

## **Commonly Exploited Protocols:**

# Windows Management Instrumentation (WMI)

December 2021

# Acknowledgments

The Center for Internet Security® (CIS®) would like to thank the many security experts who volunteer their time and talent to support the CIS Critical Security Controls® (CIS Controls®) and other CIS work. CIS products represent the effort of a veritable army of volunteers from across the industry, generously giving their time and talent in the name of a more secure online experience for everyone.

## Editor

Ginger Anderson, CIS

## Contributors

Theodore Sayers, CIS

Jennifer Jarose, CIS

---

This work is licensed under a Creative Commons Attribution-Non Commercial-No Derivatives 4.0 International Public License (the link can be found at <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>).

To further clarify the Creative Commons license related to the CIS Controls® content, you are authorized to copy and redistribute the content as a framework for use by you, within your organization and outside of your organization for non-commercial purposes only, provided that (i) appropriate credit is given to CIS, and (ii) a link to the license is provided. Additionally, if you remix, transform, or build upon the CIS Controls, you may not distribute the modified materials. Users of the CIS Controls framework are also required to refer to (<http://www.cisecurity.org/controls/>) when referring to the CIS Controls in order to ensure that users are employing the most up-to-date guidance. Commercial use of the CIS Controls is subject to the prior approval of the Center for Internet Security, Inc. (CIS®).

# Contents

	<b>Introduction</b>	<b>1</b>
	<b>Purpose</b>	<b>2</b>
	<b>WMI Attacks</b>	<b>4</b>
	<b>Reconnaissance/Discovery</b>	<b>5</b>
	Overview	5
	Recommendations	6
	<b>Initial Access</b>	<b>1</b>
	Overview	1
	Recommendations	1
	<b>Privilege Escalation</b>	<b>3</b>
	Overview	3
	Recommendations	3
	<b>Defense Evasion</b>	<b>4</b>
	Overview	4
	Recommendations	4
	<b>Execution</b>	<b>6</b>
	Overview	6
	Recommendations	6
	<b>Persistence</b>	<b>8</b>
	Overview	8
	Recommendations	8
	<b>Lateral Movement</b>	<b>10</b>
	Overview	10
	Recommendations	10
	<b>Command and Control</b>	<b>13</b>
	Overview	13
	Recommendations	13
	<b>Exfiltration</b>	<b>14</b>
	Overview	14
	Recommendations	14
	<b>Conclusion</b>	<b>15</b>
<b>Appendix A</b>	<b>WMI Mapping to MITRE ATT&amp;CK</b>	<b>16</b>
<b>Appendix B</b>	<b>CIS Controls</b>	<b>17</b>
	Implementation Groups	17
	CIS Safeguards	18
<b>Appendix C</b>	<b>CIS Benchmarks</b>	<b>20</b>
	CIS Benchmarks: WMI-Related Recommendations	20
<b>Appendix D</b>	<b>Analysis</b>	<b>29</b>
	<b>Acronyms</b>	<b>30</b>
	<b>References and Resources</b>	<b>31</b>

# Introduction

The CIS Controls are a prioritized set of actions which collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. The CIS Controls are developed by a community of Information Technology (IT) experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. The experts who develop the CIS Controls come from a wide range of sectors, including retail, manufacturing, healthcare, education, government, defense, and others. It is important to note that while the CIS Controls address general best practices that enterprises should implement to protect their environment, some operational environments may present unique requirements not addressed by the CIS Controls or require deviations from best practices.

CIS strongly believes that threats should inform defensive recommendations. As part of that belief, CIS developed the [CIS Community Defense Model \(CDM\)](#) to help defenders prioritize defensive controls based on threat summaries provided by various sources including the Verizon Data Breach Investigations Report (DBIR), CrowdStrike® Global Threat Report, and others. Additionally, CIS is proactively providing defensive guidance to address some of the most commonly used vectors and exploited protocols to conduct attacks, such as [Remote Desktop Protocol \(RDP\)](#) and [Server Message Block \(SMB\)](#). Guidance for RDP and SMB can be found on the CIS website.

Cyber threat actors (CTAs), both nation-state and cybercriminals, have increased their use of tools natively on systems to complete their objectives because the tools afford them the ability to blend into their victims' networks and hide their activity amongst legitimate processes. In fact, according to the 2020 CrowdStrike Global Threat Report, 51% of the cyber-attacks captured by CrowdStrike's Threat Graph are malware-free, an increase from the previous year's 40%. CrowdStrike defines malware-free as "those in which the initial tactic did not result in a file or file fragment being written to disk. Examples include attacks where code executes from memory or where stolen credentials are leveraged for remote logins using known tools."<sup>1</sup>

<sup>1</sup> <https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf>

# Purpose

This guide will focus on a commonly exploited protocol, Windows Management Instrumentation (WMI) Remote Protocol, and the Safeguards an enterprise can implement, in part or whole, to reduce their attack surface or detect anomalies associated with the exploitation of WMI. The goal is to deliver a set of best practices from the CIS Controls, CIS Benchmarks™, or additional guidance, that all enterprises can use to protect against WMI facilitated attacks.

This is accomplished by mapping WMI classes<sup>2</sup> or events that CTAs can use to conduct attacks to the [MITRE Adversarial Tactics, Techniques & Common Knowledge \(ATT&CK® Framework v8.2\)](#). Specifically, the guide focuses on identifying ATT&CK Tactics, the “why” behind a CTA’s actions, and the ATT&CK Techniques or ATT&CK Sub-Techniques within those Tactics. This mapping can be found in Appendix A. Once the Techniques and Sub-Techniques are identified, the CDM master mapping<sup>3</sup> is used to identify Safeguards from v8 of the CIS Controls that can be implemented to reduce the attack surface or detect anomalies, including the respective Implementation Group (IG). See Appendix B. Additionally, recommendations from the CIS Microsoft Windows 10 Enterprise Release 21H1 Benchmark v1.11.0 are provided to assist in and emphasize a defense-in-depth approach. See Appendix C for a full listing of these recommendations.

WMI is infrastructure on Windows-based operating systems (OS) used for management data and operations. It provides a uniform interface for local or remote applications or scripts to obtain management data from a computer system, network, or enterprise; the interface is designed so that WMI client applications and scripts do not have to call a wide variety of OS application programming interfaces (APIs). Windows introduced WMI during the Windows NT 4.0 and Windows 95<sup>4</sup> era; and while Windows has introduced and deprecated technology in the Windows OS over the years, WMI continues to exist in the Windows environment. It currently provides almost 4,000 different configurable items.<sup>5</sup>

Since its introduction, system administrators use WMI to automate tasks and remotely manage systems in their environment. At a broad level, some of these tasks include but are not limited to:<sup>6</sup>

- **Account and domain management:** Enumerate and manage the resources in a directory service, such as adding users and groups, and setting permissions on network resources and obtain information such as the computer domain or the users currently logged-on.
- **Computer hardware:** Obtain information about the presence, state, or properties of hardware components.
- **Computer software:** Obtain information such as which software is installed by the Microsoft Installer (MSI) and software versions.
- **Dates and times:** There are WMI classes and a scripting object to parse or convert the Common Information Model (CIM) datetime format.

<sup>2</sup> A class is a grouping of management objects. Classes are predefined based on the Common Information Model and are created when a new WMI namespace is created.

<sup>3</sup> A master mapping from CIS Controls v8 to Enterprise ATT&CK v8.2, mapping the CIS Safeguards to the ATT&CK (sub-)techniques.

<sup>4</sup> <https://web.archive.org/web/20050115045451/http://www.microsoft.com/downloads/details.aspx?FamilyID=c174cfb1-ef67-471d-9277-4c2b1014a31e&displaylang=en>

<sup>5</sup> <https://www.sans.org/blog/investigating-wmi-attacks/>

<sup>6</sup> <https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-tasks-for-scripts-and-applications>

- **Desktop management:** Obtain data from or control remote desktops. For example, you can determine whether or not the screensaver requires a password. WMI also gives you the ability to shut down a remote computer.
- **Disk and file systems:** Obtain information about disk drive hardware state, logical volumes.
- **Event logs:** Obtain event data from NT Event Log files and perform operations like backing up or clearing log files.
- **Files and folders:** Change file or folder properties through WMI, including creating a share or renaming a file.
- **Networking:** Manage and obtain information about connections and Internet Protocol (IP) or Media Access Control (MAC) addresses.
- **Operating system:** Obtain information about the operating system, such as version, whether it is activated, or which hotfixes are installed.
- **Performance monitoring:** Use the WMI classes that obtain data from performance counters to access and refresh data about computer performance.
- **Printers and printing:** Manage and obtain data about printers, such as finding or setting the default printer.
- **Processes:** Obtain information such as the account under which a process is running. You can perform actions like creating processes.
- **Registry:** Create and modify registry keys and values.
- **Schedule tasks:** Create and get information about scheduled tasks.
- **Services:** Obtain information about services, including dependent or antecedent services.

# WMI Attacks

The same capabilities that attract administrators and developers to WMI also attract cyber threat actors (CTAs). CTAs can often use WMI to deploy and execute various malware such as cryptominers (Kingminer), banking Trojans (Emotet), ransomware (Maze), and worms such as the notorious Stuxnet that affected nuclear processing facilities in Iran. For attackers, there are some advantages to using WMI, the first being that attackers often prefer to take easier and pre-existing vectors to conduct attacks as opposed to creating specialized or unique tools. WMI is a native tool installed on all Windows-operated systems dating back to Windows 95 and NT 4.0. Another advantage for attackers is that WMI allows attackers a stealthier method of executing attacks. Many permanent events run as SYSTEM and payloads are written to the WMI repository as opposed to disk. Additionally, defenders can, generally, be unaware of WMI as a multi-purpose vector.

WMI is a powerful tool that attackers can use for various phases of the attack lifecycle. The native tool provides numerous objects, methods, and events that can be used for reconnaissance, detection of anti-virus (AV) or virtual machine (VM) products, code execution, lateral movement, covert data storage, and persistence without introducing a file to disk. The pages that follow discuss ways that WMI can be used across phases of an attack with accompanying defensive approaches. While the list is not fully exhaustive, this guide provides recommendations that will defend against WMI attacks.

