Best Practice

Verbose Logging: Best Practices for Default Content's Effective Utilization

opentext^{**}

Contents

| Introduction |
|--|
| Windows Logging |
| Windows Security Logs |
| PowerShell Logs7 |
| Sysmon Logs9 |
| Linux Logging11 |
| Auditd Logs11 |
| Other Linux Logs |
| Leveraging Windows ArcSight Connectors |
| Use Cases14 |
| Windows Use Case14 |
| PowerShell Use Case15 |
| Sysmon Use Case17 |
| Linux Use Case |
| Conclusion |
| Legal Notice |

Introduction

To a cyber security professional, logs provide information about events happening in an environment. ArcSight Default Content utilizes the information provided by logs to detect attacks to your environment. However, logs do not provide sufficient information for Default Content resources unless you configure certain systems or application settings to make the information more verbose. Verbose logging is the practice of recording as much information as possible about events that occur on your system. When you enable verbose logging, the additional information recorded is essential for optimizing the Default Content resources for ArcSight ESM using the MITRE ATT&CK Framework.

Windows Logging

The Windows event logs are a detailed and chronological record of system, security, and application notifications stored by the Windows operating system. Default Content resources use these logs to identify potential attacks to your system. However, these Windows logs do not provide detailed information to trigger alerts unless you configure them.

Below are the different types of logs that must be enabled for verbose logging to optimize security alerts from Default Content Resources. Each section contains information about the log and how to enable verbose logging.

- <u>Widows Security Logs</u>
- PowerShell Logs
- Sysmon Logs

Windows Security Logs

ArcSight Default Content relies on many Windows Security logs for optimal alerts.

This section covers:

- Widows Event ID: 4688
- Other Windows Security Logs

Windows Event ID: 4688

Windows Event ID: 4688 logs process creation events. There are four principal events that cause process creation:

- System initialization
- Execution of a process creation system call by running a process.
- A user request to create a new process.
- Initiation of a batch job

Windows Event ID: 4688 is not enabled in Windows by default. However, multiple ArcSight Default Content resources require Windows Event ID:4688 to trigger an alert for a potential attack to your system. Also, once 4688 event is enabled, it should be ensured that the process command line is also enabled. If you enable the command line for 4688, more details will be recorded, including the New Process ID, New Process Name, Token Elevation Type, Mandatory Label, and more. Fig 1 shows process event ID before enabling the command line. Fig 2 shows the verbose event after command line is enabled.

| 🛃 Event Properties · | Event 4688, Microsof | ft Windows security auditi | ing. |
|---|--|--|---|
| General Details | | | |
| A new process ha | s been created. | | |
| Creator Subject: Security Account Logon IE Target Subject: Security Account Logon IE | ID: Ad Name: Ad Domain: V D: V ID: NU Name: - Domain: - D: 0x0 | dministrator 49EBD ULL SID | strator |
| Log Name: Source: Event ID: Level: User: OpCode: More Information: | Security Microsoft Windows 4688 Information N/A Info <u>Event Log Online H</u> | security i Logged: Task Category: Keywords: Computer: | 10/14/2023 11:57:01 PM Process Creation Audit Success |

Fig 1

| 😹 Event Properties - Event 4688, Micr | rosoft Windows security auditing. |
|---------------------------------------|--|
| General Details | |
| A | |
| A new process has been created. | |
| Creator Subject: | |
| Security ID: | Administrator |
| Account Name: | Administrator |
| Logon ID: | 0x49FBD |
| Logonibi | |
| Target Subject: | |
| Security ID: | NULL SID |
| Account Name: | |
| Logon ID: | - 0x0 |
| | |
| Process Information: | |
| New Process ID: | 0x20f0 |
| Token Elevation Type: | C:\windows\systemsz\reg.exe |
| Mandatory Label: | Mandatory Label/High Mandatory Level |
| Creator Process ID: | 0x1914 |
| Creator Process Name: | C:\Windows\System32\cmd.exe |
| Process Command Line: | reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1 /f |
| Ļ | |

Fig 2

Enable Windows Event ID:4688 in the Group Policy Editor

1. In Group Policy Editor, follow this path to the Detailed Tracking folder:

Windows Settings>Security Settings> Advanced Audit Policy Configuration>Audit Policies>Detailed Tracking In this document, a Windows Server 2019 is being used as an example. Please follow the configuration settings as per the windows version you are using in your environment.

