hardeningkitty_report_tfm-vm-c1_finding_list_0x6d69636b_machine-20250818-102813 - medium

ID	Category	Name	Severity	Result	Recommended	TestResult	SeverityFinding
1104	Account Policies	Allow Administrator account lockout	Passed	1	1	Passed	Medium
1200	User Rights Assignment	Access this computer from the network	Medium	Todos;BUILTIN\Administradores;BUILTIN\Usuarios;BUILTIN\Operadores de copia de seguridad	BUILTIN\Administrators	Failed	Medium
1201	User Rights Assignment	Allow log on locally	Medium	Invitado;BUILTIN\Administradores;BUILTIN\Usuarios;BUILTIN\Operadores de copia de seguridad	BUILTIN\Users;BUILTIN\Administrators	Failed	Medium
1202	User Rights Assignment	Debug programs	Medium	BUILTIN\Administradores		Failed	Medium
1203	User Rights Assignment	Deny access to this computer from the network	Medium	Invitado	BUILTIN\Guests;NT AUTHORITY\Local account	Failed	Medium
1204	User Rights Assignment	Deny log on as a batch job	Medium		BUILTIN\Guests	Failed	Medium
1205	User Rights Assignment	Deny log on as a service	Medium		BUILTIN\Guests	Failed	Medium
1206	User Rights Assignment	Deny log on through Remote Desktop Services	Medium		BUILTIN\Guests;NT AUTHORITY\Local account	Failed	Medium
1305	Security Options	Microsoft network client: Digitally sign communications (always)	Medium	0	1	Failed	Medium
1306	Security Options	Microsoft network client: Digitally sign communications (if server agrees)	Passed	1	1	Passed	Medium
1307	Security Options	Microsoft network server: Digitally sign communications (always)	Medium	0	1	Failed	Medium
1308	Security Options	Microsoft network server: Digitally sign communications (if client agrees)	Medium	0	1	Failed	Medium
1309	Security Options	Network access: Do not allow anonymous enumeration of SAM accounts	Passed	1	1	Passed	Medium
1310	Security Options	Network access: Do not allow anonymous enumeration of SAM accounts and shares	Medium	0	1	Failed	Medium
1311	Security Options	Network access: Do not allow storage of passwords and credentials for network authentication	Medium	0	1	Failed	Medium
1324	Security Options	Network access: Restrict anonymous access to Named Pipes and Shares	Passed	1	1	Passed	Medium
1325	Security Options	Network access: Restrict clients allowed to make remote calls to SAM	Medium		O:BAG:BAD:(A;;RC;;;BA)	Failed	Medium
1312	Security Options	Network security: Allow LocalSystem NULL session fallback	Passed	0	0	Passed	Medium
1313	Security Options	Network security: LAN Manager authentication level	Medium	3	5	Failed	Medium
1314	Security Options	Network security: LDAP client signing requirements	Passed	1	1	Passed	Medium
1315	Security Options	Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Medium	536870912	537395200	Failed	Medium
1316	Security Options	Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Medium	536870912	537395200	Failed	Medium
1317	Security Options	Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Medium	0	2	Failed	Medium
1318	Security Options	Network security: Restrict NTLM: Audit NTLM authentication in this domain	Medium	0	7	Failed	Medium
1319	Security Options	Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Medium	0	1	Failed	Medium
1320	Security Options	Shutdown: Allow system to be shut down without having to log on	Medium	1	0	Failed	Medium
1321	Security Options	User Account Control: Admin Approval Mode for the Built-in Administrator account	Medium	0	1	Failed	Medium
1322	Security Options	User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Medium	5	2	Failed	Medium
1323	Security Options	User Account Control: Behavior of the elevation prompt for standard users	Medium	3	1	Failed	Medium
1400	Windows Firewall	EnableFirewall (Domain Profile, Policy)	Medium	0	1	Failed	Medium
1418	Windows Firewall	EnableFirewall (Domain Profile)	Passed	1	1	Passed	Medium
1401	Windows Firewall	Inbound Connections (Domain Profile, Policy)	Passed	1	1	Passed	Medium
1419	Windows Firewall	Inbound Connections (Domain Profile)	Passed	1	1	Passed	Medium
1402	Windows Firewall	Outbound Connections (Domain Profile, Policy)	Passed	0	0	Passed	Medium
1420	Windows Firewall	Outbound Connections (Domain Profile)	Passed	0	0	Passed	Medium
1403	Windows Firewall	Log size limit (Domain Profile, Policy)	Medium	4096	16384	Failed	Medium
1421	Windows Firewall	Log size limit (Domain Profile)	Medium	4096	16384	Failed	Medium
1404	Windows Firewall	Log dropped packets (Domain Profile, Policy)	Medium	0	1	Failed	Medium
1422	Windows Firewall	Log dropped packets (Domain Profile)	Medium	0	1	Failed	Medium
1406	Windows Firewall	EnableFirewall (Private Profile, Policy)	Medium	0	1	Failed	Medium
1424	Windows Firewall	EnableFirewall (Private Profile)	Passed	1	1	Passed	Medium