# Reconnaissance/Discovery

## Overview

Reconnaissance, or discovery, is the first step in the lifecycle of any attack. Ethical hackers and penetration testers often use reconnaissance to conduct assessments of vulnerabilities in a system or network. Similarly, reconnaissance allows the CTAs to covertly discover and collect information about a system, file permissions, running network services, operating system platforms, trust relationships, and user account information. Through reconnaissance, CTAs can get a feel for the environment they will be targeting.<sup>7</sup>

WMI offers a large number of classes that can be used by CTAs to conduct reconnaissance or discovery:

- **T1007 System Service Discovery:** The Win32\_Service WMI class represents a service.
- **T1012 Query Registry:** You can obtain data from the registry by using the StdRegProv WMI class, as well as the Win32\_Registry class.
- **T1016 System Network Configuration Discovery:** The Win32\_SystemNetworkConnections WMI class relates a network connection, and the MSFT\_NetAdapter can offer information about network adapters.
- **T1018 Remote System Discovery:** The Win32\_PingStatus can return data from computers that have both IPv4 and IPv6 addresses.
- **T1057 Process Discovery:** The Win32\_Process WMI class may offer plenty of opportunities for CTAs to identify processes.
- **T1069 Permission Groups Discovery:** The Win32\_Group WMI class gives information about a group account, and Win32\_GroupUser relates a group and an account that is a member of that group.
- **T1082 System Information Discovery:** There are a variety of useful classes; for example Win32\_OperatingSystem and Win32\_SystemResources.
- **T1083 File and Directory Discovery:** The Win32\_Directory WMI class can manipulate a directory. The CIM\_DataFile WMI class represents a named collection of data. The Win32\_ShortcutFile WMI class represents shortcut files.
- **T1087 Account Discovery:** The Win32\_UserAccount WMI class contains information about a user account on a computer system, and the Win32\_LoggedOnUser WMI class relates a session and a user account. Disk volume listing: Win32\_Volume.
- **T1120 Peripheral Device Discovery:** There are a lot of useful WMI classes to discover peripheral devices, such as: Win32\_CDROMDrive, Win32\_DesktopMonitor, Win32\_InfraredDevice, Win32\_Keyboard, Win32\_Printer, Win32\_SerialPort, Win32\_USBController, Win32\_VideoController, and others.
- **T1124 System Time Discovery:** Using the Win32\_TimeZone you can retrieve time zone information.
- **T1135 Network Share Discovery:** The Win32\_Share WMI class represents a shared resource.
- **T1497 Virtualization/ Sandbox Evasion:** Both the Win32\_ComputerSystem WMI class and Win32\_BaseBoard can detect a VM.
- **T1592 Gather Victim Host Information:** Win32\_OperatingSystem and Win32\_ComputerSystem allow an attacker to gather host information.

<sup>7</sup> <https://www.bitdefender.com/files/News/CaseStudies/study/377/Bitdefender-Whitepaper-WMI-creat4871-en-EN-GenericUse.pdf>



### CIS Controls v8

- Safeguard 4.8 (IG2): Uninstall or Disable Unnecessary Services on Enterprise Assets and Software
- Safeguard 18.3 (IG2): Remediate Penetration Test Findings
- Safeguard 18.5 (IG3): Perform Periodic Internal Penetration Tests

### CIS Microsoft Windows 10 Enterprise Release 21H1 Benchmark v1.11.0

- **2.2.15:** Ensure 'Debug programs' is set to 'Administrators'
- **2.2.34:** Ensure 'Profile single process' is set to 'Administrators'
- **2.2.35:** Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost'
- **2.3.7.2:** Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled'
- **2.3.10.1:** Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'
- **2.3.10.2:** Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled'
- **2.3.10.3:** Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled'
- **2.3.10.5:** Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'
- **2.3.10.7:** Ensure 'Network access: Remotely accessible registry paths'
- **2.3.10.8:** Ensure 'Network access: Remotely accessible registry paths and sub-paths'
- **2.3.10.9:** Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled'
- **2.3.10.10:** Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow'
- **5.3:** Ensure 'Computer Browser (Browser)' is set to 'Disabled' or 'Not Installed'
- **5.9:** Ensure 'Link-Layer Topology Discovery Mapper (lltdsvc)' is set to 'Disabled'
- **5.24:** Ensure 'Remote Registry (RemoteRegistry)' is set to 'Disabled'
- **5.26:** Ensure 'Server (LanmanServer)' is set to 'Disabled'
- **5.31:** Ensure 'UPnP Device Host (upnphost)' is set to 'Disabled'
- **5.41:** Ensure 'Xbox Accessory Management Service (XboxGipSvc)' is set to 'Disabled'
- **18.5.20.1:** Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled'
- **18.5.20.2:** Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled'
- **18.8.28.1:** Ensure 'Block user from showing account details on sign-in' is set to 'Enabled'
- **18.8.28.3:** Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled'
- **18.8.28.4:** Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled'
- **18.8.34.6.1:** Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled'

- **18.8.34.6.2:** Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled'
- **18.9.4.1:** Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled'
- **18.9.15.2:** Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled'
- **18.9.35.1:** Ensure 'Prevent the computer from joining a homegroup' is set to 'Enabled'
- **18.9.59.3.11.1:** Ensure 'Do not delete temp folders upon exit' is set to 'Disabled'
- **18.9.65.5:** Ensure 'Allow indexing of encrypted files' is set to 'Disabled'
- **19.7.28.1:** Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled'

# Initial Access

## Overview

Initial access allows CTAs the ability to gain a foothold in the victim's network. Initial access allows CTAs to maintain long-term access to a network and is often accomplished through spearphishing or exploitation of external facing services and protocols.

WMI offers CTAs the ability to:

- **T1021 Remote Services:** The Win32\_Service WMI class represents a service that can be in a remote location. CTAs can use the WMI Win32\_Service class to enumerate the services installed on a computer. In addition, they can use this class to determine whether those services are currently running or return any other required information about that service, and its configuration.

## Recommendations

### CIS Controls v8

- **Safeguard 4.7 (IG1):** Manage Default Accounts on Enterprise Assets and Software
- **Safeguard 5.3 (IG1):** Disable Dormant Accounts
- **Safeguard 6.1 (IG1):** Establish an Access Granting Process
- **Safeguard 6.2 (IG1):** Establish an Access Revoking Process
- **Safeguard 6.4 (IG1):** Require MFA for Remote Network Access
- **Safeguard 6.5 (IG1):** Require MFA for Administrative Access
- **Safeguard 6.8 (IG2):** Define and Maintain Role-Based Access Control

### CIS Microsoft Windows 10 Enterprise Release 21H1 Benchmark v1.11.0

- **2.2.2:** Ensure 'Access this computer from the network' is set to 'Administrators, Remote Desktop Users'
- **2.2.6:** Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users'
- **2.2.16:** Ensure 'Deny access to this computer from the network' to include 'Guests, Local account'
- **2.2.20:** Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account'
- **2.3.1.4:** Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'
- **2.3.8.1:** Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'
- **2.3.8.2:** Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled'
- **2.3.8.3:** Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled'
- **2.3.9.2:** Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'
- **2.3.9.3:** Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'
- **5.13:** Ensure 'OpenSSH SSH Server (sshd)' is set to 'Disabled' or 'Not Installed'
- **5.21:** Ensure 'Remote Desktop Services (TermService)' is set to 'Disabled'

- **5.39:** Ensure 'Windows Remote Management (WS-Management) (WinRM)' is set to 'Disabled'
- **9.1.1:** Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'
- **9.1.2:** Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'
- **9.2.1:** Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)'
- **9.2.2:** Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'
- **9.3.1:** Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'
- **9.3.2:** Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)'
- **18.3.1:** Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled'
- **18.3.2:** Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)'
- **18.3.3:** Ensure 'Configure SMB v1 server' is set to 'Disabled'
- **18.5.8.1:** Ensure 'Enable insecure guest logons' is set to 'Disabled'
- **18.8.36.1:** Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'
- **18.8.36.2:** Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'
- **18.9.63.3.2.1:** Ensure 'Allow users to connect remotely by using Remote Desktop Services' is set to 'Disabled'
- **18.9.63.3.10.2:** Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute'
- **18.9.98.2.2:** Ensure 'Allow remote server management through WinRM' is set to 'Disabled'
- **18.9.98.2.4:** Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled'
- **18.9.99.1:** Ensure 'Allow Remote Shell Access' is set to 'Disabled'

# Privilege Escalation

## Overview

Privilege escalation allows CTAs to gain higher-level permissions on a system or network. This is often accomplished by exploiting vulnerabilities and misconfigurations. While CTA's can conduct discovery and reconnaissance activities with lower-level permissions, they often need privilege escalation to accomplish tasks such as execution and data exfiltration.

WMI offers CTAs the ability to:

- **T1053 Scheduled Task/Job:** The Win32\_ScheduledJob WMI class represents a job created with the Attention (AT) command

## Recommendations

### CIS Controls v8

- **Safeguard 4.7 (IG1):** Manage Default Accounts on Enterprise Assets and Software
- **Safeguard 4.8 (IG2):** Uninstall or Disable Unnecessary Services on Enterprise Assets and Software
- **Safeguard 5.3 (IG1):** Disable Dormant Accounts
- **Safeguard 5.4 (IG1):** Restrict Administrator Privileges to Dedicated Administrator Accounts
- **Safeguard 6.1 (IG1):** Establish an Access Granting Process
- **Safeguard 6.2 (IG1):** Establish an Access Revoking Process
- **Safeguard 6.8 (IG2):** Define and Maintain Role-Based Access Control
- **Safeguard 18.3 (IG2):** Remediate Penetration Test Findings
- **Safeguard 18.5 (IG3):** Perform Periodic Internal Penetration Tests

### CIS Microsoft Windows 10 Enterprise Release 21H1 Benchmark v1.11.0

- **2.2.17:** Ensure 'Deny log on as a batch job' to include 'Guests'
- **2.2.28:** Ensure 'Log on as a batch job' is set to 'Administrators'

# Defense Evasion

## Overview

Defense evasion allows CTAs to avoid detection throughout the extent of the compromise. CTAs can use and abuse trusted processes to hide malware and activities. Often defense evasion consists of deleting or uninstalling software, avoiding security applications, and encrypting data and scripts.

WMI offers CTAs the ability to:

- **T1112 Modify Registry:** StdRegProv WMI class contains methods that manipulate registry keys.
- **T1202 Indirect Command Execution:** Win32\_Process WMI class can be used to execute commands, without invoking cmd.exe directly. CTAs will often incorporate the class into malware to avoid detection.
- **T1562.001 Impair Defense – Disable or Modify Tools:** CTAs can impair defenses by, for example, deleting registry keys via WMI, or using wmic.exe to terminate processes.

