given criteria.

At least one evaluation must pass.
Entry 1 findings:
FAIL
security_group_management: AUDIT_SUCCESS

17.2.3. (L1) Ensure 'Audit User Account Management' is set to 'Success and Failure'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637868: PASS

Based on the following 1 results:

1.
    1. At least one specified Audit Event Policy Subcategories entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
user_account_management: AUDIT_SUCCESS_FAILURE

17.3.1. (L1) Ensure 'Audit PNP Activity' is set to include 'Success'

Proof This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1637871: PASS

Based on the following 1 results:

1.
    1. At least one specified Audit Event Policy Subcategories entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
plug_and_play_events: AUDIT_SUCCESS
2. oval-org.cisecurity.benchmarks.windows_10-def-1637873: FAIL

Based on the following 1 results:

1.
    1. At least one specified Audit Event Policy Subcategories entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
FAIL
plug_and_play_events: AUDIT_SUCCESS

17.3.2. (L1) Ensure 'Audit Process Creation' is set to include 'Success'

Proof This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1637876: PASS

Based on the following 1 results:

1.
    1. At least one specified Audit Event Policy Subcategories entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
process_creation: AUDIT_SUCCESS
2. oval-org.cisecurity.benchmarks.windows_10-def-1637878: FAIL

Based on the following 1 results:

1.
    1. At least one specified Audit Event Policy Subcategories entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:

FAIL
process_creation: AUDIT_SUCCESS

17.5.1. (L1) Ensure 'Audit Account Lockout' is set to include 'Failure'

Proof This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1637882: PASS

Based on the following 1 results:
1.
1. At least one specified Audit Event Policy Subcategories entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
account_lockout: AUDIT_FAILURE
2. oval-org.cisecurity.benchmarks.windows_10-def-1637884: FAIL

Based on the following 1 results:
1.
1. At least one specified Audit Event Policy Subcategories entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
FAIL
account_lockout: AUDIT_FAILURE

17.5.2. (L1) Ensure 'Audit Group Membership' is set to include 'Success'

Proof This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1637887: PASS

Based on the following 1 results:
1.
1. At least one specified Audit Event Policy Subcategories entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
group_membership: AUDIT_SUCCESS
2. oval-org.cisecurity.benchmarks.windows_10-def-1637889: FAIL

Based on the following 1 results:
1.
1. At least one specified Audit Event Policy Subcategories entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
FAIL
group_membership: AUDIT_SUCCESS

17.5.3. (L1) Ensure 'Audit Logoff' is set to include 'Success'

Proof This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1637896: PASS

Based on the following 1 results:

1.
    1. At least one specified Audit Event Policy Subcategories entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
logoff: AUDIT_SUCCESS
2. oval-org.cisecurity.benchmarks.windows_10-def-1637898: FAIL

Based on the following 1 results:

1.
    1. At least one specified Audit Event Policy Subcategories entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
FAIL
logoff: AUDIT_SUCCESS

17.5.4. (L1) Ensure 'Audit Logon' is set to 'Success and Failure'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637901: PASS

Based on the following 1 results:

1.
    1. At least one specified Audit Event Policy Subcategories entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
logon: AUDIT_SUCCESS_FAILURE

17.5.5. (L1) Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637904: PASS

Based on the following 1 results:

1.
    1. At least one specified Audit Event Policy Subcategories entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
other_logon_logoff_events: AUDIT_SUCCESS_FAILURE

17.5.6. (L1) Ensure 'Audit Special Logon' is set to include 'Success'

Proof This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1637908: PASS

Based on the following 1 results:

1.
    1. At least one specified Audit Event Policy Subcategories entry must match the

given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
special_logon: AUDIT_SUCCESS
2. oval-org.cisecurity.benchmarks.windows_10-def-1637910: FAIL

Based on the following 1 results:
1.
1. At least one specified Audit Event Policy Subcategories entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
FAIL
special_logon: AUDIT_SUCCESS

17.6.1. (L1) Ensure 'Audit Detailed File Share' is set to include 'Failure'

Proof This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1637913: PASS

Based on the following 1 results:
1.
1. At least one specified Audit Event Policy Subcategories entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
detailed_file_share: AUDIT_FAILURE
2. oval-org.cisecurity.benchmarks.windows_10-def-1637915: FAIL

Based on the following 1 results:
1.
1. At least one specified Audit Event Policy Subcategories entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
FAIL
detailed_file_share: AUDIT_FAILURE

17.6.2. (L1) Ensure 'Audit File Share' is set to 'Success and Failure'

Proof
Based on the following 1 results:

1.
1. At least one specified Audit Event Policy Subcategories entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
file_share: AUDIT_SUCCESS_FAILURE

17.6.3. (L1) Ensure 'Audit Other Object Access Events' is set to 'Success and Failure'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637923: PASS

Based on the following 1 results:

1.
    1. At least one specified Audit Event Policy Subcategories entry must match the given criteria.