1407	Windows Firewall	Inbound Connections (Private Profile, Policy)	Passed	1	1	Passed	Medium
1425	Windows Firewall	Inbound Connections (Private Profile)	Passed	1	1	Passed	Medium
1408	Windows Firewall	Outbound Connections (Private Profile, Policy)	Passed	0	0	Passed	Medium
1426	Windows Firewall	Outbound Connections (Private Profile)	Passed	0	0	Passed	Medium
1409	Windows Firewall	Log size limit (Private Profile, Policy)	Medium	4096	16384	Failed	Medium
1427	Windows Firewall	Log size limit (Private Profile)	Medium	4096	16384	Failed	Medium
1410	Windows Firewall	Log dropped packets (Private Profile, Policy)	Medium	0	1	Failed	Medium
1428	Windows Firewall	Log dropped packets (Private Profile)	Medium	0	1	Failed	Medium
1412	Windows Firewall	EnableFirewall (Public Profile, Policy)	Medium	0	1	Failed	Medium
1430	Windows Firewall	EnableFirewall (Public Profile)	Passed	1	1	Passed	Medium
1413	Windows Firewall	Inbound Connections (Public Profile, Policy)	Passed	1	1	Passed	Medium
1431	Windows Firewall	Inbound Connections (Public Profile)	Passed	1	1	Passed	Medium
1414	Windows Firewall	Outbound Connections (Public Profile, Policy)	Passed	0	0	Passed	Medium
1432	Windows Firewall	Outbound Connections (Public Profile)	Passed	0	0	Passed	Medium

1415	Windows Firewall	Log size limit (Public Profile, Policy)	Medium	4096	16384	Failed	Medium
1433	Windows Firewall	Log size limit (Public Profile)	Medium	4096	16384	Failed	Medium
1416	Windows Firewall	Log dropped packets (Public Profile, Policy)	Medium	0	1	Failed	Medium
1434	Windows Firewall	Log dropped packets (Public Profile)	Medium	0	1	Failed	Medium
1601	Administrative Templates: Network	DNS Client: Turn off multicast name resolution (LLMNR)	Medium	1	0	Failed	Medium
1602	Administrative Templates: Network	Lanman Workstation: Enable insecure guest logons	Medium	1	0	Failed	Medium
1603	Administrative Templates: Network	Turn off Microsoft Peer-to-Peer Networking Services	Medium	0	1	Failed	Medium
1604	Administrative Templates: Network	WLAN Settings: Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services	Medium	1	0	Failed	Medium
2111	Administrative Templates: PowerSh	Turn on PowerShell Script Block Logging	Medium	0	1	Failed	Medium
2115	Administrative Templates: PowerSh	Turn on PowerShell Transcription (PowerShell Policy)	Medium	0	1	Failed	Medium
1772	Administrative Templates: Printers	Configure Redirection Guard	Medium		1	Failed	Medium
1768	Administrative Templates: Printers	Only use Package Point and Print (CVE-2021-36958)	Medium		1	Failed	Medium
1769	Administrative Templates: Printers	Package Point and Print - Approved servers (CVE-2021-36958)	Medium		1	Failed	Medium
1771	Administrative Templates: Start Me	Notifications: Turn off notifications network usage	Medium	0	1	Failed	Medium
1605	Administrative Templates: System	Credentials Delegation: Allow delegation default credentials	Medium	1	0	Failed	Medium
1606	Administrative Templates: System	Credentials Delegation: Encryption Oracle Remediation	Passed	0	0	Passed	Medium
1699	Administrative Templates: System	Credentials Delegation: Remote host allows delegation of non-exportable credentials	Medium	0	1	Failed	Medium
1607	Administrative Templates: System	Device Installation: Device Installation Restrictions: Prevent installation of devices that match an ID	Medium	0	1	Failed	Medium
1608	Administrative Templates: System	Device Installation: Device Installation Restrictions: Prevent installation of devices that match an ID (Retroactive)	Medium	0	1	Failed	Medium
1609	Administrative Templates: System	Device Installation: Device Installation Restrictions: Prevent installation of devices that match ID PCI\CC_0C0010 (Firewire)	Medium	0	PCI\CC_0C0010	Failed	Medium
1610	Administrative Templates: System	Device Installation: Device Installation Restrictions: Prevent installation of devices that match ID PCI\CC_0C0A (Thunderbolt)	Medium	0	PCI\CC_0C0A	Failed	Medium
1611	Administrative Templates: System	Device Installation: Device Installation Restrictions: Prevent installation of devices using drivers that match an device setup class	Medium	0	1	Failed	Medium
1612	Administrative Templates: System	Device Installation: Device Installation Restrictions: Prevent installation of devices using drivers that match an device setup class (Retroactive)	Medium	0	1	Failed	Medium
1613	Administrative Templates: System	Device Installation: Device Installation Restrictions: Prevent installation of devices using drivers that match d48179be-ec20-11d1-b6b8-00c04fa372a7 (SBP-2 d	Medium	0	d48179be-ec20-11d1-b6b8-00c04fa372a7	Failed	Medium
1614	Administrative Templates: System	Device Guard: Virtualization Based Security Status	Medium	Not available	2	Failed	Medium