| File Action View Help | |
|--|---|
| | |
| | |
| Local Computer Policy Computer Configuration Software Settings Windows Settings Mame Resolution Policy Scripts (Startup/Shutdown) Scripts (Startup/Shutdown) Security Settings Account Policies Coal Policies Windows Defender Firewall with Advance Network List Manager Policies Public Key Policies Software Restriction Control Policies Software Restriction Logon Account Logon Account Management Detailed Tracking Dis Acceus | Audit Events Success and Failure Success and Failure Success and Failure Success and Failure Success and Failure |



- 2. As per Fig 3, in the Detailed Tracking Folder, select Audit Process Creation.
- 3. In the new window, select Success and Failure.
- 4. Click OK.

Then enable the command line:

5. Open the Group Policy Editor on the Windows machine you want to monitor and follow this path to the Audit Process Creation folder:

Administrative Templates>System>Audit Process Creation

- 6. Select Edit policy setting.
- 7. In the new window, select Enabled.

| Juccal Group Policy Editor | | | | | _ | | \times |
|--|-------|-------------------------------|---------|--|------------|----------|----------|
| File Action View Help | | | | | | | |
| 🗢 🔿 🙍 📾 🔒 🛛 🖬 🔻 | | | | | | | |
| Local Computer Policy | ^ | Audit Process Creation | - | | | | |
| Computer Configuration | In | lude command line in process | Sot | ting | Sta | to | |
| Software Settings | cr | eation events | Det | ang | 5 ca | | |
| > iii Windows Settings | | | 88 | include command line in process creation events | Enab | lea | |
| Administrative Templates | Ed | it policy setting | ^ | | | | |
| > 🦲 Control Panel | | Include command line in pro | cess co | eation events | | п | × |
| LAPS | Re | | ccoo cr | | | | ~ |
| > Network | | 🗮 Include command line in pro | cess cr | eation events | | | |
| Printers | | | | | | | |
| Server | De | | | | | | |
| Start Menu and Taskbar | Th | Not Configured Commen | 8 | | | | \sim |
| System | wr | Enabled | | | | | |
| Access-Denied Assistance | pre | O Enabled | | | | | |
| > App-V | 1. | Disabled | | | | | ~ |
| Audit Process Creation | Th | Supporte | d on: | At least Windows Server 2012 R2, Windows 8.1 or Windows RT 8 | .1 | | ^ |
| Credentials Delegation | Au | | | | | | ~ |
| Device Guard | set | | | | | | |
| Device Realth Attestation Service | inf | Options: | | Help: | | | |
| | be | | | | | | |
| Disk Ouotas | se | | | This policy setting determines what informati | on is logo | ged in | ^ |
| Display | 46 | | | security audit events when a new process has | been cre | ated. | |
| > Distributed COM | cre | | | This setting on the set is a start to be set in the set in the set | | | |
| | - Sei | 1 | | Init setting only applies when the Audit Procession | ess creati | on polic | |

Fig 4

8. Select OK.

To save the new settings in Group Policy Object, it's important to run the gpupdate /force command to force a background update of all Group Policy settings, regardless of if they have changed. By default, Windows will update group policy settings every 90 minutes or during a computer reboot. However, this is one of those times when an immediate update is necessary, by using the gpupdate command, you can force a policy update. A system restart may be required for those

Group Policy client-side extensions that do not process policy on a background update cycle but do process policy at a computer start up.

Other Windows Security Logs

To optimize ArcSight Default Content resources, it is necessary to enable Audit Policy events for event IDs such as 4624, 4719, etc. It provides information about basic audit policies that are available in Windows and links to information about each setting.

Enable Audit Policy Events in the Group Policy Editor

- In Group Policy Editor, follow this path to the Detailed Tracking folder: Windows Settings>Security Settings> Local Policy>Audit Policies
- 2. In the Audit Policy folder, select each of these policies shown in Fig. 5 and enable them to alert for successes and failures.