At least one evaluation must pass.
Entry 1 findings:
PASS
other_object_access_events: AUDIT_SUCCESS_FAILURE

17.6.4. (L1) Ensure 'Audit Removable Storage' is set to 'Success and Failure'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637926: PASS

Based on the following 1 results:

1.
    1. At least one specified Audit Event Policy Subcategories entry must match the given criteria.

At least one evaluation must pass.
Entry 1 findings:
PASS
removable_storage: AUDIT_SUCCESS_FAILURE

17.7.1. (L1) Ensure 'Audit Audit Policy Change' is set to include 'Success'

Proof This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1637930: PASS

Based on the following 1 results:

1.
    1. At least one specified Audit Event Policy Subcategories entry must match the given criteria.

At least one evaluation must pass.
Entry 1 findings:
PASS
audit_policy_change: AUDIT_SUCCESS
2. oval-org.cisecurity.benchmarks.windows_10-def-1637933: FAIL

Based on the following 1 results:

1.
    1. At least one specified Audit Event Policy Subcategories entry must match the given criteria.

At least one evaluation must pass.
Entry 1 findings:
FAIL
audit_policy_change: AUDIT_SUCCESS

17.7.2. (L1) Ensure 'Audit Authentication Policy Change' is set to include 'Success'

Proof This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1637936: PASS

Based on the following 1 results:

1.
    1. At least one specified Audit Event Policy Subcategories entry must match the given criteria.

At least one evaluation must pass.

Entry 1 findings:
PASS
authentication_policy_change: AUDIT_SUCCESS
2. oval-org.cisecurity.benchmarks.windows_10-def-1637939: FAIL

Based on the following 1 results:
1.
1. At least one specified Audit Event Policy Subcategories entry must match the given criteria.
At least one evaluation must pass.
Entry 1 findings:
FAIL
authentication_policy_change: AUDIT_SUCCESS

17.7.3. (L1) Ensure 'Audit Authorization Policy Change' is set to include 'Success'

Proof This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1637943: PASS

Based on the following 1 results:
1.
1. At least one specified Audit Event Policy Subcategories entry must match the given criteria.
At least one evaluation must pass.
Entry 1 findings:
PASS
authorization_policy_change: AUDIT_SUCCESS
2. oval-org.cisecurity.benchmarks.windows_10-def-1637946: FAIL

Based on the following 1 results:
1.
1. At least one specified Audit Event Policy Subcategories entry must match the given criteria.
At least one evaluation must pass.
Entry 1 findings:
FAIL
authorization_policy_change: AUDIT_SUCCESS

17.7.4. (L1) Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637948: PASS

Based on the following 1 results:
1.
1. At least one specified Audit Event Policy Subcategories entry must match the given criteria.
At least one evaluation must pass.
Entry 1 findings:
PASS
mpssvc_rule_level_policy_change: AUDIT_SUCCESS_FAILURE

17.7.5. (L1) Ensure 'Audit Other Policy Change Events' is set to include 'Failure'

Proof This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1637952: PASS

Based on the following 1 results:

1.
    1. At least one specified Audit Event Policy Subcategories entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
other_policy_change_events: AUDIT_FAILURE
2. oval-org.cisecurity.benchmarks.windows_10-def-1637955: FAIL

Based on the following 1 results:

1.
    1. At least one specified Audit Event Policy Subcategories entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
FAIL
other_policy_change_events: AUDIT_FAILURE

17.8.1. (L1) Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637958: PASS

Based on the following 1 results:

1.
    1. At least one specified Audit Event Policy Subcategories entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
sensitive_privilege_use: AUDIT_SUCCESS_FAILURE

17.9.1. (L1) Ensure 'Audit IPsec Driver' is set to 'Success and Failure'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637963: PASS

Based on the following 1 results:

1.
    1. At least one specified Audit Event Policy Subcategories entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
ipsec_driver: AUDIT_SUCCESS_FAILURE

17.9.2. (L1) Ensure 'Audit Other System Events' is set to 'Success and Failure'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637966: PASS

Based on the following 1 results:

1.

1. At least one specified Audit Event Policy Subcategories entry must match the given criteria.

At least one evaluation must pass.
Entry 1 findings:
PASS
other_system_events: AUDIT_SUCCESS_FAILURE

17.9.3. (L1) Ensure 'Audit Security State Change' is set to include 'Success'

Proof This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1637969: PASS

Based on the following 1 results:
1.
1. At least one specified Audit Event Policy Subcategories entry must match the given criteria.

At least one evaluation must pass.
Entry 1 findings:
PASS
security_state_change: AUDIT_SUCCESS
2. oval-org.cisecurity.benchmarks.windows_10-def-1637971: FAIL

Based on the following 1 results:
1.
1. At least one specified Audit Event Policy Subcategories entry must match the given criteria.