1615	Administrative Templates: System	Device Guard: Available Security Properties: Secure Boot	Passed	2	2	Passed	Medium
1616	Administrative Templates: System	Device Guard: Available Security Properties: DMA protection	Medium	Not available	3	Failed	Medium
1617	Administrative Templates: System	Device Guard: Security Services Configured: Credential Guard	Medium	Not available	1	Failed	Medium
1619	Administrative Templates: System	Device Guard: Security Services Running: Credential Guard	Medium	Not available	1	Failed	Medium
1618	Administrative Templates: System	Device Guard: Security Services Configured: HVCI	Medium	Not available	2	Failed	Medium
1620	Administrative Templates: System	Device Guard: Security Services Running: HVCI	Medium	Not available	2	Failed	Medium
1623	Administrative Templates: System	Device Guard: Require UEFI Memory Attributes Table (Policy)	Medium		1	Failed	Medium
1621	Administrative Templates: System	Device Guard: Secure Launch Configuration (Policy)	Medium	0	1	Failed	Medium
1622	Administrative Templates: System	Device Guard: Windows Defender Application Control deployed (Policy)	Medium	0	1	Failed	Medium
1630	Administrative Templates: System	Early Launch Antimalware: Boot-Start Driver Initialization Policy	Medium	0	3	Failed	Medium
1640	Administrative Templates: System	Internet Communication Management: Internet Communication settings: Turn off the Windows Messenger Customer Experience Improvement Program	Medium	0	2	Failed	Medium
1641	Administrative Templates: System	Internet Communication Management: Internet Communication settings: Turn off downloading of print drivers over HTTP	Medium	0	1	Failed	Medium
1642	Administrative Templates: System	Internet Communication Management: Internet Communication settings: Turn off Windows Error Reporting 1	Medium	1	0	Failed	Medium
1643	Administrative Templates: System	Internet Communication Management: Internet Communication settings: Turn off Windows Error Reporting 2	Medium	0	1	Failed	Medium
1644	Administrative Templates: System	Internet Communication Management: Internet Communication settings: Turn off Internet download for Web publishing and online ordering wizards	Medium	0	1	Failed	Medium
1645	Administrative Templates: System	Internet Communication Management: Internet Communication settings: Turn off Windows Customer Experience Improvement Program	Medium	1	0	Failed	Medium
1650	Administrative Templates: System	Kernel DMA Protection: Enumeration policy for external devices incompatible with Kernel DMA Protection	Medium	2	0	Failed	Medium
1660	Administrative Templates: System	Logon: Turn on convenience PIN sign-in	Medium	1	0	Failed	Medium
1661	Administrative Templates: System	Logon: Turn off app notifications on the lock screen	Medium	0	1	Failed	Medium
1662	Administrative Templates: System	Logon: Do not display network selection UI	Medium	0	1	Failed	Medium
1670	Administrative Templates: System	Mitigation Options: Untrusted Font Blocking	Medium	0	1000000000000	Failed	Medium
1680	Administrative Templates: System	OS Policies: Allow Clipboard synchronization across devices	Medium	1	0	Failed	Medium
1685	Administrative Templates: System	Sleep Settings: Require a password when a computer wakes (plugged in)	Medium	0	1	Failed	Medium
1686	Administrative Templates: System	Sleep Settings: Require a password when a computer wakes (on battery)	Medium	0	1	Failed	Medium
1687	Administrative Templates: System	Sleep Settings: Allow standby states (S1-S3) when sleeping (plugged in)	Medium	1	0	Failed	Medium
1688	Administrative Templates: System	Sleep Settings: Allow standby states (S1-S3) when sleeping (on battery)	Medium	1	0	Failed	Medium
1690	Administrative Templates: System	Remote Assistance: Configure Offer Remote Assistance	Medium	1	0	Failed	Medium
1691	Administrative Templates: System	Remote Assistance: Configure Solicited Remote Assistance	Medium	1	0	Failed	Medium
1692	Administrative Templates: System	Remote Procedure Call: Enable RPC Endpoint Mapper Client Authentication	Medium	0	1	Failed	Medium
1693	Administrative Templates: System	Remote Procedure Call: Restrict Unauthenticated RPC clients	Medium	0	2	Failed	Medium
1694	Administrative Templates: System	Security Settings: Enable svchost.exe mitigation options	Medium	0	1	Failed	Medium
1695	Administrative Templates: System	Windows Performance PerfTrack: Enable/Disable PerfTrack	Medium	1	0	Failed	Medium

1696	Administrative Templates: System	User Profiles: Turn off the advertising ID	Medium	0	1	Failed	Medium
1697	Administrative Templates: System	Time Providers: Enable Windows NTP Client	Medium	0	1	Failed	Medium