Fig 5

| Local Group Policy Editor | | |
|---|--|--|
| File Action View Help | Audit policy change Properties ? | × |
| Local Computer Policy Computer Configuration Software Settings | Local Security Setting Explain Audit policy change | Security Setting No auditing No auditing |
| ✓ Windows Settings ➤ Name Resolution Policy ☑ Scripts (Startup/Shutdown) ✓ ➡ Security Settings | Audit these attempts: | No auditing No auditing No auditing No auditing |
| Account Policies Gal Policies Gal Audit Policy Gal User Rights Assignment | ⊠ Success ⊠ Failure | Success, Failure Success, Failure Success, Failure |
| A carrier of the security | This setting might not be enforced if other policy is configured to override category level audit policy. For more information, see <u>Audit policy change</u> . (Q921468) | |

Fig 6

- 3. In the new window, select Success and Failure.
- 4. Click OK.

PowerShell Logs

ArcSight Default Content relies on PowerShell logs to trigger alerts to potential threats to your system.

PowerShell supports three types of logging: module, script block, and transcription. PowerShell events are written to the PowerShell operational log: Microsoft-Windows-PowerShell Operational.

- Module logging records pipeline execution details as PowerShell executes, including variable initialization and command invocations. This type of log captures some details missed by other PowerShell logging sources, though it may not reliably capture the commands executed.
- Script block logging records blocks of code as they are executed by the PowerShell engine, thereby capturing the full contents of codes executed by an attacker, including scripts and commands.
- Transcription logging creates a unique record of every PowerShell session, including all input and output, exactly as it appears in the session.

Enable the Above Logging Capabilities

1. In Group Policy Editor, follow this path to the Windows PowerShell settings folder:

Computer Configuration> Administrative Templates> Windows Components> Windows PowerShell

| Local Group Policy Editor | | | |
|---|--|---|--|
| File Action View Help | | | |
| 🕈 🌩 🖄 📷 🗟 🖬 🛛 🏹 | | | |
| Tenant Restrictions Tenant Restrictions Tenant Restrictions Text Input Windows Color System Windows Color System Windows Color System Windows Color System Windows Evorence Improve Windows Eror Reporting Windows Eror Reporting Windows Error Reporting Windows Hello for Business Windows Installer Windows Installer Windows Media Digital Rights Manage Windows Media Player Windows Media Player Windows Messenger Windows Mobility Center Windows Mobility Center Windows PowerShell | Windows PowerShell Select an item to view its description. | Setting Turn on Module Logging Turn on PowerShell Script Block Logging Turn on Script Execution Turn on PowerShell Transcription Set the default source path for Update-Help | State Enabled Enabled Enabled Not configured |
| Windows Reliability Analysis Windows Remote Management (WinRN | | | |

Fig 7

2. Select the settings and enable Module, Script Block and Transcription logging.

Below is an example of enabling module logging.

- 1. In the Options pane, click Module Name as per Fig 8. In the Module Name window, enter * to record all modules.
- 2. Click OK.

Alternatively, setting the following registry values using command line will have the same effect. For example, the below commands can be run to enable PowerShell Module logging.

- reg add HKLM\SOFTWARE\Wow6432Node\Policies\Microsoft\Windows\PowerShell\ModuleLogging /d 1
- reg add HKLM\SOFTWARE\Wow6432Node\Policies\Microsoft\Windows\PowerShell\ModuleLogging /v \ModuleNames /d *

| Turn on Module L | ogging | | | | | × |
|--|--|------------------------------|--|--|---|-------------|
| Turn on Module I | Logging | | Previous Setting | Next Setting | | |
| O Not Configured | Comment: | | | | | ^ |
| Enabled | | | | | | |
| O Disabled | | | | | | \sim |
| | Supported on: | At least Micros | oft Windows 7 or Windows Server | 2008 family | | ^ |
| | | | | | | \sim |
| Options: | | | Help: | | | |
| To turn on logging fo Show, and then type Wildcards are suppor | or one or more moo the module names ted. | dules, click in the list. | This policy setting allows y Windows PowerShell modules. | ou to turn on logging | for | Ŷ |
| Module Names SI | how | | If you enable this policy se | tting, pipeline execution | on events | for |
| To turn on logging fo modules, type the fol list: | or the Windows Poo lowing module na | werShell core mes in the | PowerShell log in Event Viewer. module is equivalent to setting property of the module to True | Iles are recorded in th Enabling this policy so the LogPipelineExecu | e Window etting for a tionDetails | s a s |
| Microsoft.PowerShell | .* | | If you disable this policy se | etting, logging of exec | ution ever | nts |
| Microsoft.WSMan.Ma | anagement | | is disabled for all Windows Pow | erShell modules. Disa | bling this | |
| | | | LogPipelineExecutionDetails pro | quivalent to setting the perty of the module t | ie to False. | |
| | | | | | | |



There are two locations where the PowerShell Logs are recorded in the windows event viewer.