At least one evaluation must pass.
Entry 1 findings:
FAIL
security_state_change: AUDIT_SUCCESS

17.9.4. (L1) Ensure 'Audit Security System Extension' is set to include 'Success'

Proof This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1637974: PASS

Based on the following 1 results:
1.
1. At least one specified Audit Event Policy Subcategories entry must match the given criteria.

At least one evaluation must pass.
Entry 1 findings:
PASS
security_system_extension: AUDIT_SUCCESS
2. oval-org.cisecurity.benchmarks.windows_10-def-1637976: FAIL

Based on the following 1 results:
1.
1. At least one specified Audit Event Policy Subcategories entry must match the given criteria.

At least one evaluation must pass.
Entry 1 findings:
FAIL
security_system_extension: AUDIT_SUCCESS

17.9.5. (L1) Ensure 'Audit System Integrity' is set to 'Success and Failure'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637978: PASS

Based on the following 1 results:

1.
    1. At least one specified Audit Event Policy Subcategories entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
system_integrity: AUDIT_SUCCESS_FAILURE

18.1.1.1. (L1) Ensure 'Prevent enabling lock screen camera' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637907: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\Personalization
name: NoLockScreenCamera
type: reg_dword
value: 1

18.1.1.2. (L1) Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637912: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\Personalization
name: NoLockScreenSlideshow
type: reg_dword
value: 1

18.1.2.2. (L1) Ensure 'Allow users to enable online speech recognition services' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637917: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\InputPersonalization
name: AllowInputPersonalization
type: reg_dword
value: 0

18.3.2. (L1) Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637970: PASS

Based on the following 1 results:
1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\mrxsmb10
name: Start
type: reg_dword
value: 4

18.3.3. (L1) Ensure 'Configure SMB v1 server' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637975: PASS

Based on the following 1 results:
1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
name: SMB1
type: reg_dword
value: 0

18.3.4. (L1) Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637979: PASS

Based on the following 1 results:
1.

1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Control\Session Manager\kernel
name: DisableExceptionChainValidation
type: reg_dword
value: 0

18.3.5. (L1) Ensure 'NetBT NodeType configuration' is set to 'Enabled: P-node (recommended)'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637982: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\NetBT\Parameters
name: NodeType
type: reg_dword
value: 2

18.3.6. (L1) Ensure 'WDigest Authentication' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637984: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest
name: UseLogonCredential
type: reg_dword
value: 0

18.4.1. (L1) Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637986: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
name: AutoAdminLogon
type: reg_sz
value: 0

2. oval-org.cisecurity.benchmarks.windows_10-def-1637989: PASS

Based on the following 1 results:

1.
    1. The specified Windows registry information entry must not match the given criteria. The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
name: DefaultPassword

18.4.2. (L1) Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637991: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Services\Tcpip6\Parameters
name: DisableIPSourceRouting
type: reg_dword
value: 2

18.4.3. (L1) Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637993: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Services\Tcpip\Parameters
name: DisableIPSourceRouting
type: reg_dword
value: 2

18.4.5. (L1) Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637999: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Services\Tcpip\Parameters
name: EnableICMPRedirect
type: reg_dword
value: 0

18.4.7. (L1) Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638003: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: System\CurrentControlSet\Services\NetBT\Parameters
name: NoNameReleaseOnDemand
type: reg_dword
value: 1

18.4.9. (L1) Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638007: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Control\Session Manager
name: SafeDllSearchMode
type: reg_dword
value: 1

18.4.10. (L1) Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638009: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Microsoft\Windows NT\CurrentVersion\Winlogon
name: ScreenSaverGracePeriod
type: reg_sz
value: 5

18.4.13. (L1) Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638015: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SYSTEM\CurrentControlSet\Services\Eventlog\Security
name: WarningLevel
type: reg_dword
value: 90

18.5.4.1. (L1) Ensure 'Turn off multicast name resolution' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638017: PASS

Based on the following 1 results:

1.
    1. Any number of Windows registry information entries may match the given criteria.At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows NT\DNSClient
name: EnableMulticast
type: reg_dword
value: 0

18.5.8.1. (L1) Ensure 'Enable insecure guest logons' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638021: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\LanmanWorkstation
name: AllowInsecureGuestAuth
type: reg_dword
value: 0

18.5.11.2. (L1) Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638039: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\Network Connections
name: NC_AllowNetBridge_NLA
type: reg_dword
value: 0

18.5.11.3. (L1) Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled'

Proof

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\Network Connections
name: NC_ShowSharedAccessUI
type: reg_dword
value: 0

18.5.14.1. (L1) Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638045: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths
name: *\NETLOGON
type: reg_sz
value: RequireMutualAuthentication=1, RequireIntegrity=1
2. oval-org.cisecurity.benchmarks.windows_10-def-1638047: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths
name: *\SYSVOL
type: reg_sz
value: RequireMutualAuthentication=1, RequireIntegrity=1

18.5.21.1. (L1) Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled: 3 = Prevent Wi-Fi when on Ethernet'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638062: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\WcmSvc\GroupPolicy
name: fMinimizeConnections
type: reg_dword
value: 3

18.5.23.2.1. (L1) Ensure 'Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638066: PASS