1698	Administrative Templates: System	Time Providers: Enable Windows NTP Server	Passed	0	0	Passed	Medium
1700	Administrative Templates: Windows	App Package Deployment: Allow a Windows app to share application data between users	Medium	1	0	Failed	Medium
1701	Administrative Templates: Windows	App Privacy: Let Windows apps activate with voice while the system is locked	Medium	0	2	Failed	Medium
1702	Administrative Templates: Windows	App runtime: Block launching Universal Windows apps with Windows Runtime API access from hosted content	Medium	0	1	Failed	Medium
1703	Administrative Templates: Windows	Application Compatibility: Turn off Application Telemetry	Medium	1	0	Failed	Medium
1704	Administrative Templates: Windows	AutoPlay Policies: Turn off Autoplay	Medium	0	255	Failed	Medium
1705	Administrative Templates: Windows	AutoPlay Policies: Disallow Autoplay for non-volume devices	Medium	0	1	Failed	Medium
1706	Administrative Templates: Windows	AutoPlay Policies: Set the default behavior for AutoRun	Medium	0	1	Failed	Medium
1707	Administrative Templates: Windows	Biometrics: Allow the use of biometrics	Medium	1	0	Failed	Medium
1773	Administrative Templates: Windows	Biometrics: Facial Features: Configure enhanced anti-spoofing	Medium		1	Failed	Medium
1761	Administrative Templates: Windows	BitLocker Drive Encryption: Choose drive encryption method and cipher strength (for operating system drives)	Passed	6	6	Passed	Medium
1762	Administrative Templates: Windows	BitLocker Drive Encryption: Drive encryption method (for operating system drives)	Passed	XtsAes128	XtsAes128	Passed	Medium
1709	Administrative Templates: Windows	BitLocker Drive Encryption: Disable new DMA devices when this computer is locked	Medium	0	1	Failed	Medium
1710	Administrative Templates: Windows	BitLocker Drive Encryption: Operating System Drives: Allow Secure Boot for integrity validation	Medium	0	1	Failed	Medium
1711	Administrative Templates: Windows	BitLocker Drive Encryption: Operating System Drives: Require additional authentication at startup	Medium	0	1	Failed	Medium
1715	Administrative Templates: Windows	BitLocker Drive Encryption: Operating System Drives: Require additional authentication at startup: Allow BitLocker without a compatible TPM	Medium	1	0	Failed	Medium
1716	Administrative Templates: Windows	BitLocker Drive Encryption: Operating System Drives: Require additional authentication at startup: Configure TPM startup	Passed	0	0	Passed	Medium
1717	Administrative Templates: Windows	BitLocker Drive Encryption: Operating System Drives: Require additional authentication at startup: Configure TPM startup PIN	Medium	0	1	Failed	Medium
1718	Administrative Templates: Windows	BitLocker Drive Encryption: Operating System Drives: Require additional authentication at startup: Configure TPM startup key	Passed	0	0	Passed	Medium
1719	Administrative Templates: Windows	BitLocker Drive Encryption: Operating System Drives: Require additional authentication at startup: Configure TPM startup key and PIN	Passed	0	0	Passed	Medium
1712	Administrative Templates: Windows	BitLocker Drive Encryption: Operating System Drives: Allow enhanced PINs for startup	Medium	0	1	Failed	Medium
1713	Administrative Templates: Windows	BitLocker Drive Encryption: Operating System Drives: Configure use of hardware-based encryption for operating system drives	Passed	0	0	Passed	Medium
1763	Administrative Templates: Windows	BitLocker Drive Encryption: Operating System Drives: Configure minimum PIN length for startup	Medium		8	Failed	Medium
1720	Administrative Templates: Windows	Cloud Content: Do not show Windows tips	Medium	0	1	Failed	Medium
1721	Administrative Templates: Windows	Cloud Content: Turn off Microsoft consumer experiences	Medium	0	1	Failed	Medium
1722	Administrative Templates: Windows	Credential User Interface: Do not display the password reveal button	Medium	0	1	Failed	Medium
1724	Administrative Templates: Windows	Credential User Interface: Enumerate administrator accounts on elevation	Medium	1	0	Failed	Medium
1725	Administrative Templates: Windows	Data Collection and Preview Builds: Allow Diagnostic Data	Medium	2	1	Failed	Medium
1726	Administrative Templates: Windows	Data Collection and Preview Builds: Allow device name to be sent in Windows diagnostic data	Medium	1	0	Failed	Medium
1727	Administrative Templates: Windows	Delivery Optimization: Download Mode	Medium	1	99	Failed	Medium
1728	Administrative Templates: Windows	Event Log Service: Application: Specify the maximum log file size (KB)	Medium	4096	32768	Failed	Medium
1729	Administrative Templates: Windows	Event Log Service: Security: Specify the maximum log file size (KB)	Medium	4096	196608	Failed	Medium