## Recommendations

### CIS Controls v8

- **Safeguard 3.3 (IG1):** Configure Data Access Control Lists
- **Safeguard 4.1 (IG1):** Establish and Maintain a Secure Configuration Process
- **Safeguard 4.7 (IG1):** Manage Default Accounts on Enterprise Assets and Software
- **Safeguard 5.3 (IG1):** Disable Dormant Accounts
- **Safeguard 5.4 (IG1):** Restrict Administrator Privileges to Dedicated Administrator Accounts
- **Safeguard 6.1 (IG1):** Establish an Access Granting Process
- **Safeguard 6.2 (IG1):** Establish an Access Revoking Process
- **Safeguard 6.8 (IG2):** Define and Maintain Role-Based Access Control

### CIS Microsoft Windows 10 Enterprise Release 21H1 Benchmark v1.11.0

- **2.2.15:** Ensure 'Debug programs' is set to 'Administrators'
- **2.2.34:** Ensure 'Profile single process' is set to 'Administrators'
- **2.2.35:** Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost'
- **2.3.7.2:** Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled'
- **2.3.10.1:** Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'
- **2.3.10.2:** Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled'
- **2.3.10.3:** Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled'
- **2.3.10.5:** Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'
- **2.3.10.7:** Ensure 'Network access: Remotely accessible registry paths'
- **2.3.10.8:** Ensure 'Network access: Remotely accessible registry paths and sub-paths'

- **2.3.10.9:** Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled'
- **2.3.10.10:** Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow'
- **5.3:** Ensure 'Computer Browser (Browser)' is set to 'Disabled' or 'Not Installed'
- **5.9:** Ensure 'Link-Layer Topology Discovery Mapper (lltdsvc)' is set to 'Disabled'
- **5.24:** Ensure 'Remote Registry (RemoteRegistry)' is set to 'Disabled'
- **5.26:** Ensure 'Server (LanmanServer)' is set to 'Disabled'
- **5.31:** Ensure 'UPnP Device Host (upnphost)' is set to 'Disabled'
- **5.41:** Ensure 'Xbox Accessory Management Service (XboxGipSvc)' is set to 'Disabled'
- **18.5.20.1:** Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled'
- **18.5.20.2:** Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled'
- **18.8.28.1:** Ensure 'Block user from showing account details on sign-in' is set to 'Enabled'
- **18.8.28.3:** Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled'
- **18.8.28.4:** Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled'
- **18.8.34.6.1:** Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled'
- **18.8.34.6.2:** Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled'
- **18.9.4.1:** Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled'
- **18.9.15.2:** Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled'
- **18.9.35.1:** Ensure 'Prevent the computer from joining a homegroup' is set to 'Enabled'
- **18.9.45.4.1.1:** Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled'
- **18.9.45.4.1.2:** Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is 'configured'
- **18.9.45.8.3:** Ensure 'Turn on behavior monitoring' is set to 'Enabled'
- **18.9.63.3.11.1:** Ensure 'Do not delete temp folders upon exit' is set to 'Disabled'
- **18.9.65.3:** Ensure 'Allow Cortana' is set to 'Disabled'
- **18.9.65.4:** Ensure 'Allow Cortana above lock screen' is set to 'Disabled'
- **18.9.65.6:** Ensure 'Allow search and Cortana to use location' is set to 'Disabled'
- **19.7.28.1:** Ensure 'Prevent users from sharing files within their profile' is set to 'Enabled'

# Execution

## Overview

Execution consists of CTA-controlled code running on a local or remote system. The execution of code is usually paired with other techniques in order to accomplish the CTA's end goal. In WMI there are two common methods of achieving remote code execution: through the use of the Win32\_Process Create method and the use of event consumers.

WMI offers CTAs the ability to execute malicious code by:

- **T1047 Windows Management Instrumentation:** As a technique, WMI provides a uniform environment to access Windows system components locally and remotely in order to execute malicious code and payloads.
- **T1053 Scheduled Task/Job:** The Win32\_ScheduledJob WMI class represents a job created with the AT command.
- **T1059.001 Command and Scripting Interpreter – PowerShell:** The Get-WmiObject is the standard cmdlet PowerShell used to retrieve class and instance information from WMI. CTAs can use the cmdlet to execute PowerShell scripts and commands without invoking the powershell.exe binary.
- **T1559.001 Inter-Process Communication – Component Object Model (COM):** Interacting with WMI is done through COM.

## Recommendations

### CIS Controls v8

- **Safeguard 2.3 (IG1):** Address Unauthorized Software
- **Safeguard 2.5 (IG2):** Allowlist Authorized Software
- **Safeguard 2.7 (IG3):** Allowlist Authorized Scripts
- **Safeguard 4.1 (IG1):** Establish and Maintain a Secure Configuration Process
- **Safeguard 4.7 (IG1):** Manage Default Accounts on Enterprise Assets and Software
- **Safeguard 4.8 (IG2):** Uninstall or Disable Unnecessary Services on Enterprise Assets and Software
- **Safeguard 5.2 (IG1):** Use Unique Passwords
- **Safeguard 5.3 (IG1):** Disable Dormant Accounts
- **Safeguard 5.4 (IG1):** Restrict Administrator Privileges to Dedicated Administrator Accounts
- **Safeguard 6.1 (IG1):** Establish an Access Granting Process
- **Safeguard 6.2 (IG1):** Establish an Access Revoking Process
- **Safeguard 6.8 (IG2):** Define and Maintain Role-Based Access Control
- **Safeguard 9.7 (IG3):** Deploy and Maintain Email Server Anti-Malware Protections
- **Safeguard 10.1 (IG1):** Deploy and Maintain Anti-Malware Software
- **Safeguard 10.2 (IG1):** Configure Automatic Anti-Malware Signature Updates
- **Safeguard 10.7 (IG2):** Use Behavior-Based Anti-Malware Software
- **Safeguard 13.2 (IG2):** Deploy a Host-Based Intrusion Detection Solution
- **Safeguard 13.7 (IG3):** Deploy a Host-Based Intrusion Prevention Solution
- **Safeguard 16.10 (IG2):** Apply Secure Design Principles in Application Architectures
- **Safeguard 18.3 (IG2):** Remediate Penetration Test Findings
- **Safeguard 18.5 (IG3):** Perform Periodic Internal Penetration Tests



## CIS Microsoft Windows 10 Enterprise Release 21H1 Benchmark v1.11.0

- **2.2.17:** Ensure 'Deny log on as a batch job' to include 'Guests'
- **2.2.28:** Ensure 'Log on as a batch job' is set to 'Administrators'
- **9.1.2:** Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'
- **9.2.2:** Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'
- **9.3.2:** Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)'
- **18.3.2:** Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)'
- **18.3.3:** Ensure 'Configure SMB v1 server' is set to 'Disabled'
- **18.9.30.4:** Ensure 'Turn off shell protocol protected mode' is set to 'Disabled'

# Persistence

## Overview

Persistence allows CTAs to maintain a foothold in a victim's network. Persistence techniques allow CTAs to maintain access to key systems through restarts, changed credentials, and other potential interruptions. CTAs may use configuration changes or actions to allow them to maintain persistence.

CTAs can maintain persistence using WMI by:

- **T1053 Scheduled Task/Job:** The Win32\_ScheduledJob WMI class represents a job created with the AT command
- **T1133 External Remote Services:** WinRM allows CTAs to write scripts to automate the management of servers and obtain data for management applications.
- **T1546.003 Event Triggered Execution – Windows Instrumentation Management Event Subscription:** CTAs can use WMI to install event filters, providers, consumers and bindings that execute code when a defined event occurs.
- **T1547.001 Boot or Logon Autostart Execution – Registry Run Keys/Startup Folder:** StdRegPro WMI class contains methods that manipulate registry run keys.

## Recommendations

### CIS Controls v8

- **Safeguard 2.3 (IG1):** Address Unauthorized Software
- **Safeguard 2.5 (IG2):** Allowlist Authorized Software
- **Safeguard 3.12 (IG2):** Segment Data Processing and Storage Based on Sensitivity
- **Safeguard 4.1 (IG1):** Establish and Maintain a Secure Configuration Process
- **Safeguard 4.2 (IG1):** Establish and Maintain a Secure Configuration Process for Network Infrastructure
- **Safeguard 4.4 (IG1):** Implement and Manage a Firewall on Servers
- **Safeguard 4.7 (IG1):** Manage Default Accounts on Enterprise Assets and Software
- **Safeguard 4.8 (IG2):** Uninstall or Disable Unnecessary Services on Enterprise Assets and Software
- **Safeguard 5.2 (IG1):** Use Unique Passwords
- **Safeguard 5.3 (IG1):** Disable Dormant Accounts
- **Safeguard 5.4 (IG1):** Restrict Administrator Privileges to Dedicated Administrator Accounts
- **Safeguard 6.1 (IG1):** Establish an Access Granting Process
- **Safeguard 6.2 (IG1):** Establish an Access Revoking Process
- **Safeguard 6.3 (IG1):** Require MFA for Externally-Exposed Applications
- **Safeguard 6.4 (IG1):** Require MFA for Remote Network Access
- **Safeguard 6.5 (IG1):** Require MFA for Administrative Access
- **Safeguard 6.8 (IG2):** Define and Maintain Role-Based Access Control
- **Safeguard 7.6 (IG2):** Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets
- **Safeguard 7.7 (IG2):** Remediate Detected Vulnerabilities
- **Safeguard 12.2 (IG2):** Establish and Maintain a Secure Network Architecture
- **Safeguard 12.7 (IG2):** Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure

- **Safeguard 12.8 (IG3):** Establish and Maintain Dedicated Computing Resources for All Administrative Work
- **Safeguard 13.5 (IG2):** Manage Access Control for Remote Assets
- **Safeguard 13.10 (IG3):** Perform Application Layer Filtering
- **Safeguard 16.8 (IG2):** Separate Production and Non-Production Systems
- **Safeguard 16.10 (IG2):** Apply Secure Design Principles in Application Architectures
- **Safeguard 18.3 (IG2):** Remediate Penetration Test Findings
- **Safeguard 18.5 (IG3):** Perform Periodic Internal Penetration Tests

#### **CIS Microsoft Windows 10 Enterprise Release 21H1 Benchmark v1.11.0**

- **2.2.17:** Ensure 'Deny log on as a batch job' to include 'Guests'
- **2.2.28:** Ensure 'Log on as a batch job' is set to 'Administrators'
- **5.29:** Ensure 'Special Administration Console Helper (sacsvr)' is set to 'Disabled' or 'Not Installed'
- **5.39:** Ensure 'Windows Remote Management (WS-Management) (WinRM)' is set to 'Disabled'
- **9.1.2:** Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'
- **9.2.2:** Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'
- **9.3.2:** Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)'
- **18.3.1:** Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled'
- **18.8.36.1:** Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'
- **18.8.36.2:** Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'

# Lateral Movement

## Overview

Lateral movement allows CTAs to move through a victim's environment. It can be used to accomplish two things: explore the network to identify targets and subsequently gain access to those targets. CTAs can use custom-made remote tools or legitimate credentials with native network and operating system tools.

CTAs can use WMI to conduct lateral movement:

- **T1021 Remote Services:** The Win32\_Service WMI class represents a service that can be in a remote location. CTAs can use the WMI Win32\_Service class to enumerate the services installed on a computer. In addition, they can use this class to determine whether those services are currently running, return any other required information about that service, and its configuration.
- **T1021.006 Remote Services - Windows Remote Management:** WMI supplies management data for WinRM. WinRM allows systems to access or exchange management information across a common network.