Based on the following 1 results:
1.
1. All specified Windows registry information entries must match the given

criteria.At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Microsoft\WcmSvc\wifinetworkmanager\config
name: AutoConnectAllowedOEM
type: reg_dword
value: 0

18.8.4.1. (L1) Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients'

Proof

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\CredSSP\Parameters
name: AllowEncryptionOracle
type: reg_dword
value: 0

18.8.4.2. (L1) Ensure 'Remote host allows delegation of non-exportable credentials' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638071: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\CredentialsDelegation
name: AllowProtectedCreds
type: reg_dword
value: 1

18.8.14.1. (L1) Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638087: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE

key: System\CurrentControlSet\Policies\EarlyLaunch
name: DriverLoadPolicy
type: reg_dword
value: 3

18.8.21.4. (L1) Ensure 'Continue experiences on this device' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638090: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\System
name: EnableCdp
type: reg_dword
value: 0

18.8.21.5. (L1) Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638091: PASS

Based on the following 1 results:
1.
1. The specified Windows registry information entry must not match the given criteria.
The specified Windows registry information entry was not found based on the given criteria:
hive: HKEY_LOCAL_MACHINE
key: Software\Microsoft\Windows\CurrentVersion\Policies\System
name: DisableBkGndGroupPolicy

18.8.22.1.2. (L1) Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638093: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows NT\Printers
name: DisableWebPnPDownload
type: reg_dword
value: 1

18.8.22.1.6. (L1) Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638097: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
name: NoWebServices
type: reg_dword
value: 1

18.8.28.1. (L1) Ensure 'Block user from showing account details on sign-in' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638111: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\System
name: BlockUserFromShowingAccountDetailsOnSignin
type: reg_dword
value: 1

18.8.28.2. (L1) Ensure 'Do not display network selection UI' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638112: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\System
name: DontDisplayNetworkSelectionUI
type: reg_dword
value: 1

18.8.28.5. (L1) Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638115: PASS

Based on the following 1 results:

1.

1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\System
name: DisableLockScreenAppNotifications
type: reg_dword
value: 1

18.8.28.7. (L1) Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638117: PASS

Based on the following 1 results:

1.

1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\System
name: AllowDomainPINLogon
type: reg_dword
value: 0

18.8.34.6.1. (L1) Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638120: PASS

Based on the following 1 results:

1.

1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Power\PowerSettings\f15576e8-98b7-4186-b944-eafa664402d9
name: DCSettingIndex
type: reg_dword
value: 0

18.8.34.6.2. (L1) Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638121: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Power\PowerSettings\f15576e8-98b7-4186-b944-eafa664402d9
name: ACSettingIndex
type: reg_dword
value: 0

18.8.34.6.5. (L1) Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638124: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Power\PowerSettings\0e796bdb-100d-47d6-a2d5-f7d2daa51f51
name: DCSettingIndex
type: reg_dword
value: 1

18.8.34.6.6. (L1) Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638125: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Power\PowerSettings\0e796bdb-100d-47d6-a2d5-f7d2daa51f51
name: ACSettingIndex
type: reg_dword

value: 1

18.8.36.1. (L1) Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638126: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\policies\Microsoft\Windows NT\Terminal Services
name: fAllowUnsolicited
type: reg_dword
value: 0

18.8.36.2. (L1) Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638127: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\policies\Microsoft\Windows NT\Terminal Services
name: fAllowToGetHelp
type: reg_dword
value: 0

18.8.37.1. (L1) Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638128: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows NT\Rpc
name: EnableAuthEpResolution
type: reg_dword
value: 1

18.8.37.2. (L1) Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638129: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows NT\Rpc
name: RestrictRemoteClients
type: reg_dword
value: 1

18.9.4.2. (L1) Ensure 'Prevent non-admin users from installing packaged Windows apps' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638136: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\Appx
name: BlockNonAdminUserInstall
type: reg_dword
value: 1

18.9.5.1. (L1) Ensure 'Let Windows apps activate with voice while the system is locked' is set to 'Enabled: Force Deny'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638137: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\AppPrivacy
name: LetAppsActivateWithVoiceAboveLock
type: reg_dword
value: 2

18.9.6.1. (L1) Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638138: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Microsoft\Windows\CurrentVersion\Policies\System
name: MSAOptional
type: reg_dword
value: 1

18.9.8.1. (L1) Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638140: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\Explorer
name: NoAutoplayfornonVolume
type: reg_dword
value: 1

18.9.8.2. (L1) Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638141: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer
name: NoAutorun
type: reg_dword
value: 1

18.9.8.3. (L1) Ensure 'Turn off Autoplay' is set to 'Enabled: All drives'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638142: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
name: NoDriveTypeAutoRun
type: reg_dword
value: 255

18.9.10.1.1. (L1) Ensure 'Configure enhanced anti-spoofing' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638143: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Biometrics\FacialFeatures
name: EnhancedAntiSpoofing
type: reg_dword
value: 1