- Application and Services Logs> Windows PowerShell records events such as 800 (Fig 9).
- Application Service Logs> Microsoft>Windows>PowerShell records events such as 4104 (Fig 10).

| 🛃 Event Viewer | | | | | |
|-----------------------------|---|-------------|----------------|------------------|----------|
| File Action View Help | | | | | |
| | | | | | |
| | | | | | |
| > 🎽 MsLbfoProvider | ^ | PowerShell | | | |
| > 🧮 MSPaint | | Namo | Tuno | Number of Events | Sizo |
| > 🛄 MUI | | Name | type | Number of Events | 5120 |
| > Ncasvc | | Admin | Administrative | 0 | 68 KB |
| | | Operational | Operational | 7,477 | 15.00 MB |
| > NDIS | | | | | |
| > NdisImPlatform | | | | | |
| > NetworkProfile | | | | | |
| > NetworkProvider | | | | | |
| > NiaSvc | | | | | |
| > NTIS | | | | | |
| | | | | | |
| > Const | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| Partition | | | | | |
| > PerceptionRuntime | | | | | |
| PerceptionSensorDataService | | | | | |
| PersistentMemory-Nvdimm | | | | | |
| PersistentMemory-PmemDisk | | | | | |
| PersistentMemory-ScmBus | | | | | |
| Policy-based QoS | | | | | |
| V PowerShell | | | | | |
| Admin 💽 | | | | | |
| Operational | | | | | |





Fig 10

Sysmon Logs

ArcSight Default Content relies on Sysmon logs to trigger alerts to potential threats in your environment, such as: Microsoft-Windows-Sysmon 1, 3, 7, 8, 10, 11, 12, 13, 15, 17, 19, 20 and 21.

Sysmon is part of the Sys-internals software package, now owned by Microsoft, and enriches the standard Windows logs by producing some higher-level monitoring of events such as process creations, network connections, and changes to the file system.

The latest release of Sysmon can be downloaded from the Microsoft page (https://learn.microsoft.com/enus/sysinternals/downloads/sysmon) and installed.

| 🔜 i 🗹 📕 🗧 i Sysmon | | | | | | | |
|--|--|--|-------------------|----------------|-----|---------------|-----|
| File Home Shar | e View | | | | | | ~ 🕜 |
| \leftrightarrow \rightarrow \checkmark \uparrow 📜 \rightarrow This | PC > Documents > Sysmon | | | | ٽ ~ | Search Sysmon | م |
| | Name | Date modified | Туре | Size | | | |
| | Eula | 9/28/2018 1:55 AM | Text Document | 8 KB | | | |
| Desktop | Sysmon | 7/14/2020 3:00 PM | Application | 4,182 KB | | | |
| Downloads | Sysmon64 | 7/14/2020 2:56 PM | Application | 2,251 KB | | | |
| Documents > | sysmonconfig-export | 1/16/2020 6:04 PM | XML Document | 111 KB | | | |
| Pictures 🔊 | | | | | | | |
| Music | | | | | | | |
| 🚆 Videos | Administrator: Comman | d Prompt | | | | - | |
| > 🝊 OneDrive | Microsoft Windows [Ver (c) 2020 Microsoft Con | rsion 10.0.19041.264] rporation. All rights reser | ved. | | | | ^ |
| > 🧢 This PC | C:\Users\administrato | r>cd C:\Users\administrator | \Documents\Sysmon | | | | |
| > 🎐 Network | C:\Users\administrato | r\Documents\Sysmon>Sysmon64 | .exe -i sysmoncon | fig-export.xml | | | |



Once the Sysmon is installed, you can verify if Sysmon service is up and running in the services app on your Windows Machine as per Fig 12.