## Recommendations

### CIS Controls v8

- **Safeguard 2.3 (IG1):** Address Unauthorized Software
- **Safeguard 2.5 (IG2):** Allowlist Authorized Software
- **Safeguard 3.12 (IG2):** Segment Data Processing and Storage Based on Sensitivity
- **Safeguard 4.1 (IG1):** Establish and Maintain a Secure Configuration Process
- **Safeguard 4.4 (IG1):** Implement and Manage a Firewall on Servers
- **Safeguard 4.5 (IG1):** Implement and Manage a Firewall on End-User Devices
- **Safeguard 4.7 (IG1):** Manage Default Accounts on Enterprise Assets and Software
- **Safeguard 4.8 (IG2):** Uninstall or Disable Unnecessary Services on Enterprise Assets and Software
- **Safeguard 5.3 (IG1):** Disable Dormant Accounts
- **Safeguard 5.4 (IG1):** Restrict Administrator Privileges to Dedicated Administrator Accounts
- **Safeguard 6.1 (IG1):** Establish an Access Granting Process
- **Safeguard 6.2 (IG1):** Establish an Access Revoking Process
- **Safeguard 6.4 (IG1):** Require MFA for Remote Network Access
- **Safeguard 6.5 (IG1):** Require MFA for Administrative Access
- **Safeguard 6.8 (IG2):** Define and Maintain Role-Based Access Control
- **Safeguard 7.6 (IG2):** Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets
- **Safeguard 7.7 (IG2):** Remediate Detected Vulnerabilities
- **Safeguard 12.2 (IG2):** Establish and Maintain a Secure Network Architecture
- **Safeguard 12.7 (IG2):** Ensure Remote Devices Utilize a VPN and Are Connecting to an Enterprise's AAA Infrastructure
- **Safeguard 12.8 (IG3):** Establish and Maintain Dedicated Computing Resources for All Administrative Work
- **Safeguard 13.3 (IG2):** Deploy a Network Intrusion Detection Solution
- **Safeguard 13.8 (IG3):** Deploy a Network Intrusion Prevention Solution

- **Safeguard 18.3 (IG2):** Remediate Penetration Test Findings
- **Safeguard 18.5 (IG3):** Perform Periodic Internal Penetration Tests

### **CIS Microsoft Windows 10 Enterprise Release 21H1 Benchmark v1.11.0**

- **2.2.2:** Ensure 'Access this computer from the network' is set to 'Administrators, Remote Desktop Users'
- **2.2.6:** Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users'
- **2.2.16:** Ensure 'Deny access to this computer from the network' to include 'Guests, Local account'
- **2.2.20:** Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account'
- **2.3.1.4:** Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'
- **2.3.8.1:** Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'
- **2.3.8.2:** Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled'
- **2.3.8.3:** Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled'
- **2.3.9.2:** Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'
- **2.3.9.3 Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'**
- **5.11:** Ensure 'Microsoft FTP Service (FTPSVC)' is set to 'Disabled' or 'Not Installed'
- **5.13:** Ensure 'OpenSSH SSH Server (sshd)' is set to 'Disabled' or 'Not Installed'
- **5.21:** Ensure 'Remote Desktop Services (TermService)' is set to 'Disabled'
- **5.39:** Ensure 'Windows Remote Management (WS-Management) (WinRM)' is set to 'Disabled'
- **9.1.1:** Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'
- **9.1.2:** Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'
- **9.2.1:** Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)'
- **9.2.2:** Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'
- **9.3.1:** Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'
- **9.3.2:** Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)'
- **18.3.1:** Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled'
- **18.3.2:** Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)'
- **18.3.3:** Ensure 'Configure SMB v1 server' is set to 'Disabled'
- **18.5.8.1:** Ensure 'Enable insecure guest logons' is set to 'Disabled'

- **18.8.36.1:** Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'
- **18.8.36.2:** Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'
- **18.9.63.3.2.1:** Ensure 'Allow users to connect remotely by using Remote Desktop Services' is set to 'Disabled'
- **18.9.63.3.10.2:** Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute'
- **18.9.98.2.2:** Ensure 'Allow remote server management through WinRM' is set to 'Disabled'
- **18.9.98.2.4:** Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled'
- **18.9.99.1:** Ensure 'Allow Remote Shell Access' is set to 'Disabled'

# Command and Control

## Overview

Command and control allows a CTA to communicate with compromised systems and infrastructure. Command and control can be used to disseminate commands to steal data, spread malware, disrupt web services, and more. It can also assist CTAs in conducting lateral movement within a victim's network.

CTAs can use WMI classes to establish command and control:

- **T1105 Ingress Tool Transfer:** Can be achieved using the Win32\_Share WMI class.
- **T1219 Remote Access Software:** ManagementScope.Connect method connects the scope object to a WMI namespace on a remote computer. Calling it, explicitly, allows CTAs to control the time of the connection. The method will return within two minutes.
- **T1571 Non-Standard Port:** WMI calls use port 135 and then choose a random port.

## Recommendations

### CIS Controls v8

- **Safeguard 2.5 (IG2):** Allowlist Authorized Software
- **Safeguard 4.2 (IG1):** Establish and Maintain a Secure Configuration Process for Network Infrastructure
- **Safeguard 4.4 (IG1):** Implement and Manage a Firewall on Servers
- **Safeguard 7.6 (IG2):** Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets
- **Safeguard 9.3 (IG2):** Maintain and Enforce Network-Based URL Filters
- **Safeguard 13.3 (IG2):** Deploy a Network Intrusion Detection Solution
- **Safeguard 13.4 (IG2):** Perform Traffic Filtering Between Network Segments
- **Safeguard 13.8 (IG3):** Deploy a Network Intrusion Prevention Solution
- **Safeguard 18.2 (IG2):** Perform Periodic External Penetration Tests
- **Safeguard 18.3 (IG2):** Remediate Penetration Test Findings

### CIS Microsoft Windows 10 Enterprise Release 21H1 Benchmark v1.11.0

- **5.11:** Ensure 'Microsoft FTP Service (FTPSVC)' is set to 'Disabled' or 'Not Installed'
- **9.1.2:** Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'
- **9.2.2:** Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'
- **9.3.2:** Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)'
- **18.8.36.1:** Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'
- **18.8.36.2:** Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'

# Exfiltration

## Overview

Exfiltration consists of techniques that CTAs can use to steal data from a network. Once CTAs have collected data, they often package it to avoid detection while removing it. Exfiltration can include compression and encryption. Techniques for getting data out of a target network typically include transferring it over a command and control channel and may include putting size limits on the transmission.

CTAs can use WMI to exfiltrate data by:

- **T1041 Exfiltration Over C2 Channel:** Exfiltration can be achieved using the ManagementScope object connected to a namespace on a remote computer.

## Recommendations

### CIS Controls v8

- **Safeguard 13.3 (IG2):** Deploy a Network Intrusion Detection Solution
- **Safeguard 13.8 (IG3):** Deploy a Network Intrusion Prevention Solution

### CIS Microsoft Windows 10 Enterprise Release 21H1 Benchmark v1.11.0

- **None**



# Conclusion

Most cyber-attacks, including those that are facilitated through exploitation of WMI, occur due to a lack of good, essential cyber hygiene. This guide shows that implementing Safeguards in IG1, or essential cyber hygiene, such as account management, restricting administrative privileges to dedicated accounts, access control, and disconnecting idle sessions are some great ways that an enterprise can defend against these types of attacks. By implementing the security best practices recommended in this guide, enterprises can apply a defense-in-depth strategy to strengthen their cybersecurity posture and help better defend against WMI-based attacks.

# WMI Mapping to MITRE ATT&CK

**Layer** | **Domain:** Enterprise ATT&CK v10 | **Platforms:** Linux®, macOS®, Windows®, Office 365®, Azure® AD, IaaS, SaaS, PRE, Network, Google Workspace, Containers

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Gather Victim Host Information	Compromise Accounts	Exploit Public-Facing Application	AppleScript	BITS Jobs	Access Token Manipulation	Brute Force	Credentials from Password Stores	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information	Compromise Infrastructure	External Remote Services	JavaScript	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	Credentials from Password Stores	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Gather Victim Network Information	Develop Capabilities	Hardware Additions	Network Device CLI	Active Setup	Boot or Logon Initialization Scripts	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation
Gather Victim Org Information	Establish Accounts	Phishing	PowerShell	Authentication Package	Create or Modify System Process	Deobfuscate/Decode Files or Information	Forge Web Credentials	Cloud Service Dashboard	Remote Services	Browser Session Hijacking	Dynamic Resolution	Exfiltration Over Other Network Medium	Disk Wipe
Phishing for Information	Obtain Capabilities	Replication Through Removable Media	Python	Kernel Modules and Extensions	Domain Policy Modification	Deploy Container	Input Capture	Cloud Service Discovery	Distributed Component Object Model	Clipboard Data	Encrypted Channel	Exfiltration Over Physical Medium	Endpoint Denial of Service
Search Closed Sources	Stage Capabilities	Supply Chain Compromise	Unix Shell	Login Items	Escape to Host	Direct Volume Access	Modify Authentication Process	Cloud Storage Object Discovery	Remote Desktop Protocol	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service	Firmware Corruption
Search Open Technical Databases		Trusted Relationship	Visual Basic	LSASS Driver	Event Triggered Execution	Domain Policy Modification	Network Sniffing	Container and Resource Discovery	SMB/Windows Admin Shares	Data from Configuration Repository	Ingress Tool Transfer	Exfiltration Over Physical Medium	Inhibit System Recovery
Search Open Websites/ Domains		Valid Accounts	Windows Command Shell	Plist Modification	Exploitation for Privilege Escalation	Execution Guardrails	OS Credential Dumping	Domain Trust Discovery	SSH	Data from Information Repositories	Multi-Stage Channels	Exfiltration Over Web Service	Network Denial of Service
Search Victim-Owned Websites			Container Administration Command	Port Monitors	Hijack Execution Flow	Exploitation for Defense Evasion	Steal Application Access Token	File and Directory Discovery	VNC	Data from Local System	Non-Application Layer Protocol	Scheduled Transfer	Resource Hijacking
			Deploy Container	Print Processors	Process Injection	Hide Artifacts	Steal or Forge Kerberos Tickets	File and Directory Permissions Modification	Windows Remote Management	Data from Network Shared Drive	Non-Standard Port	Transfer Data to Cloud Account	Service Stop
			Exploitation for Client Execution	Re-opened Applications	Scheduled Task/Job	Hijack Execution Flow	Steal Web Session Cookie	Impair Defenses	Replication Through Removable Media	Data from Network Shared Drive	Protocol Tunneling		System Shutdown/Reboot
			Inter-Process Communication	Registry Run Keys / Startup Folder	Valid Accounts	Process Injection	Two-Factor Authentication Interception	Impair Defenses	Software Deployment Tools	Data from Removable Media	Web Service		
			Component Object Model	Security Support Provider		Hijack Execution Flow	Unsecured Credentials	Disable Cloud Logs	Taint Shared Content	Email Collection			
			Dynamic Data Exchange	Shortcut Modification		Impair Defenses		Disable or Modify Cloud Firewall	Use Alternate Authentication Material	Input Capture			
			Native API	Time Providers		Disable or Modify System Firewall		Disable or Modify System Firewall		Screen Capture			
			Scheduled Task/Job	Winlogon Helper DLL		Disable or Modify Tools		Disable Windows Event Logging		Video Capture			
			Shared Modules	XDG Autostart Entries		Disable or Modify Tools		Downgrade Attack					
			Software Deployment Tools	Boot or Logon Initialization Scripts		Indicator Removal on Host		Impair Command History Logging					
			System Services	Browser Extensions		Indirect Command Execution		Indicator Blocking					
			User Execution	Compromise Client Software Binary		Masquerading		Safe Mode Boot					
			Windows Management Instrumentation	Create Account		Modify Authentication Process		Process Injection					
				Create or Modify System Process		Modify Cloud Compute Infrastructure		Reflective Code Loading					
				Event Triggered Execution		Modify Registry		Rogue Domain Controller					
				Accessibility Features		Modify System Image		Rootkit					
				AppCert DLLs		Network Boundary Bridging		Signed Binary Proxy Execution					
				Applnit DLLs		Obfuscated Files or Information		Signed Script Proxy Execution					
				Application Shimming		Pre-OS Boot		Subvert Trust Controls					
				Change Default File Association		Process Injection		Template Injection					
				Component Object Model Hijacking		Reflective Code Loading		Traffic Signaling					
				Emond		Rogue Domain Controller		Trusted Developer Utilities Proxy Execution					
				Image File Execution Options Injection		Rootkit		Unused/Unsupported Cloud Regions					
				LC_LOAD_DYLIB Addition		Signed Binary Proxy Execution		Use Alternate Authentication Material					
				Netsh Helper DLL		Subvert Trust Controls		Valid Accounts					
				PowerShell Profile		Template Injection		Virtualization/Sandbox Evasion					
				Screensaver		Traffic Signaling		Weaken Encryption					
				Trap		Trusted Developer Utilities Proxy Execution		XSL Script Processing					
				Unix Shell Configuration Modification		Trusted Developer Utilities Proxy Execution							
				Windows Management Instrumentation Event Subscription		Trusted Developer Utilities Proxy Execution							
				External Remote Services		Trusted Developer Utilities Proxy Execution							
				Hijack Execution Flow		Trusted Developer Utilities Proxy Execution							
				Implant Internal Image		Trusted Developer Utilities Proxy Execution							
				Modify Authentication Process		Trusted Developer Utilities Proxy Execution							
				Office Application Startup		Trusted Developer Utilities Proxy Execution							
				Pre-OS Boot		Trusted Developer Utilities Proxy Execution							
				Scheduled Task/Job		Trusted Developer Utilities Proxy Execution							
				Server Software Component		Trusted Developer Utilities Proxy Execution							
				Traffic Signaling		Trusted Developer Utilities Proxy Execution							
				Valid Accounts		Trusted Developer Utilities Proxy Execution							