18.9.13.2. (L1) Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638198: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\CloudContent
name: DisableWindowsConsumerFeatures
type: reg_dword
value: 1

18.9.14.1. (L1) Ensure 'Require pin for pairing' is set to 'Enabled: First Time' OR 'Enabled: Always'

Proof This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1638199: FAIL

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
FAIL
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\Connect
name: RequirePinForPairing
type: reg_dword
value: 2
2. oval-org.cisecurity.benchmarks.windows_10-def-1638200: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\Connect
name: RequirePinForPairing
type: reg_dword
value: 2

18.9.15.1. (L1) Ensure 'Do not display the password reveal button' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638201: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\CredUI
name: DisablePasswordReveal
type: reg_dword
value: 1

18.9.15.2. (L1) Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638202: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Microsoft\Windows\CurrentVersion\Policies\CredUI
name: EnumerateAdministrators
type: reg_dword
value: 0

18.9.15.3. (L1) Ensure 'Prevent the use of security questions for local accounts' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638203: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\System
name: NoLocalPasswordResetQuestions
type: reg_dword
value: 1

18.9.16.1. (L1) Ensure 'Allow Telemetry' is set to 'Enabled: 0 - Security [Enterprise Only]' or 'Enabled: 1 - Basic'

Proof This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1638204: FAIL

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
FAIL
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\DataCollection
name: AllowTelemetry
type: reg_dword
value: 1
2. oval-org.cisecurity.benchmarks.windows_10-def-1638205: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\DataCollection

name: AllowTelemetry
type: reg_dword
value: 1

18.9.16.3. (L1) Ensure 'Do not show feedback notifications' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638207: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\DataCollection
name: DoNotShowFeedbackNotifications
type: reg_dword
value: 1

18.9.16.4. (L1) Ensure 'Toggle user control over Insider builds' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638208: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\PreviewBuilds
name: AllowBuildPreview
type: reg_dword
value: 0

18.9.17.1. (L1) Ensure 'Download Mode' is NOT set to 'Enabled: Internet'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638209: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\DeliveryOptimization
name: DODownloadMode
type: reg_dword

value: 1

18.9.26.1.1. (L1) Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638210: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\EventLog\Application
name: Retention
type: reg_sz
value: 0

18.9.26.1.2. (L1) Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638211: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\EventLog\Application
name: MaxSize
type: reg_dword
value: 32768

18.9.26.2.1. (L1) Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638212: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\EventLog\Security
name: Retention
type: reg_sz
value: 0

18.9.26.2.2. (L1) Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638213: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\EventLog\Security
name: MaxSize
type: reg_dword
value: 196608

18.9.26.3.1. (L1) Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638214: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\EventLog\Setup
name: Retention
type: reg_sz
value: 0

18.9.26.3.2. (L1) Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638215: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\EventLog\Setup
name: MaxSize
type: reg_dword
value: 32768

18.9.26.4.1. (L1) Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638216: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\EventLog\System
name: Retention
type: reg_sz
value: 0

18.9.26.4.2. (L1) Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638217: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\EventLog\System
name: MaxSize
type: reg_dword
value: 32768

18.9.30.2. (L1) Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638218: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\Explorer
name: NoDataExecutionPrevention
type: reg_dword
value: 0

18.9.30.3. (L1) Ensure 'Turn off heap termination on corruption' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638219: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\Explorer
name: NoHeapTerminationOnCorruption
type: reg_dword
value: 0

18.9.30.4. (L1) Ensure 'Turn off shell protocol protected mode' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638220: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
name: PreXPSP2ShellProtocolBehavior
type: reg_dword
value: 0

18.9.35.1. (L1) Ensure 'Prevent the computer from joining a homegroup' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638221: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\HomeGroup
name: DisableHomeGroup
type: reg_dword
value: 1

18.9.44.1. (L1) Ensure 'Block all consumer Microsoft account user authentication' is set to 'Enabled'

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638224: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\MicrosoftAccount
name: DisableUserAuth
type: reg_dword
value: 1

18.9.45.3.1. (L1) Ensure 'Configure local setting override for reporting to Microsoft MAPS' is set to 'Disabled'

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638225: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows Defender\Spynet
name: LocalSettingOverrideSpynetReporting
type: reg_dword
value: 0

18.9.45.4.1.1. (L1) Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled'

Proof

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR
name: ExploitGuard_ASR_Rules
type: reg_dword
value: 1

18.9.45.4.1.2. (L1) Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is configured

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638240: PASS

Based on the following 1 results:

1.

1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules
name: e6db77e5-3df2-4cf1-b95a-636979351e5b
type: reg_sz
value: 1

2.

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638239: PASS

Based on the following 1 results:

1.

1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules
name: d4f940ab-401b-4efc-aadc-ad5f3c50688a
type: reg_sz
value: 1

2.

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638238: PASS

Based on the following 1 results:

1.

1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules
name: d3e037e1-3eb8-44c8-a917-57927947596d
type: reg_sz
value: 1

2.

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638237: PASS

Based on the following 1 results:

1.