1730	Administrative Templates: Windows	Event Log Service: System: Specify the maximum log file size (KB)	Medium	4096	32768	Failed	Medium
1774	Administrative Templates: Windows	Event Log Service: Microsoft-Windows-PowerShell/Operational: Specify the maximum log file size (KB)	Medium	15728640	268435456	Failed	Medium
1775	Administrative Templates: Windows	Event Log Service: PowerShellCore/Operational: Specify the maximum log file size (KB)	Medium	15728640	268435456	Failed	Medium
1731	Administrative Templates: Windows	File Explorer: Allow the use of remote paths in file shortcut icons	Passed	0	0	Passed	Medium
1732	Administrative Templates: Windows	HomeGroup: Prevent the computer from joining a homegroup	Medium	0	1	Failed	Medium
1800	Microsoft Defender Antivirus	Turn off Microsoft Defender Antivirus	Passed	0	0	Passed	Medium
1826	Microsoft Defender Antivirus	Enable Tamper Protection (Status)	Passed	True	True	Passed	Medium
1801	Microsoft Defender Antivirus	Configure detection for potentially unwanted applications	Medium	0	1	Failed	Medium
1806	Microsoft Defender Antivirus	Exclusions: Extension Exclusions (Policy)	Passed			Passed	Medium
1813	Microsoft Defender Antivirus	Exclusions: Extension Exclusions (Intune)	Passed			Passed	Medium
1807	Microsoft Defender Antivirus	Exclusions: Extension Exclusions	Passed			Passed	Medium
1808	Microsoft Defender Antivirus	Exclusions: Path Exclusions (Policy)	Passed			Passed	Medium
1814	Microsoft Defender Antivirus	Exclusions: Path Exclusions (Intune)	Passed			Passed	Medium
1809	Microsoft Defender Antivirus	Exclusions: Path Exclusions	Passed			Passed	Medium
1810	Microsoft Defender Antivirus	Exclusions: Process Exclusions (Policy)	Passed			Passed	Medium
1815	Microsoft Defender Antivirus	Exclusions: Process Exclusions (Intune)	Passed			Passed	Medium
1811	Microsoft Defender Antivirus	Exclusions: Process Exclusions	Passed			Passed	Medium
1816	Microsoft Defender Antivirus	MAPS: Join Microsoft MAPS	Medium	0	2	Failed	Medium
1817	Microsoft Defender Antivirus	MAPS: Configure the 'Block at First Sight' feature	Medium		0	Failed	Medium
1818	Microsoft Defender Antivirus	MAPS: Send file samples when further analysis is required	Medium		0	Failed	Medium
1819	Microsoft Defender Antivirus	MpEngine: Enable file hash computation feature	Medium		1	Failed	Medium
1820	Microsoft Defender Antivirus	MpEngine: Select cloud protection level	Medium	0	2	Failed	Medium
1821	Microsoft Defender Antivirus	Real-time Protection: Scan all downloaded files and attachments	Passed	0	0	Passed	Medium

1822	Microsoft Defender Antivirus	Real-time Protection: Turn off real-time protection	Passed	0	0	Passed	Medium
1823	Microsoft Defender Antivirus	Real-time Protection: Turn on behavior monitoring (Policy)	Passed	0	0	Passed	Medium
1824	Microsoft Defender Antivirus	Real-time Protection: Turn on script scanning	Passed	0	0	Passed	Medium
1825	Microsoft Defender Antivirus	Scan: Scan removable drives	Medium	1	0	Failed	Medium
1812	Microsoft Defender Antivirus	Enable sandboxing for Microsoft Defender Antivirus	Medium	0	1	Failed	Medium
1900	Microsoft Defender Exploit Guard	Attack Surface Reduction rules	Medium	0	1	Failed	Medium
1901	Microsoft Defender Exploit Guard	ASR: Block executable content from email client and webmail (Policy)	Medium	0	1	Failed	Medium
1916	Microsoft Defender Exploit Guard	ASR: Block executable content from email client and webmail	Medium	0	1	Failed	Medium
1933	Microsoft Defender Exploit Guard	ASR: Block executable content from email client and webmail (Intune)	Medium	0	1	Failed	Medium
1902	Microsoft Defender Exploit Guard	ASR: Block all Office applications from creating child processes (Policy)	Medium	0	1	Failed	Medium
1917	Microsoft Defender Exploit Guard	ASR: Block all Office applications from creating child processes	Medium	0	1	Failed	Medium
1934	Microsoft Defender Exploit Guard	ASR: Block all Office applications from creating child processes (Intune)	Medium	0	1	Failed	Medium
1903	Microsoft Defender Exploit Guard	ASR: Block Office applications from creating executable content (Policy)	Medium	0	1	Failed	Medium
1918	Microsoft Defender Exploit Guard	ASR: Block Office applications from creating executable content	Medium	0	1	Failed	Medium
1935	Microsoft Defender Exploit Guard	ASR: Block Office applications from creating executable content (Intune)	Medium	0	1	Failed	Medium
1904	Microsoft Defender Exploit Guard	ASR: Block Office applications from injecting code into other processes (Policy)	Medium	0	1	Failed	Medium
1919	Microsoft Defender Exploit Guard	ASR: Block Office applications from injecting code into other processes	Medium	0	1	Failed	Medium