# CIS Controls

## Implementation Groups

CIS Controls v7.1 introduced Implementation Groups (IGs) to provide granularity and some explicit structure to the different realities faced by enterprises of varied sizes.



The number of Safeguards an enterprise is expected to implement increases based on which group the enterprise falls into.

**153**  
TOTAL SAFEGUARDS

**IG3** assists enterprises with IT security experts to secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.

**23**  
SAFEGUARDS

**IG2** assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

**74**  
SAFEGUARDS

**IG1** is the definition of essential cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.

**56**  
SAFEGUARDS

### IG1

A Group 1 enterprise is small to medium-sized with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel. The principal concern of these enterprises is to keep the business operational, as they have a limited tolerance for downtime. The sensitivity of the data they are trying to protect is low and principally involves employee and financial information. However, there may be some small to medium-sized enterprises that are responsible for protecting sensitive data and, therefore, will fall into a higher group. Safeguards for Group 1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These Safeguards will also typically be designed to work in conjunction with small or home office commercial-off-the-shelf (COTS) hardware and software.

## IG2

A Group 2 enterprise employs individuals responsible for managing and protecting IT infrastructure. These enterprises support multiple departments with different risk profiles based on job function and mission. Small organizational units may have regular compliance burdens. Group 2 enterprises often store and process sensitive client or company information and can withstand short interruptions of service. A major concern is loss of public confidence if a breach occurs. Safeguards selected for Group 2 help security teams cope with increased operational complexity. Some Safeguards will depend on enterprise-grade technology and specialized expertise to properly install and configure.

## IG3

A Group 3 enterprise employs security experts that specialize in the different facets of cybersecurity (e.g., risk management, penetration testing, application security). Group 3 systems and data contain sensitive information or functions that are subject to regulatory and compliance oversight. A Group 3 enterprise must address availability of services and the confidentiality and integrity of sensitive data. Successful attacks can cause significant harm to the public welfare. Safeguards selected for Group 3 must abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks.

If you would like to know more about the Implementation Groups and how they pertain to enterprises of all sizes, there are many resources that explore the Implementation Groups and the CIS Controls in general on our website at <https://www.cisecurity.org/controls/cis-controls-list/>.

## CIS Safeguards

Below is a list of CIS Safeguards associated with securing WMI.

Control	Safeguard	CIS Control Title	Asset Type	Security Function	IG1	IG2	IG3
2	2.3	<a href="#">Address Unauthorized Software</a>	Applications	Respond	●	●	●
2	2.5	<a href="#">Allowlist Authorized Software</a>	Applications	Protect		●	●
2	2.7	<a href="#">Allowlist Authorized Scripts</a>	Applications	Protect			●
3	3.3	<a href="#">Configure Data Access Control Lists</a>	Data	Protect	●	●	●
3	3.12	<a href="#">Segment Data Processing and Storage Based on Sensitivity</a>	Network	Protect		●	●
4	4.1	<a href="#">Establish and Maintain a Secure Configuration Process</a>	Applications	Protect	●	●	●
4	4.2	<a href="#">Establish and Maintain a Secure Configuration Process for Network Infrastructure</a>	Network	Protect	●	●	●
4	4.4	<a href="#">Implement and Manage a Firewall on Servers</a>	Devices	Protect	●	●	●
4	4.5	<a href="#">Implement and Manage a Firewall on End-User Devices</a>	Devices	Protect	●	●	●
4	4.7	<a href="#">Manage Default Accounts on Enterprise Assets and Software</a>	Users	Protect	●	●	●
4	4.8	<a href="#">Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</a>	Devices	Protect		●	●
5	5.2	<a href="#">Use Unique Passwords</a>	Users	Protect	●	●	●
5	5.3	<a href="#">Disable Dormant Accounts</a>	Users	Respond	●	●	●

Control	Safeguard	CIS Control Title	Asset Type	Security Function	IG1	IG2	IG3
5	5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	Users	Protect	●	●	●
6	6.1	Establish an Access Granting Process	Users	Protect	●	●	●
6	6.2	Establish an Access Revoking Process	Users	Protect	●	●	●
6	6.3	Require MFA for Externally-Exposed Applications	Users	Protect	●	●	●
6	6.4	Require MFA for Remote Network Access	Users	Protect	●	●	●
6	6.5	Require MFA for Administrative Access	Users	Protect	●	●	●
6	6.8	Define and Maintain Role-Based Access Control	Data	Protect		●	●
7	7.6	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets	Applications	Identify		●	●
7	7.7	Remediate Detected Vulnerabilities	Applications	Respond		●	●
9	9.3	Maintain and Enforce Network-Based URL Filters	Network	Protect		●	●
9	9.7	Deploy and Maintain Email Server Anti-Malware Protections	Network	Protect			●
10	10.1	Deploy and Maintain Anti-Malware Software	Devices	Protect	●	●	●
10	10.2	Configure Automatic Anti-Malware Signature Updates	Devices	Protect	●	●	●
10	10.7	Use Behavior-Based Anti-Malware Software	Devices	Detect		●	●
12	12.2	Establish and Maintain a Secure Network Architecture	Network	Protect		●	●
12	12.7	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure	Devices	Protect		●	●
12	12.8	Establish and Maintain Dedicated Computing Resources for All Administrative Work	Devices	Protect			●
13	13.2	Deploy a Host-Based Intrusion Detection Solution	Devices	Detect		●	●
13	13.3	Deploy a Network Intrusion Detection Solution	Network	Detect		●	●
13	13.4	Perform Traffic Filtering Between Network Segments	Network	Protect		●	●
13	13.5	Manage Access Control for Remote Assets	Devices	Protect		●	●
13	13.7	Deploy a Host-Based Intrusion Prevention Solution	Devices	Protect			●
13	13.8	Deploy a Network Intrusion Prevention Solution	Network	Protect			●
13	13.10	Perform Application Layer Filtering	Network	Protect			●
16	16.8	Separate Production and Non-Production Systems	Applications	Protect		●	●
16	16.10	Apply Secure Design Principles in Application Architectures	Applications	Protect		●	●
18	18.2	Perform Periodic External Penetration Tests	Network	Identify		●	●
18	18.3	Remediate Penetration Test Findings	Network	Protect		●	●
18	18.5	Perform Periodic Internal Penetration Tests	N/A	Identify			●

# CIS Benchmarks

## CIS Benchmarks: WMI-Related Recommendations

Below is a list of CIS Benchmarks associated with securing WMI. Note that each Benchmark is designated with Level 1 (L1) or Level 2 (L2). The Level 1 profile is considered a base recommendation that can be implemented fairly promptly and is designed to not have an extensive performance impact. The intent of the Level 1 profile Benchmark is to lower the attack surface of an organization while keeping machines usable and not hindering business functionality.

The Level 2 profile is considered to be “defense-in-depth” and is intended for environments where security is paramount. The recommendations associated with the Level 2 profile can have an adverse effect on an organization if not implemented appropriately or without due care.

Benchmark Section	Benchmark Recommendation	Benchmark Profile	Benchmark Title/Description
2.2	2.2.2	L1	<b>Ensure 'Access this computer from the network' is set to 'Administrators, Remote Desktop Users'</b> This policy setting allows other users on the network to connect to the computer and is required by various network protocols that include Server Message Block (SMB)-based protocols, NetBIOS, Common Internet File System (CIFS), and Component Object Model Plus (COM+). The recommended state for this setting is: Administrators, Remote Desktop Users.
2.2	2.2.6	L1	<b>Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users'</b> This policy setting determines which users or groups have the right to log on as a Remote Desktop Services client. If your organization uses Remote Assistance as part of its help desk strategy, create a group and assign it this user right through Group Policy. If the help desk in your organization does not use Remote Assistance, assign this user right only to the Administrators group or use the Restricted Groups feature to ensure that no user accounts are part of the Remote Desktop Users group. Restrict this user right to the Administrators group, and possibly the Remote Desktop Users group, to prevent unwanted users from gaining access to computers on your network by means of the Remote Assistance feature. The recommended state for this setting is: Administrators, Remote Desktop Users.
2.2	2.2.8	L1	<b>Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE'</b> This policy setting determines which users and groups can change the time and date on the internal clock of the computers in your environment. Users who are assigned this user right can affect the appearance of event logs. When a computer's time setting is changed, logged events reflect the new time, not the actual time that the events occurred. The recommended state for this setting is: Administrators, LOCAL SERVICE.
2.2	2.2.9	L1	<b>Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE, Users'</b> This setting determines which users can change the time zone of the computer. This ability holds no great danger for the computer and may be useful for mobile workers. The recommended state for this setting is: Administrators, LOCAL SERVICE, Users.
2.2	2.2.13	L1	<b>Ensure 'Create permanent shared objects' is set to 'No One'</b> This user right is useful to kernel-mode components that extend the object namespace. However, components that run in kernel mode have this user right inherently. Therefore, it is typically not necessary to specifically assign this user right. The recommended state for this setting is: No One.