1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE

key: SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules
name: be9ba2d9-53ea-4cdc-84e5-9b1eeee46550
type: reg_sz
value: 1
2.
This is a complex check. Operator = AND
1. oval-org.cisecurity.benchmarks.windows_10-def-1638236: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules
name: b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4
type: reg_sz
value: 1
2.
This is a complex check. Operator = AND
1. oval-org.cisecurity.benchmarks.windows_10-def-1638235: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules
name: 9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2
type: reg_sz
value: 1
2.
This is a complex check. Operator = AND
1. oval-org.cisecurity.benchmarks.windows_10-def-1638234: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules
name: 92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b
type: reg_sz
value: 1
2.
This is a complex check. Operator = AND
1. oval-org.cisecurity.benchmarks.windows_10-def-1638233: PASS

Based on the following 1 results:
1.

1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules
name: 7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c
type: reg_sz
value: 1

2.
This is a complex check. Operator = AND
1. oval-org.cisecurity.benchmarks.windows_10-def-1638232: PASS

Based on the following 1 results:

1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules
name: 75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84
type: reg_sz
value: 1

2.
This is a complex check. Operator = AND
1. oval-org.cisecurity.benchmarks.windows_10-def-1638231: PASS

Based on the following 1 results:

1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules
name: 5beb7efe-fd9a-4556-801d-275e5ffc04cc
type: reg_sz
value: 1

2.
This is a complex check. Operator = AND
1. oval-org.cisecurity.benchmarks.windows_10-def-1638229: PASS

Based on the following 1 results:

1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules
name: 26190899-1602-49e8-8b27-eb1d0a1ce869
type: reg_sz
value: 1

2. oval-org.cisecurity.benchmarks.windows_10-def-1638230: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules
name: 3b576869-a4ec-4529-8536-b80a7769e899
type: reg_sz
value: 1

18.9.45.4.3.1. (L1) Ensure 'Prevent users and apps from accessing dangerous websites' is set to 'Enabled: Block'

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638241: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\Network Protection
name: EnableNetworkProtection
type: reg_dword
value: 1

18.9.45.8.1. (L1) Ensure 'Scan all downloaded files and attachments' is set to 'Enabled'

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638243: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection
name: DisableIOAVProtection
type: reg_dword
value: 0

18.9.45.8.2. (L1) Ensure 'Turn off real-time protection' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638244: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection
name: DisableRealtimeMonitoring
type: reg_dword
value: 0

18.9.45.8.3. (L1) Ensure 'Turn on behavior monitoring' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638245: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection
name: DisableBehaviorMonitoring
type: reg_dword
value: 0

18.9.45.11.1. (L1) Ensure 'Scan removable drives' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638247: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows Defender\Scan
name: DisableRemovableDriveScanning
type: reg_dword
value: 0

18.9.45.11.2. (L1) Ensure 'Turn on e-mail scanning' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638248: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows Defender\Scan
name: DisableEmailScanning
type: reg_dword
value: 0

18.9.45.14. (L1) Ensure 'Configure detection for potentially unwanted applications' is set to 'Enabled: Block'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638249: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows Defender
name: PUAProtection
type: reg_dword
value: 1

18.9.45.15. (L1) Ensure 'Turn off Microsoft Defender AntiVirus' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638250: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows Defender
name: DisableAntiSpyware
type: reg_dword
value: 0

18.9.55.1. (L1) Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638270: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\OneDrive
name: DisableFileSyncNGSC
type: reg_dword
value: 1

18.9.62.2.2. (L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638272: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services
name: DisablePasswordSaving
type: reg_dword
value: 1

18.9.62.3.3.2. (L1) Ensure 'Do not allow drive redirection' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638275: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services
name: fDisableCdm
type: reg_dword
value: 1

18.9.62.3.9.1. (L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638278: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services
name: fPromptForPassword
type: reg_dword
value: 1

18.9.62.3.9.2. (L1) Ensure 'Require secure RPC communication' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638279: PASS

Based on the following 1 results:
1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows NT\Terminal Services
name: fEncryptRPCTraffic
type: reg_dword
value: 1

18.9.62.3.9.3. (L1) Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL'

Proof
Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services
name: SecurityLayer
type: reg_dword
value: 2

18.9.62.3.9.4. (L1) Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled'

Proof
Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services

name: UserAuthentication
type: reg_dword
value: 1

18.9.62.3.9.5. (L1) Ensure 'Set client connection encryption level' is set to 'Enabled: High Level'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638282: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services
name: MinEncryptionLevel
type: reg_dword
value: 3

18.9.62.3.11.1. (L1) Ensure 'Do not delete temp folders upon exit' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638286: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services
name: DeleteTempDirsOnExit
type: reg_dword
value: 1

18.9.63.1. (L1) Ensure 'Prevent downloading of enclosures' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638287: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Internet Explorer\Feeds
name: DisableEnclosureDownload
type: reg_dword

value: 1

18.9.64.3. (L1) Ensure 'Allow Cortana' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638290: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\Windows Search
name: AllowCortana
type: reg_dword
value: 0