| File Action View | Help | | | | | | |
|-----------------------|------------------------|--|---------|-----------------|----------------|---------------|--|
| | 4 II 8 1 1 | | | | | | |
| Service (Incel) | | | | | | | |
| and sections (second) | Services (Local) | ^ | 11222 | no est i | 150 450 I | | |
| | Sysmon64 | Name | Status | Startup Type | Description | log On As | |
| | | State Repository Service | Running | Manual | Provides req | .ocal System | |
| | Stop the service | Still Image Acquisition Events | | Manual | Launches ap | .ocal System | |
| | Restart the service | Storage Service | Running | Automatic (D | Provides en_ | local System | |
| | | Storage Tiers Management | | Manual | Optimizes t | .ocal System | |
| | Description: | Sync Host_69d1c | Running | Automatic (D | This service _ | .ocal System | |
| | System Monitor service | SysMain | Running | Automatic | Maintains a_ | local System | |
| | | 😳 Sysmon64 | Running | Automatic | System Mon | local System | |
| | | System Event Notification Service | Running | Automatic | Monitors sy_ | local System | |
| | | System Events Broker | Running | Automatic (Tri_ | Coordinates | .ocal System | |
| | | System Guard Runtime Monitor Broker | Running | Automatic (D., | Monitors an | .ocal System | |
| | | Carl Task Scheduler | Running | Automatic | Enables a us | .ocal System | |
| | | CP/IP NetBIOS Helper | Running | Manual (Trig | Provides su_ | local Service | |
| | | Carl Telephony | | Manual | Provides Tel_ | Network Se | |
| | | Chemes | Running | Automatic | Provides use | .ocal System | |
| | | 🚇 Time Broker | Running | Manual (Trig | Coordinates | local Service | |
| | | Touch Keyboard and Handwriting Panel Service | Running | Manual (Trig | Enables Tou | local System | |
| | | Q Udk User Service_69d1c | | Manual | Shell compo | local System | |
| | | Update Orchestrator Service | Running | Automatic (D., | Manages Wi | ocal System | |
| | | UPnP Device Host | | Manual | Allows UPnP | local Service | |
| | | User Data Access_69d1c | | Manual | Provides ap_ | local System | |
| | | C. User Data Storage 69d1c | | Manual | Handles stor | oral System | |

Fig 12

Sysmon allows you to craft the exact logs that you would like to monitor using its configuration file. This capability provides a lot of flexibility and verbosity in the logs recorded. Depending on the user's environment and requirement, one can craft their own Sysmon logs.

All the details on how the configuration file is modified can be understood by running C:\Windows>Sysmon64.exe -? config. The important filter tags that should be included in the configuration file are listed in the table below.

| Event ID | XML Tag | Event Function |
|-----------------------------|----------------------|----------------------------------|
| Microsoft-Windows-Sysmon 1 | ProcessCreate | Process Create |
| Microsoft-Windows-Sysmon 3 | NetworkConnect | Network connection detected |
| Microsoft-Windows-Sysmon 7 | ImageLoad | Image loaded |
| Microsoft-Windows-Sysmon 10 | ProcessAccess | Process accessed |
| Microsoft-Windows-Sysmon 11 | FileCreate | File created |
| Microsoft-Windows-Sysmon 12 | RegistryEvent | Registry object added or deleted |
| Microsoft-Windows-Sysmon 13 | RegistryEvent | Registry value set |
| Microsoft-Windows-Sysmon 15 | FileCreateStreamHash | File stream created |
| Microsoft-Windows-Sysmon 17 | PipeEvent | Pipe Created |
| Microsoft-Windows-Sysmon 18 | PipeEvent | Pipe Connected |
| Microsoft-Windows-Sysmon 19 | WmiEvent | WmiEventFilter activity detected |

| Microsoft-Windows-Sysmon 20 WmiEvent | | WmiEventConsumer activity detected | | | |
|--------------------------------------|----------|---|--|--|--|
| Microsoft-Windows-Sysmon 21 | WmiEvent | WmiEventConsumerToFilter activity detected | | | |

Below is an example of a snippet from Sysmon configuration file that can be added for monitoring certain Sysmon events.