Benchmark Section	Benchmark Recommendation	Benchmark Profile	Benchmark Title/Description
2.2	2.2.15	L1	<p><b>Ensure 'Debug programs' is set to 'Administrators'</b></p> <p>This policy setting determines which user accounts will have the right to attach a debugger to any process or to the kernel, which provides complete access to sensitive and critical operating system components. Developers who are debugging their own applications do not need to be assigned this user right; however, developers who are debugging new system components will need it. The recommended state for this setting is: Administrators</p>
2.2	2.2.16	L1	<p><b>Ensure 'Deny access to this computer from the network' to include 'Guests, Local account'</b></p> <p>This policy setting prohibits users from connecting to a computer from across the network, which would allow users to access and potentially modify data remotely. In high security environments, there should be no need for remote users to access data on a computer. Instead, file sharing should be accomplished through the use of network servers. This user right supersedes the Access this computer from the network user right if an account is subject to both policies. The recommended state for this setting is to include: Guests, Local account.</p>
2.2	2.2.17	L1	<p><b>Ensure 'Deny log on as a batch job' to include 'Guests'</b></p> <p>This policy setting determines which accounts will not be able to log on to the computer as a batch job. A batch job is not a batch (.bat) file, but rather a batch-queue facility. Accounts that use the Task Scheduler to schedule jobs need this user right. This user right supersedes the Log on as a batch job user right, which could be used to allow accounts to schedule jobs that consume excessive system resources. Such an occurrence could cause a DoS condition. Failure to assign this user right to the recommended accounts can be a security risk. The recommended state for this setting is to include: Guests.</p>
2.2	2.2.20	L1	<p><b>Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account'</b></p> <p>This policy setting determines whether users can log on as Remote Desktop clients. After the baseline workstation is joined to a domain environment, there is no need to use local accounts to access the workstation from the network. Domain accounts can access the workstation for administration and end-user processing. This user right supersedes the Allow log on through Remote Desktop Services user right if an account is subject to both policies. The recommended state for this setting is to include: Guests, Local account.</p>
2.2	2.2.23	L1	<p><b>Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE'</b></p> <p>This policy setting determines which users or processes can generate audit records in the Security log. The recommended state for this setting is: LOCAL SERVICE, NETWORK SERVICE</p>
2.2	2.2.28	L2	<p><b>Ensure 'Log on as a batch job' is set to 'Administrators'</b></p> <p>This policy setting allows accounts to log on using the task scheduler service. Because the task scheduler is often used for administrative purposes, it may be needed in enterprise environments. However, its use should be restricted in high security environments to prevent misuse of system resources or to prevent attackers from using the right to launch malicious code after gaining user level access to a computer. The recommended state for this setting is: Administrators.</p>
2.2	2.2.30	L1	<p><b>Ensure 'Manage auditing and security log' is set to 'Administrators'</b></p> <p>This policy setting determines which users can change the auditing options for files and directories and clear the Security log. The recommended state for this setting is: Administrators</p>
2.2	2.2.34	L1	<p><b>Ensure 'Profile single process' is set to 'Administrators'</b></p> <p>This policy setting determines which users can use tools to monitor the performance of non-system processes. Typically, you do not need to configure this user right to use the Microsoft Management Console (MMC) Performance snap-in. However, you do need this user right if System Monitor is configured to collect data using Windows Management Instrumentation (WMI). Restricting the Profile single process user right prevents intruders from gaining additional information that could be used to mount an attack on the system. The recommended state for this setting is: Administrators.</p>
2.2	2.2.35	L1	<p><b>Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost'</b></p> <p>This policy setting allows users to use tools to view the performance of different system processes, which could be abused to allow attackers to determine a system's active processes and provide insight into the potential attack surface of the computer. The recommended state for this setting is: Administrators, NT SERVICE\WdiServiceHost.</p>



Benchmark Section	Benchmark Recommendation	Benchmark Profile	Benchmark Title/Description
2.2	2.2.39	L1	<p><b>Ensure 'Take ownership of files or other objects' is set to 'Administrators'</b></p> <p>This policy setting allows users to take ownership of files, folders, registry keys, processes, or threads. This user right bypasses any permissions that are in place to protect objects to give ownership to the specified user. The recommended state for this setting is: Administrators.</p>
2.3.1	2.3.1.4	L1	<p><b>Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'</b></p> <p>This policy setting determines whether local accounts that are not password protected can be used to log on from locations other than the physical computer console. If you enable this policy setting, local accounts that have blank passwords will not be able to log on to the network from remote client computers. Such accounts will only be able to log on at the keyboard of the computer. The recommended state for this setting is: Enabled</p>
2.3.7	2.3.7.2	L1	<p><b>Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled'</b></p> <p>This policy setting determines whether the account name of the last user to log on to the client computers in your organization will be displayed in each computer's respective Windows logon screen. Enable this policy setting to prevent intruders from collecting account names visually from the screens of desktop or laptop computers in your organization. The recommended state for this setting is: Enabled</p>
2.3.8	2.3.8.1	L1	<p><b>Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'</b></p> <p>This policy setting determines whether packet signing is required by the SMB client component.</p>
2.3.8	2.3.8.2	L1	<p><b>Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled'</b></p> <p>This policy setting determines whether the SMB client will attempt to negotiate SMB packet signing.</p>
2.3.8	2.3.8.3	L1	<p><b>Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled'</b></p> <p>This policy setting determines whether the SMB redirector will send plaintext passwords during authentication to third-party SMB servers that do not support password encryption. It is recommended that you disable this policy setting unless there is a strong business case to enable it. If this policy setting is enabled, unencrypted passwords will be allowed across the network. The recommended state for this setting is: Disabled.</p>
2.3.9	2.3.9.2	L1	<p><b>Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'</b></p> <p>This policy setting determines whether packet signing is required by the SMB server component. Enable this policy setting in a mixed environment to prevent downstream clients from using the workstation as a network server. The recommended state for this setting is: Enabled</p>
2.3.9	2.3.9.3	L1	<p><b>Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'</b></p> <p>This policy setting determines whether the SMB server will negotiate SMB packet signing with clients that request it. If no signing request comes from the client, a connection will be allowed without a signature if the Microsoft network server: Digitally sign communications (always) setting is not enabled</p>
2.3.10	2.3.10.1	L1	<p><b>Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'</b></p> <p>This policy setting determines whether an anonymous user can request security identifier (SID) attributes for another user, or use a SID to obtain its corresponding user name. The recommended state for this setting is: Disabled.</p>
2.3.10	2.3.10.2	L1	<p><b>Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled'</b></p> <p>This policy setting controls the ability of anonymous users to enumerate the accounts in the Security Accounts Manager (SAM). If you enable this policy setting, users with anonymous connections will not be able to enumerate domain account user names on the systems in your environment. This policy setting also allows additional restrictions on anonymous connections. The recommended state for this setting is: Enabled.</p>



Benchmark Section	Benchmark Recommendation	Benchmark Profile	Benchmark Title/Description
2.3.10	2.3.10.3	L1	<p><b>Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled'</b></p> <p>This policy setting controls the ability of anonymous users to enumerate SAM accounts as well as shares. If you enable this policy setting, anonymous users will not be able to enumerate domain account user names and network share names on the systems in your environment. The recommended state for this setting is: Enabled.</p>
2.3.10	2.3.10.5	L1	<p><b>Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'</b></p> <p>This policy setting determines what additional permissions are assigned for anonymous connections to the computer. The recommended state for this setting is: Disabled</p>
2.3.10	2.3.10.7	L1	<p><b>Ensure 'Network access: Remotely accessible registry paths'</b></p> <p>This policy setting determines which registry paths will be accessible over the network, regardless of the users or groups listed in the access control list (ACL) of the winreg registry key.</p>
2.3.10	2.3.10.8	L1	<p><b>Ensure 'Network access: Remotely accessible registry paths and sub-paths'</b></p> <p>This policy setting determines which registry paths and sub-paths will be accessible over the network, regardless of the users or groups listed in the access control list (ACL) of the winreg registry key.</p>
2.3.10	2.3.10.9	L1	<p><b>Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled'</b></p> <p>When enabled, this policy setting restricts anonymous access to only those shares and pipes that are named in the Network access: Named pipes that can be accessed anonymously and Network access: Shares that can be accessed anonymously settings. This policy setting controls null session access to shares on your computers by adding RestrictNullSessAccesswith the value 1 in the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters registry key. This registry value toggles null session shares on or off to control whether the server service restricts unauthenticated clients' access to named resources. The recommended state for this setting is: Enabled.</p>
2.3.10	2.3.10.10	L1	<p><b>Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow'</b></p> <p>This policy setting allows you to restrict remote RPC connections to SAM. The recommended state for this setting is: Administrators: Remote Access: Allow</p>
5	5.1	L2	<p><b>Ensure 'Bluetooth Audio Gateway Service (BTAGService)' is set to 'Disabled'</b></p> <p>Service supporting the audio gateway role of the Bluetooth Handsfree Profile. The recommended state for this setting is: Disabled</p>
5	5.3	L1	<p><b>Ensure 'Computer Browser (Browser)' is set to 'Disabled' or 'Not Installed'</b></p> <p>Maintains an updated list of computers on the network and supplies this list to computers designated as browsers. The recommended state for this setting is: Disabled or Not Installed</p>
5	5.9	L2	<p><b>Ensure 'Link-Layer Topology Discovery Mapper (lltdsvc)' is set to 'Disabled'</b></p> <p>Creates a Network Map, consisting of PC and device topology (connectivity) information, and metadata describing each PC and device. The recommended state for this setting is: Disabled</p>
5	5.11	L1	<p><b>Ensure 'Microsoft FTP Service (FTPSVC)' is set to 'Disabled' or 'Not Installed'</b></p> <p>Enables the server to be a File Transfer Protocol (FTP) server. The recommended state for this setting is: Disabled or Not Installed.</p>
5	5.13	L1	<p><b>Ensure 'OpenSSH SSH Server (sshd)' is set to 'Disabled' or 'Not Installed'</b></p> <p>This service provides infrastructure support for the Microsoft Store. The recommended state for this setting is: Disabled.</p>
5	5.21	L2	<p><b>Ensure 'Remote Desktop Services (TermService)' is set to 'Disabled'</b></p> <p>Remote Desktop Configuration service (RDCS) is responsible for all Remote Desktop related configuration and session maintenance activities that require SYSTEM context. These include per-session temporary folders, RD themes, and RD certificates. The recommended state for this setting is: Disabled.</p>