18.9.64.4. (L1) Ensure 'Allow Cortana above lock screen' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638291: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\Windows Search
name: AllowCortanaAboveLock
type: reg_dword
value: 0

18.9.64.5. (L1) Ensure 'Allow indexing of encrypted files' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638292: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\Windows Search
name: AllowIndexingEncryptedStoresOrItems
type: reg_dword
value: 0

18.9.64.6. (L1) Ensure 'Allow search and Cortana to use location' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638293: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\Windows Search
name: AllowSearchToUseLocation
type: reg_dword
value: 0

18.9.72.2. (L1) Ensure 'Only display the private store within the Microsoft Store' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638296: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\WindowsStore
name: RequirePrivateStoreOnly
type: reg_dword
value: 1

18.9.72.3. (L1) Ensure 'Turn off Automatic Download and Install of updates' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638297: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\WindowsStore
name: AutoDownload
type: reg_dword
value: 4

18.9.72.4. (L1) Ensure 'Turn off the offer to update to the latest version of Windows' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638298: PASS

Based on the following 1 results:

1.

1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\WindowsStore
name: DisableOSUpgrade
type: reg_dword
value: 1

18.9.80.1.1. (L1) Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638301: PASS

Based on the following 1 results:

1.

1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\System
name: ShellSmartScreenLevel
type: reg_sz
value: Block

2. oval-org.cisecurity.benchmarks.windows_10-def-1638300: PASS

Based on the following 1 results:

1.

1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\System
name: EnableSmartScreen
type: reg_dword
value: 1

18.9.80.2.1. (L1) Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638302: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\MicrosoftEdge\PhishingFilter
name: EnabledV9
type: reg_dword
value: 1

18.9.80.2.2. (L1) Ensure 'Prevent bypassing Windows Defender SmartScreen prompts for sites' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638303: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\MicrosoftEdge\PhishingFilter
name: PreventOverride
type: reg_dword
value: 1

18.9.82.1. (L1) Ensure 'Enables or disables Windows Game Recording and Broadcasting' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638304: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\GameDVR
name: AllowGameDVR
type: reg_dword
value: 0

18.9.84.2. (L1) Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Disabled' but not 'Enabled: On'

Proof This is a complex check. Operator = OR

1. oval-org.cisecurity.benchmarks.windows_10-def-1638306: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\WindowsInkWorkspace
name: AllowWindowsInkWorkspace
type: reg_dword
value: 1
2. oval-org.cisecurity.benchmarks.windows_10-def-1638307: FAIL

Based on the following 1 results:
1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
FAIL
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\WindowsInkWorkspace
name: AllowWindowsInkWorkspace
type: reg_dword
value: 1

18.9.85.1. (L1) Ensure 'Allow user control over installs' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638308: PASS

Based on the following 1 results:
1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\Installer
name: EnableUserControl
type: reg_dword
value: 0

18.9.85.2. (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled'

Proof
Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\Installer
name: AlwaysInstallElevated
type: reg_dword
value: 0

18.9.86.1. (L1) Ensure 'Sign-in and lock last interactive user automatically after a restart' is set to 'Disabled'

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638311: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Microsoft\Windows\CurrentVersion\Policies\System
name: DisableAutomaticRestartSignOn
type: reg_dword
value: 1

18.9.95.2. (L1) Ensure 'Turn on PowerShell Transcription' is set to 'Disabled'

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638313: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\PowerShell\Transcription
name: EnableTranscripting
type: reg_dword
value: 0

18.9.97.1.1. (L1) Ensure 'Allow Basic authentication' is set to 'Disabled'

Proof

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\WinRM\Client
name: AllowBasic
type: reg_dword
value: 0

18.9.97.1.2. (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638315: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\WinRM\Client
name: AllowUnencryptedTraffic
type: reg_dword
value: 0

18.9.97.1.3. (L1) Ensure 'Disallow Digest authentication' is set to 'Enabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638316: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\WinRM\Client
name: AllowDigest
type: reg_dword
value: 0

18.9.97.2.1. (L1) Ensure 'Allow Basic authentication' is set to 'Disabled'

Proof

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\WinRM\Service
name: AllowBasic
type: reg_dword
value: 0

18.9.97.2.3. (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638319: PASS

Based on the following 1 results:

1.
    1. All specified Windows registry information entries must match the given criteria.At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\WinRM\Service
name: AllowUnencryptedTraffic
type: reg_dword
value: 0

18.9.97.2.4. (L1) Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled'

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638320: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\WinRM\Service
name: DisableRunAs
type: reg_dword
value: 1

18.9.99.2.1. (L1) Ensure 'Prevent users from modifying settings' is set to 'Enabled'

Proof

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows Defender Security Center\App and Browser protection
name: DisallowExploitProtectionOverride
type: reg_dword
value: 1

18.9.102.1.3. (L1) Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days'

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638328: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate
name: DeferQualityUpdates
type: reg_dword
value: 1

2. oval-org.cisecurity.benchmarks.windows_10-def-1638329: PASS

Based on the following 1 results:

1.