1936	Microsoft Defender Exploit Guard	ASR: Block Office applications from injecting code into other processes (Intune)	Medium	0	1	Failed	Medium
1905	Microsoft Defender Exploit Guard	ASR: Block JavaScript or VBScript from launching downloaded executable content (Policy)	Medium	0	1	Failed	Medium
1920	Microsoft Defender Exploit Guard	ASR: Block JavaScript or VBScript from launching downloaded executable content	Medium	0	1	Failed	Medium
1937	Microsoft Defender Exploit Guard	ASR: Block JavaScript or VBScript from launching downloaded executable content (Intune)	Medium	0	1	Failed	Medium
1906	Microsoft Defender Exploit Guard	ASR: Block execution of potentially obfuscated scripts (Policy)	Medium	0	1	Failed	Medium
1921	Microsoft Defender Exploit Guard	ASR: Block execution of potentially obfuscated scripts	Medium	0	1	Failed	Medium
1938	Microsoft Defender Exploit Guard	ASR: Block execution of potentially obfuscated scripts (Intune)	Medium	0	1	Failed	Medium
1907	Microsoft Defender Exploit Guard	ASR: Block Win32 API calls from Office macros (Policy)	Medium	0	1	Failed	Medium
1922	Microsoft Defender Exploit Guard	ASR: Block Win32 API calls from Office macros	Medium	0	1	Failed	Medium
1939	Microsoft Defender Exploit Guard	ASR: Block Win32 API calls from Office macros (Intune)	Medium	0	1	Failed	Medium
1908	Microsoft Defender Exploit Guard	ASR: Block executable files from running unless they meet a prevalence, age, or trusted list criterion (Policy)	Medium	0	1	Failed	Medium
1923	Microsoft Defender Exploit Guard	ASR: Block executable files from running unless they meet a prevalence, age, or trusted list criterion	Medium	0	1	Failed	Medium
1940	Microsoft Defender Exploit Guard	ASR: Block executable files from running unless they meet a prevalence, age, or trusted list criterion (Intune)	Medium	0	1	Failed	Medium
1909	Microsoft Defender Exploit Guard	ASR: Use advanced protection against ransomware (Policy)	Medium	0	1	Failed	Medium
1924	Microsoft Defender Exploit Guard	ASR: Use advanced protection against ransomware	Medium	0	1	Failed	Medium
1941	Microsoft Defender Exploit Guard	ASR: Use advanced protection against ransomware (Intune)	Medium	0	1	Failed	Medium
1910	Microsoft Defender Exploit Guard	ASR: Block credential stealing from the Windows local security authority subsystem (lsass.exe) (Policy)	Medium	0	1	Failed	Medium
1925	Microsoft Defender Exploit Guard	ASR: Block credential stealing from the Windows local security authority subsystem (lsass.exe)	Medium	0	1	Failed	Medium
1942	Microsoft Defender Exploit Guard	ASR: Block credential stealing from the Windows local security authority subsystem (lsass.exe) (Intune)	Medium	0	1	Failed	Medium
1911	Microsoft Defender Exploit Guard	ASR: Block process creations originating from PSExec and WMI commands (Policy)	Medium	0	1	Failed	Medium
1926	Microsoft Defender Exploit Guard	ASR: Block process creations originating from PSExec and WMI commands	Medium	0	1	Failed	Medium
1943	Microsoft Defender Exploit Guard	ASR: Block process creations originating from PSExec and WMI commands (Intune)	Medium	0	1	Failed	Medium
1912	Microsoft Defender Exploit Guard	ASR: Block untrusted and unsigned processes that run from USB (Policy)	Medium	0	1	Failed	Medium
1927	Microsoft Defender Exploit Guard	ASR: Block untrusted and unsigned processes that run from USB	Medium	0	1	Failed	Medium
1944	Microsoft Defender Exploit Guard	ASR: Block untrusted and unsigned processes that run from USB (Intune)	Medium	0	1	Failed	Medium
1913	Microsoft Defender Exploit Guard	ASR: Block Office communication application from creating child processes (Policy)	Medium	0	1	Failed	Medium
1928	Microsoft Defender Exploit Guard	ASR: Block Office communication application from creating child processes	Medium	0	1	Failed	Medium
1945	Microsoft Defender Exploit Guard	ASR: Block Office communication application from creating child processes (Intune)	Medium	0	1	Failed	Medium
1914	Microsoft Defender Exploit Guard	ASR: Block Adobe Reader from creating child processes (Policy)	Medium	0	1	Failed	Medium
1929	Microsoft Defender Exploit Guard	ASR: Block Adobe Reader from creating child processes	Medium	0	1	Failed	Medium
1946	Microsoft Defender Exploit Guard	ASR: Block Adobe Reader from creating child processes (Intune)	Medium	0	1	Failed	Medium
1915	Microsoft Defender Exploit Guard	ASR: Block persistence through WMI event subscription (Policy)	Medium	0	1	Failed	Medium
1930	Microsoft Defender Exploit Guard	ASR: Block persistence through WMI event subscription	Medium	0	1	Failed	Medium
1947	Microsoft Defender Exploit Guard	ASR: Block persistence through WMI event subscription (Intune)	Medium	0	1	Failed	Medium