Benchmark Section	Benchmark Recommendation	Benchmark Profile	Benchmark Title/Description
5	5.24	L2	<p><b>Ensure 'Remote Registry (RemoteRegistry)' is set to 'Disabled'</b></p> <p>In Windows 2003 and older versions of Windows, the Remote Procedure Call (RPC) Locator service manages the RPC name service database. In Windows Vista and newer versions of Windows, this service does not provide any functionality and is present for application compatibility. The recommended state for this setting is: Disabled</p>
5	5.26	L2	<p><b>Ensure 'Server (LanmanServer)' is set to 'Disabled'</b></p> <p>Offers routing services to businesses in local area and wide area network environments. The recommended state for this setting is: Disabled.</p>
5	5.29	L1	<p><b>Ensure 'Special Administration Console Helper (sacsvr)' is set to 'Disabled' or 'Not Installed'</b></p> <p>Enables Simple Network Management Protocol (SNMP) requests to be processed by this computer. The recommended state for this setting is: Disabled or Not Installed.</p>
5	5.31	L1	<p><b>Ensure 'UPnP Device Host (upnphost)' is set to 'Disabled'</b></p> <p>Allows UPnP devices to be hosted on this computer. The recommended state for this setting is: Disabled</p>
5	5.39	L2	<p><b>Ensure 'Windows Remote Management (WS-Management) (WinRM)' is set to 'Disabled'</b></p> <p>Windows Remote Management (WinRM) service implements the WS-Management protocol for remote management. WS-Management is a standard web services protocol used for remote software and hardware management. The WinRM service listens on the network for WS-Management requests and processes them. The recommended state for this setting is: Disabled</p>
5	5.41	L1	<p><b>Ensure 'Xbox Accessory Management Service (XboxGipSvc)' is set to 'Disabled'</b></p> <p>This service manages connected Xbox Accessories. The recommended state for this setting is: Disabled.</p>
9.1	9.1.1	L1	<p><b>Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'</b></p> <p>Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile. The recommended state for this setting is: On (recommended)</p>
9.1	9.1.2	L1	<p><b>Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'</b></p> <p>This setting determines the behavior for inbound connections that do not match an inbound firewall rule. The recommended state for this setting is: Block (default).</p>
9.2	9.2.1	L1	<p><b>Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)'</b></p> <p>Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile. The recommended state for this setting is: On (recommended)</p>
9.2	9.2.2	L1	<p><b>Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'</b></p> <p>This setting determines the behavior for inbound connections that do not match an inbound firewall rule. The recommended state for this setting is: Block (default)</p>
9.3	9.3.1	L1	<p><b>Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'</b></p> <p>Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile. The recommended state for this setting is: On (recommended).</p>
9.3	9.3.2	L1	<p><b>Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)'</b></p> <p>This setting determines the behavior for inbound connections that do not match an inbound firewall rule. The recommended state for this setting is: Block (default).</p>

Benchmark Section	Benchmark Recommendation	Benchmark Profile	Benchmark Title/Description
18.3	18.3.1	L1	<p><b>Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled'</b></p> <p>This setting controls whether local accounts can be used for remote administration via network logon (e.g., NET USE, connecting to C\$, etc.). Local accounts are at high risk for credential theft when the same account and password is configured on multiple systems. Enabling this policy significantly reduces that risk</p>
18.3	18.3.2	L1	<p><b>Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)'</b></p> <p>This setting configures the start type for the Server Message Block version 1 (SMBv1) client driver service (MRxSmb10), which is recommended to be disabled. The recommended state for this setting is: Enabled: Disable driver (recommended).</p>
18.3	18.3.3	L1	<p><b>Ensure 'Configure SMB v1 server' is set to 'Disabled'</b></p> <p>This setting configures the server-side processing of the Server Message Block version 1 (SMBv1) protocol. The recommended state for this setting is: Disabled.</p>
18.5.8	18.5.8.1	L1	<p><b>Ensure 'Enable insecure guest logons' is set to 'Disabled'</b></p> <p>This policy setting determines if the SMB client will allow insecure guest logons to an SMB server. The recommended state for this setting is: Disabled.</p>
18.5.11	18.5.11.4	L1	<p><b>Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled'</b></p> <p>This policy setting determines whether to require domain users to elevate when setting a network's location. The recommended state for this setting is: Enabled.</p>
18.5.20	18.5.20.1	L2	<p><b>Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled'</b></p> <p>This policy setting allows the configuration of wireless settings using Windows Connect Now (WCN). The WCN Registrar enables the discovery and configuration of devices over Ethernet (UPnP) over in-band 802.11 Wi-Fi through the Windows Portable Device API (WPD) and via USB Flash drives. Additional options are available to allow discovery and configuration over a specific medium. The recommended state for this setting is: Disabled.</p>
18.5.20	18.5.20.2	L2	<p><b>Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled'</b></p> <p>This policy setting prohibits access to Windows Connect Now (WCN) wizards. The recommended state for this setting is: Enabled</p>
18.8.5	18.8.5.3	NG	<p><b>Ensure 'Turn On Virtualization Based Security: Virtualization Based Protection of Code Integrity' is set to 'Enabled with UEFI lock'</b></p> <p>This setting enables virtualization based protection of Kernel Mode Code Integrity. When this is enabled, kernel mode memory protections are enforced and the Code Integrity validation path is protected by the Virtualization Based Security feature. The recommended state for this setting is: Enabled with UEFI lock.</p>
18.8.5	18.8.5.5	NG	<p><b>Ensure 'Turn On Virtualization Based Security: Credential Guard Configuration' is set to 'Enabled with UEFI lock'</b></p> <p>This setting lets users turn on Credential Guard with virtualization-based security to help protect credentials. The "Enabled with UEFI lock" option ensures that Credential Guard cannot be disabled remotely. In order to disable the feature, you must set the Group Policy to "Disabled" as well as remove the security functionality from each computer, with a physically present user, in order to clear configuration persisted in UEFI. The recommended state for this setting is: Enabled with UEFI lock</p>
18.8.21	18.8.21.2	L1	<p><b>Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE'</b></p> <p>The "Do not apply during periodic background processing" option prevents the system from updating affected policies in the background while the computer is in use. When background updates are disabled, policy changes will not take effect until the next user logon or system restart. The recommended state for this setting is: Enabled: FALSE (unchecked).</p>
18.8.21	18.8.21.3	L1	<p><b>Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE'</b></p> <p>The "Process even if the Group Policy objects have not changed" option updates and reapplies policies even if the policies have not changed. The recommended state for this setting is: Enabled: TRUE (checked)</p>

Benchmark Section	Benchmark Recommendation	Benchmark Profile	Benchmark Title/Description
18.8.21	18.8.21.5	L1	<p><b>Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled'</b></p> <p>This policy setting prevents Group Policy from being updated while the computer is in use. This policy setting applies to Group Policy for computers, users and Domain Controllers. The recommended state for this setting is: Disabled.</p>
18.8.28	18.8.28.1	L1	<p><b>Ensure 'Block user from showing account details on sign-in' is set to 'Enabled'</b></p> <p>This policy prevents the user from showing account details (email address or user name) on the sign-in screen. The recommended state for this setting is: Enabled.</p>
18.8.28	18.8.28.3	L1	<p><b>Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled'</b></p> <p>This policy setting prevents connected users from being enumerated on domain-joined computers. The recommended state for this setting is: Enabled</p>
18.8.28	18.8.28.4	L1	<p><b>Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled'</b></p> <p>This policy setting allows local users to be enumerated on domain-joined computers. The recommended state for this setting is: Disabled</p>
18.8.34.6	18.8.34.6.1	L1	<p><b>Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled'</b></p> <p>This policy setting allows you to control the network connectivity state in standby on modern standby-capable systems. The recommended state for this setting is: Disabled.</p>
18.8.34.6	18.8.34.6.2	L1	<p><b>Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled'</b></p> <p>This policy setting allows you to control the network connectivity state in standby on modern standby-capable systems. The recommended state for this setting is: Disabled.</p>
18.8.36	18.8.36.1	L1	<p><b>Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'</b></p> <p>This policy setting allows you to turn on or turn off Offer (Unsolicited) Remote Assistance on this computer. Help desk and support personnel will not be able to proactively offer assistance, although they can still respond to user assistance requests. The recommended state for this setting is: Disabled.</p>
18.8.36	18.8.36.2	L1	<p><b>Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'</b></p> <p>This policy setting allows you to turn on or turn off Solicited (Ask for) Remote Assistance on this computer. The recommended state for this setting is: Disabled</p>
18.9.4	18.9.4.1	L2	<p><b>Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled'</b></p> <p>Manages a Windows app's ability to share data between users who have installed the app. Data is shared through the SharedLocal folder. This folder is available through the Windows.Storage API. The recommended state for this setting is: Disabled.</p>
18.9.5	18.9.5.1	L1	<p><b>Ensure 'Let Windows apps activate with voice while the system is locked' is set to 'Enabled: Force Deny'</b></p> <p>This policy setting specifies whether Windows apps can be activated by voice (apps and Cortana) while the system is locked. The recommended state for this setting is: Enabled: Force Deny</p>
18.9.15	18.9.15.2	L1	<p><b>Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled'</b></p> <p>This policy setting controls whether administrator accounts are displayed when a user attempts to elevate a running application. The recommended state for this setting is: Disabled.</p>
18.9.30	18.9.30.4	L1	<p><b>Ensure 'Turn off shell protocol protected mode' is set to 'Disabled'</b></p> <p>This policy setting allows you to configure the amount of functionality that the shell protocol can have. When using the full functionality of this protocol, applications can open folders and launch files. The protected mode reduces the functionality of this protocol allowing applications to only open a limited set of folders. Applications are not able to open files with this protocol when it is in the protected mode. It is recommended to leave this protocol in the protected mode to increase the security of Windows. The recommended state for this setting is: Disabled</p>
18.9.35	18.9.35.1	L1	<p><b>Ensure 'Prevent the computer from joining a homegroup' is set to 'Enabled'</b></p> <p>By default, users can add their computer to a HomeGroup on a home network. The recommended state for this setting is: Enabled</p>