1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate
name: DeferQualityUpdatesPeriodInDays
type: reg_dword
value: 0

18.9.102.2. (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled'

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638330: PASS

Based on the following 1 results:

1.

1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\WindowsUpdate\AU
name: NoAutoUpdate
type: reg_dword
value: 0

18.9.102.3. (L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638331: PASS

Based on the following 1 results:

1.

1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\WindowsUpdate\AU
name: ScheduledInstallDay
type: reg_dword
value: 0

18.9.102.4. (L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled'

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1638332: PASS

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: Software\Policies\Microsoft\Windows\WindowsUpdate\AU
name: NoAutoRebootWithLoggedOnUsers
type: reg_dword
value: 0

18.9.102.5. (L1) Ensure 'Remove access to “Pause updates” feature' is set to 'Enabled'

Proof

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_LOCAL_MACHINE
key: SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate
name: SetDisablePauseUXAccess
type: reg_dword
value: 1

19.1.3.1. (L1) Ensure 'Enable screen saver' is set to 'Enabled'

Proof

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.

Entry 1 findings:
PASS
hive: HKEY_USERS
key: S-1-5-21-3293848366-2354669173-3456164447-1001\Software\Policies\Microsoft\Windows\Control Panel\Desktop
name: ScreenSaveActive
type: reg_sz
value: 1

19.1.3.2. (L1) Ensure 'Password protect the screen saver' is set to 'Enabled'

Proof

Based on the following 1 results:

1.

1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_USERS
key: S-1-5-21-3293848366-2354669173-3456164447-1001\Software\Policies\Microsoft\Windows\Control Panel\Desktop
name: ScreenSaverIsSecure
type: reg_sz
value: 1

19.1.3.3. (L1) Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0'

Proof

This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637929: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_USERS
key: S-1-5-21-3293848366-2354669173-3456164447-1001\Software\Policies\Microsoft\Windows\Control Panel\Desktop
name: ScreenSaveTimeOut
type: reg_sz
value: 900
2. oval-org.cisecurity.benchmarks.windows_10-def-1637934: PASS

Based on the following 1 results:
1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_USERS
key: S-1-5-21-3293848366-2354669173-3456164447-1001\Software\Policies\Microsoft\Windows\Control Panel\Desktop
name: ScreenSaveTimeOut
type: reg_sz
value: 900

19.5.1.1. (L1) Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled'

Proof

Based on the following 1 results:

1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_USERS
key: S-1-5-21-3293848366-2354669173-3456164447-1001\Software\Policies\Microsoft\Windows\CurrentVersion\PushNotifications
name: NoToastApplicationNotificationOnLockScreen

type: reg_dword
value: 1

19.7.4.1. (L1) Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled'

Proof

Based on the following 1 results:

1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_USERS
key: S-1-5-21-3293848366-2354669173-3456164447-1001\Software\Microsoft\Windows\CurrentVersion\Policies\Attachments
name: SaveZoneInformation
type: reg_dword
value: 2

19.7.4.2. (L1) Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled'

Proof

Based on the following 1 results:

1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_USERS
key: S-1-5-21-3293848366-2354669173-3456164447-1001\Software\Microsoft\Windows\CurrentVersion\Policies\Attachments
name: ScanWithAntiVirus
type: reg_dword
value: 3

19.7.8.1. (L1) Ensure 'Configure Windows spotlight on lock screen' is set to Disabled'

Proof

Based on the following 1 results:

1.
1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_USERS
key: S-1-5-21-3293848366-2354669173-3456164447-1001\Software\Policies\Microsoft\Windows\CloudContent
name: ConfigureWindowsSpotlight
type: reg_dword
value: 2

19.7.8.2. (L1) Ensure 'Do not suggest third-party content in Windows spotlight' is set to 'Enabled'

Proof

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_USERS
key: S-1-5-21-3293848366-2354669173-3456164447-1001\Software\Policies\Microsoft\Windows\CloudContent
name: DisableThirdPartySuggestions
type: reg_dword
value: 1

19.7.28.1. (L1) Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled'

Proof

Based on the following 1 results:

1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_USERS
key: S-1-5-21-3293848366-2354669173-3456164447-1001\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
name: NoInplaceSharing
type: reg_dword
value: 1

19.7.43.1. (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled'

Proof This is a complex check. Operator = AND

1. oval-org.cisecurity.benchmarks.windows_10-def-1637994: PASS

Based on the following 1 results:
1.
    1. At least one specified Windows registry information entry must match the given criteria. At least one evaluation must pass.
Entry 1 findings:
PASS
hive: HKEY_USERS
key: S-1-5-21-3293848366-2354669173-3456164447-1001\Software\Policies\Microsoft\Windows\Installer
name: AlwaysInstallElevated
type: reg_dword
value: 0