1931	Microsoft Defender Exploit Guard	ASR: Block abuse of exploited vulnerable signed drivers (Policy)	Medium	0	1	Failed	Medium
1932	Microsoft Defender Exploit Guard	ASR: Block abuse of exploited vulnerable signed drivers	Medium	0	1	Failed	Medium
1948	Microsoft Defender Exploit Guard	ASR: Block abuse of exploited vulnerable signed drivers (Intune)	Medium	0	1	Failed	Medium
1966	Microsoft Defender Exploit Guard	ASR: Exclude files and paths from Attack Surface Reduction Rules (Policy)	Passed			Passed	Medium
1967	Microsoft Defender Exploit Guard	ASR: Exclude files and paths from Attack Surface Reduction Rules	Passed			Passed	Medium
1968	Microsoft Defender Exploit Guard	ASR: Exclude files and paths from Attack Surface Reduction Rules (Intune)	Passed			Passed	Medium

1965	Microsoft Defender Exploit Guard	Network Protection: Prevent users and apps from accessing dangerous websites	Medium		1	Failed	Medium
1767	Administrative Templates: Windows	News and interests: Enable news and interests on the taskbar	Medium		0	Failed	Medium
1733	Administrative Templates: Windows	OneDrive: Prevent the usage of OneDrive for file storage	Medium	0	1	Failed	Medium
1734	Administrative Templates: Windows	Remote Desktop Connection Client: Do not allow passwords to be saved	Medium	0	1	Failed	Medium
1735	Administrative Templates: Windows	Remote Desktop Session Host: Allow users to connect remotely by using Remote Desktop Services	Medium	0	1	Failed	Medium
1736	Administrative Templates: Windows	Remote Desktop Session Host: Device and Resource Redirection: Do not allow drive redirection	Medium	0	1	Failed	Medium
1737	Administrative Templates: Windows	Remote Desktop Session Host: Security: Always prompt for password upon connection	Medium	0	1	Failed	Medium
1738	Administrative Templates: Windows	Remote Desktop Session Host: Security: Require secure RPC communication	Medium	0	1	Failed	Medium
1739	Administrative Templates: Windows	Remote Desktop Session Host: Security: Set client connection encryption level	Medium	0	3	Failed	Medium
1740	Administrative Templates: Windows	Search: Allow Cloud Search	Medium	1	0	Failed	Medium
1741	Administrative Templates: Windows	Search: Allow Cortana	Medium	1	0	Failed	Medium
1742	Administrative Templates: Windows	Search: Allow Cortana above lock screen	Medium	1	0	Failed	Medium
1743	Administrative Templates: Windows	Search: Allow indexing of encrypted files	Medium	1	0	Failed	Medium
1744	Administrative Templates: Windows	Search: Allow search and Cortana to use location	Medium	1	0	Failed	Medium
1745	Administrative Templates: Windows	Search: Set what information is shared in Search	Medium	1	3	Failed	Medium
1746	Administrative Templates: Windows	Windows Error Reporting: Disable Windows Error Reporting	Medium	0	1	Failed	Medium
1748	Administrative Templates: Windows	Windows Ink Workspace: Allow Windows Ink Workspace	Medium	1	0	Failed	Medium
1749	Administrative Templates: Windows	Windows Installer: Always install with elevated privileges	Passed	0	0	Passed	Medium
1750	Administrative Templates: Windows	Windows Installer: Allow user control over installs	Medium	1	0	Failed	Medium
1751	Administrative Templates: Windows	Windows Installer: Prevent Internet Explorer security prompt for Windows Installer scripts	Medium	1	0	Failed	Medium
1752	Administrative Templates: Windows	Windows Logon Options: Sign-in and lock last interactive user automatically after a restart	Medium	0	1	Failed	Medium
1770	Administrative Templates: Windows	Windows Installer: Disable Co-Installer (USB AutoInstall)	Medium		1	Failed	Medium
1753	Administrative Templates: Windows	WinRM Client: Allow Basic authentication	Medium	1	0	Failed	Medium
1754	Administrative Templates: Windows	WinRM Client: Allow unencrypted traffic	Medium	1	0	Failed	Medium
1755	Administrative Templates: Windows	WinRM Client: Disallow Digest authentication	Medium	1	0	Failed	Medium
1756	Administrative Templates: Windows	WinRM Service: Allow remote server management through WinRM	Medium	1	0	Failed	Medium
1757	Administrative Templates: Windows	WinRM Service: Allow Basic authentication	Medium	1	0	Failed	Medium
1758	Administrative Templates: Windows	WinRM Service: Allow unencrypted traffic	Medium	1	0	Failed	Medium
1759	Administrative Templates: Windows	WinRM Service: Disallow WinRM from storing RunAs credentials	Medium	0	1	Failed	Medium
1760	Administrative Templates: Windows	Windows Remote Shell: Allow Remote Shell Access	Medium	1	0	Failed	Medium
2000	Administrative Templates: Windows	File Explorer: Configure Windows Defender SmartScreen	Passed	1	1	Passed	Medium
2001	Administrative Templates: Windows	File Explorer: Configure Windows Defender SmartScreen to warn and prevent bypass	Medium	Warn	Block	Failed	Medium