Benchmark Section	Benchmark Recommendation	Benchmark Profile	Benchmark Title/Description
18.9.45.4.1	18.9.45.4.1.1	L1	<p><b>Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled'</b></p> <p>This policy setting controls the state for the Attack Surface Reduction (ASR) rules. The recommended state for this setting is: Enabled</p>
18.9.45.4.1	18.9.45.4.1.2	L1	<p><b>Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is 'configured'</b></p> <p>This policy setting sets the Attack Surface Reduction rules. The recommended state for this setting is: 26190899-1602-49e8-8b27-eb1d0a1ce869 - 1 (Block Office communication application from creating child processes) 3b576869-a4ec-4529-8536-b80a7769e899 - 1 (Block Office applications from creating executable content) 5beb7efe-fd9a-4556-801d-275e5ffc04cc - 1 (Block execution of potentially obfuscated scripts) 75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84 - 1 (Block Office applications from injecting code into other processes) 7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c - 1 (Block Adobe Reader from creating child processes) 92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b - 1 (Block Win32 API calls from Office macro) 9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2 - 1 (Block credential stealing from the Windows local security authority subsystem (lsass.exe)) b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4 - 1 (Block untrusted and unsigned processes that run from USB) be9ba2d9-53ea-4cdc-84e5-9b1eeee46550 - 1 (Block executable content from email client and webmail) d3e037e1-3eb8-44c8-a917-57927947596d - 1 (Block JavaScript or VBScript from launching downloaded executable content) d4f940ab-401b-4efc-aadc-ad5f3c50688a - 1 (Block Office applications from creating child processes)</p>
18.9.45.8	18.9.45.8.3	L1	<p><b>Ensure 'Turn on behavior monitoring' is set to 'Enabled'</b></p> <p>This policy setting allows you to configure behavior monitoring for Windows Defender Antivirus. The recommended state for this setting is: Enabled.</p>
18.9.59.3.2	18.9.59.3.2.1	L2	<p><b>Ensure 'Allow users to connect remotely by using Remote Desktop Services' is set to 'Disabled'</b></p> <p>This policy setting allows you to configure remote access to computers by using Remote Desktop Services. The recommended state for this setting is: Disabled</p>
18.9.59.3.10	18.9.59.3.10.2	L2	<p><b>Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute'</b></p> <p>This policy setting allows you to configure a time limit for disconnected Remote Desktop Services sessions. The recommended state for this setting is: Enabled: 1 minute.</p>
18.9.59.3.11	18.9.59.3.11.1	L1	<p><b>Ensure 'Do not delete temp folders upon exit' is set to 'Disabled'</b></p> <p>This policy setting specifies whether Remote Desktop Services retains a user's per-session temporary folders at logoff. The recommended state for this setting is: Disabled</p>
18.9.61	18.9.61.3	L1	<p><b>Ensure 'Allow Cortana' is set to 'Disabled'</b></p> <p>This policy setting specifies whether Cortana is allowed on the device. The recommended state for this setting is: Disabled</p>
18.9.61	18.9.61.4	L1	<p><b>Ensure 'Allow Cortana above lock screen' is set to 'Disabled'</b></p> <p>This policy setting determines whether or not the user can interact with Cortana using speech while the system is locked. The recommended state for this setting is: Disabled.</p>
18.9.61	18.9.61.5	L1	<p><b>Ensure 'Allow indexing of encrypted files' is set to 'Disabled'</b></p> <p>This policy setting controls whether encrypted items are allowed to be indexed. When this setting is changed, the index is rebuilt completely. Full volume encryption (such as BitLocker Drive Encryption or a non-Microsoft solution) must be used for the location of the index to maintain security for encrypted files. The recommended state for this setting is: Disabled.</p>
18.9.61	18.9.61.6	L1	<p><b>Ensure 'Allow search and Cortana to use location' is set to 'Disabled'</b></p> <p>This policy setting specifies whether search and Cortana can provide location aware search and Cortana results. The recommended state for this setting is: Disabled</p>
18.9.84	18.9.84.2	L1	<p><b>Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Disabled' but not 'Enabled: On'</b></p> <p>This policy setting determines whether Windows Ink items are allowed above the lock screen. The recommended state for this setting is: Enabled: On, but disallow access above lockOR Disabled.</p>

Benchmark Section	Benchmark Recommendation	Benchmark Profile	Benchmark Title/Description
18.9.97.2	18.9.97.2.2	L2	<p><b>Ensure 'Allow remote server management through WinRM' is set to 'Disabled'</b></p> <p>This policy setting allows you to manage whether the Windows Remote Management (WinRM) service automatically listens on the network for requests on the HTTP transport over the default HTTP port. The recommended state for this setting is: Disabled.</p>
18.9.97.2	18.9.97.2.4	L1	<p><b>Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled'</b></p> <p>This policy setting allows you to manage whether the Windows Remote Management (WinRM) service will allow RunAs credentials to be stored for any plug-ins. The recommended state for this setting is: Enabled</p>
18.9.98	18.9.98.1	L2	<p><b>Ensure 'Allow Remote Shell Access' is set to 'Disabled'</b></p> <p>This policy setting allows you to manage configuration of remote access to all supported shells to execute scripts and commands. The recommended state for this setting is: Disabled.</p>
18.9.99.2	18.9.99.2.1	L1	<p><b>Ensure 'Prevent users from modifying settings' is set to 'Enabled'</b></p> <p>This policy setting prevent users from making changes to the Exploit protection settings area in the Windows Security settings. The recommended state for this setting is: Enabled</p>
19.7.4	19.7.4.2	L1	<p><b>Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled'</b></p> <p>This policy setting manages the behavior for notifying registered antivirus programs. If multiple programs are registered, they will all be notified. The recommended state for this setting is: Enabled.</p>
19.7.26	19.7.26.1	L1	<p><b>Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled'</b></p> <p>This policy setting determines whether users can share files within their profile. By default, users are allowed to share files within their profile to other users on their network after an administrator opts in the computer. An administrator can opt in the computer by using the sharing wizard to share a file within their profile. The recommended state for this setting is: Enabled</p>

# Analysis

FIGURE 1. Controls Implementation Group Breakdown

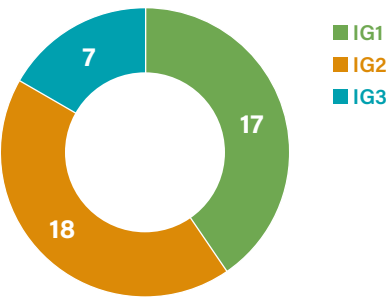
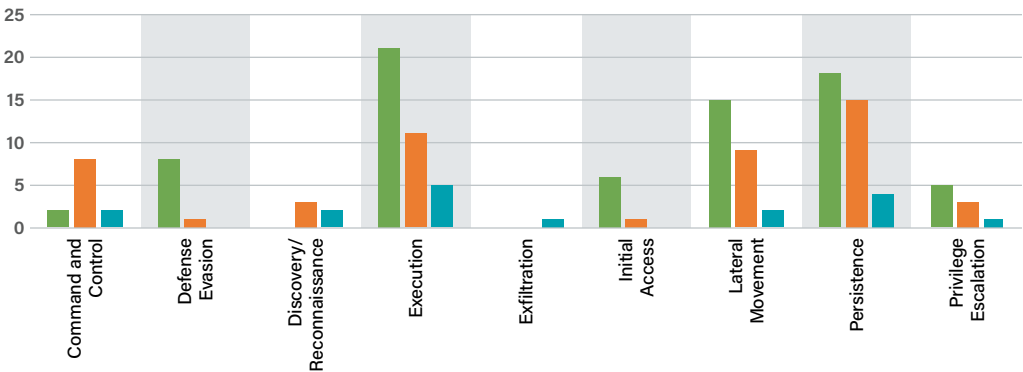


FIGURE 2. Count of Implementation Group Recommendations per Tactic



# Acronyms

<b>AAA</b>	Authentication, Authorization, and Accounting	<b>OS</b>	Operating System
<b>ACL</b>	Access Control List	<b>RD</b>	Remote Desktop
<b>API</b>	Application Programming Interface	<b>RDCS</b>	Remote Desktop Configuration Service
<b>AT</b>	Attention	<b>SACSVR</b>	Special Administration Console Helper
<b>AV</b>	Anti-Virus	<b>SAM</b>	Security Account Manager
<b>CDM</b>	Community Defense Model	<b>SID</b>	Security Identifier
<b>CIFS</b>	Common Internet File System	<b>SMB</b>	Server Message Block
<b>CIM</b>	Common Information Model	<b>STDREGPROV</b>	Standard Registry Provider
<b>CIS</b>	Center for Internet Security	<b>TERMSERVICE</b>	Remote Desktop Services
<b>COTS</b>	Commercial-off-the-Shelf	<b>UAC</b>	User Account Controls
<b>CTA</b>	Cyber Threat Actor	<b>UEFI</b>	Unified Extensible Firmware Interface
<b>FTP</b>	File Transfer Protocol	<b>UPnP</b>	Universal Plug and Play
<b>HTTP</b>	Hypertext Transfer Protocol	<b>UPnPHOST</b>	UPNP Device Host
<b>IG</b>	Implementation Group	<b>URL</b>	Uniform Resource Locator
<b>IP</b>	Internet Protocol	<b>VM</b>	Virtual Machine
<b>IT</b>	Information Technology	<b>VPN</b>	Virtual Private Network
<b>LLTDSVC</b>	Link-Layer Topology Discovery Mapper Service	<b>WDI</b>	Windows Diagnostics Infrastructure
<b>MAC</b>	Media Access Control	<b>Win32</b>	Windows 32 Bit
<b>MFA</b>	Multi-Factor Authentication	<b>WinR</b>	Windows Innovation Network for Real Estate
<b>MSFT</b>	Microsoft	<b>WinRM</b>	Windows Remote Management Controls
<b>MSI</b>	Microsoft Installer	<b>WMI</b>	Windows Management Instrumentation
<b>NT</b>	Not Tested	<b>WS-Management</b>	Web Service Management
<b>PC</b>	Personal Computer	<b>XBOX</b>	Microsoft Video Game Console




# References and Resources

- **2020 CrowdStrike Global Threat Report:** <https://www.crowdstrike.com/resources/reports/2020-crowdstrike-global-threat-report/>
- **A Decade of WMI Abuse – An Overview of Techniques in Modern Malware:** <https://www.bitdefender.com/files/News/CaseStudies/study/377/Bitdefender-Whitepaper-WMI-creat4871-en-EN-GenericUse.pdf>
- **CIS Benchmarks:** <https://www.cisecurity.org/cis-benchmarks/>
- **CIS Community Defense Model 2.0:** <https://www.cisecurity.org/white-papers/cis-community-defense-model-2-0/>
- **CIS Controls v7.1 Exploited Protocols: Remote Desktop Protocol (RDP):** <https://www.cisecurity.org/white-papers/exploited-protocols-remote-desktop-protocol-rdp/>
- **CIS Controls v8 Exploited Protocols: Server Message Block (SMB):** <https://www.cisecurity.org/white-papers/cis-controls-v8-exploited-protocols-server-message-block-smb/>
- **CIS Controls:** <https://www.cisecurity.org/controls/>
- **Microsoft WMI Tasks for Scripts and Applications:** <https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-tasks-for-scripts-and-applications>
- **MITRE ATT&CK® Framework v8.2:** <https://attack.mitre.org/versions/v8/matrices/enterprise/>
- **SANS Institute:** <https://www.sans.org/blog/investigating-wmi-attacks/>
- **Windows Management Instrumentation (WMI CORE 1.5 (Windows NT 4.0)):** <https://web.archive.org/web/20050115045451/http://www.microsoft.com/downloads/details.aspx?FamilyID=c174cfb1-ef67-471d-9277-4c2b1014a31e&displaylang=en>

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Critical Security Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. election offices. To learn more, visit [CISecurity.org](https://CISecurity.org) or follow us on Twitter: @CISecurity.

 [cisecurity.org](https://cisecurity.org)

 [info@cisecurity.org](mailto:info@cisecurity.org)

 518-266-3460

 Center for Internet Security

 @CISecurity

 TheCISecurity

 cisecurity