2100	PowerShell	Turn on PowerShell Script Block Logging	Medium	0	1	Failed	Medium
2103	PowerShell	Disable PowerShell version 2	Medium	Enabled	Disabled	Failed	Medium
2104	PowerShell	Disable PowerShell version 2 (root)	Medium	Enabled	Disabled	Failed	Medium
2200	MS Security Guide	LSA Protection	Medium	2	1	Failed	Medium
2202	MS Security Guide	NetBT NodeType configuration	Medium	0	2	Failed	Medium
2209	MS Security Guide	Enable Structured Exception Handling Overwrite Protection (SEHOP)	Passed	0	0	Passed	Medium
2210	MS Security Guide	Limits print driver installation to Administrators	Medium		1	Failed	Medium
2211	MS Security Guide	Configure RPC packet level privacy setting for incoming connections	Medium		1	Failed	Medium
2212	MS Security Guide	Manage processing of Queue-specific files	Medium		1	Failed	Medium
2204	MSS (Legacy)	MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)	Medium	0	1	Failed	Medium
2205	MSS (Legacy)	MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)	Medium	0	2	Failed	Medium
2206	MSS (Legacy)	MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)	Medium	1	2	Failed	Medium
2207	MSS (Legacy)	MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes	Medium	1	0	Failed	Medium
2208	MSS (Legacy)	MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers	Medium	0	1	Failed	Medium
2400	Scheduled Task	XblGameSave Standby Task	Medium	Ready	Disabled	Failed	Medium
2411	System Services	Disable mDNS in Dnscache service	Medium		0	Failed	Medium
2401	System Services	Print Spooler (Spooler)	Medium	2	4	Failed	Medium
2402	System Services	Print Spooler (Spooler) (Service Startup type)	Medium	Automatic	Disabled	Failed	Medium
2412	System Services	WebClient (WebClient)	Medium	3	4	Failed	Medium
2413	System Services	WebClient (WebClient) (Service Startup type)	Medium	Manual	Disabled	Failed	Medium
2403	System Services	Xbox Accessory Management Service (XboxGipSvc)	Medium	3	4	Failed	Medium
2404	System Services	Xbox Accessory Management Service (XboxGipSvc) (Service Startup type)	Medium	Manual	Disabled	Failed	Medium
2405	System Services	Xbox Live Auth Manager (XblAuthManager)	Medium	3	4	Failed	Medium
2406	System Services	Xbox Live Auth Manager (XblAuthManager) (Service Startup type)	Medium	Manual	Disabled	Failed	Medium
2407	System Services	Xbox Live Game Save (XblGameSave)	Medium	3	4	Failed	Medium

2408	System Services	Xbox Live Game Save (XblGameSave) (Service Startup type)	Medium	Manual	Disabled	Failed	Medium
2409	System Services	Xbox Live Networking Service (XboxNetApiSvc)	Medium	3	4	Failed	Medium
2410	System Services	Xbox Live Networking Service (XboxNetApiSvc) (Service Startup type)	Medium	Manual	Disabled	Failed	Medium
1950	Microsoft Defender Exploit Guard	Exploit protection: Control flow guard (CFG)	Medium	NOTSET	ON	Failed	Medium
1951	Microsoft Defender Exploit Guard	Exploit protection: Data Execution Prevention (DEP)	Medium	NOTSET	ON	Failed	Medium
1952	Microsoft Defender Exploit Guard	Exploit protection: Override Data Execution Prevention (DEP)	Passed	False	False	Passed	Medium
1954	Microsoft Defender Exploit Guard	Exploit protection: Force randomization for images (Mandatory ASLR)	Medium	NOTSET	ON	Failed	Medium
1955	Microsoft Defender Exploit Guard	Exploit protection: Override force randomization for images (Mandatory ASLR)	Passed	False	False	Passed	Medium
1956	Microsoft Defender Exploit Guard	Exploit protection: Randomize memory allocations (Bottom-up ASLR)	Medium	NOTSET	ON	Failed	Medium
1957	Microsoft Defender Exploit Guard	Exploit protection: Override randomize memory allocations (Bottom-up ASLR)	Passed	False	False	Passed	Medium
1958	Microsoft Defender Exploit Guard	Exploit protection: High-entropy ASLR	Medium	NOTSET	ON	Failed	Medium
1959	Microsoft Defender Exploit Guard	Exploit protection: Override high-entropy ASLR	Passed	False	False	Passed	Medium
1960	Microsoft Defender Exploit Guard	Exploit protection: Validate exception chains (SEHOP)	Medium	NOTSET	ON	Failed	Medium
1961	Microsoft Defender Exploit Guard	Exploit protection: Validate exception chains (SEHOP (Telemetry only)	Medium	NOTSET	OFF	Failed	Medium
1962	Microsoft Defender Exploit Guard	Exploit protection: Override validate exception chains (SEHOP)	Passed	False	False	Passed	Medium
1963	Microsoft Defender Exploit Guard	Exploit protection: Validate heap integrity	Medium	NOTSET	ON	Failed	Medium
1964	Microsoft Defender Exploit Guard	Exploit protection: Override validate heap integrity	Passed	False	False	Passed	Medium
1953	Microsoft Defender Exploit Guard	Force use of Data Execution Prevention (DEP)	Medium	OptIn	AlwaysOn	Failed	Medium