| <pre><!--SYSMON EVENT ID 2 : FILE CREATION TIME RETROACTIVELY CHANGED IN THE FILESYSTEM [FileCreateTime]--></pre> | |
|---|------------------------|
| DATA: UtcTime, ProcessGuid, ProcessId, Image, TargetFilename, CreationUtcTime, PreviousCreationUtcTime<br <rulegroup grouprelation="or" name=""> <filecreatetime onmatch="include"></filecreatetime></rulegroup> | -> |
| <pre></pre> <pre> </pre> | ally les a be wi |
| | |
| <rulegroup grouprelation="or" name=""></rulegroup> | |
| <filecreatetime onmatch="exclude"></filecreatetime> | |
| <pre><image condition="image"/>oneDrive.exe <!--OneDrive constantly changes file times--></pre> | |
| <pre><image condition="image"/><: Windows \systems/ backgroundTaskhost.exe</pre> | |
| <pre><image condition="containe"/>setup (:=1gnore setups=>) </pre> | |
| <pre><image condition="Gontains'/Indata//Indata/ /Indata/</pre></td><td></td></tr><tr><td><pre><Image condition=" end="" with"=""/>redist. rac(/Image < 1-Imore setups> </pre> | |
| <pre></pre> | |
| <pre><image condition="is"/>TrustedInstaller.exe <!--Ignore setups--></pre> | |
| | |
| | |
| SYSMON EVENT ID 3 : NETWORK CONNECTION INITIATED [NetworkConnect] | |
| COMMENT: By default this configuration takes a very conservative approach to network logging, limite</td <td>d to</td> | d to |
| <pre><!--COMMENT: [https://attack.mitre.org/wiki/Command and Control] [https://attack.mitre.org/wiki/Exfil</pre--></pre> | trat |
| TECHNICAL: For the DestinationHostname, Sysmon uses the GetNameInfo API, which will often not have an</td <td>info</td> | info |
| TECHNICAL: For the DestinationPortName, Sysmon uses the GetNameInfo API for the friendly name of ports</td <td>you</td> | you |
| TECHNICAL: These exe do not initiate their connections, and thus includes do not work in this section:</td <td>BIT</td> | BIT |
| <pre><!-- https://www.first.org/resources/papers/conf2017/APT-Log-Analysis-Tracking-Attack-Tools-by-Audit-Policy</pre--></pre> | -and- |
| DATA: UtcTime, ProcessGuid, ProcessId, Image, User, Protocol, Initiated, SourceIsIpv6, SourceIp, Source</td <td>Hosti</td> | Hosti |
| <rulegroup grouprelation="or" name=""></rulegroup> | |
| <networkconnect onmatch="include"></networkconnect> | |
| <pre><!--Suspicious sources for network-connecting binaries--> </pre> | . |
| <pre><image condition="begin with" name="Usermode"/>c:\u00ed users<!--Tools downloaded by users can use of Condition="begin with"-->c:\u00ed users</pre> | ner |
| <pre>Simage name="caucion" condition="begin with">C: keeggie <: - Nothing should operate from the Rec Simage condition="lkeegin with">C: keeggie <: - Nothing should operate from the Rec Simage condition="lkeegin with">C: keeggie <: - Nothing should operate from the Rec Simage condition="lkeegin with">C: keeggie <: - Nothing should operate from the Rec Simage condition="lkeegin with">C: keeggie</pre> | Астег |
| <pre>simage condition="begin with">:(rrogramulacy image> (i="Notmaily, network communications should be so (image condition="begin with">:(rrogramulacy image> (i="Notmaily, network communications should be so (image condition="begin with">:(rrogramulacy image> (i="Notmaily, network communications should be so (image condition="begin with">:(rrogramulacy image> (i="Notmaily, network communications should be so (image condition="begin with">:(rrogramulacy image> (i="Notmaily, network communications should be so (image condition="begin with">:(rogramulacy image> (i="Notmaily, network communications should be so (image condition="begin with");</pre> | TCed |
| <pre><mage control="" sogn="" with="">0. (windows (resp) image> <: Subpletoes and VSC shouldn't be execution chance</mage></pre> | |
| | |



Linux Logging

Typically, you will find Linux server logs in the /var/log directory and sub-directory. This is where syslog daemons are normally configured to write.

Auditd Logs

These logs are a special case of kernel messages designed for auditing actions such as file access. By default, services like auditd, write messages to /var/log/audit/audit.log. Auditd logs by default contain limited information and certain settings must be configured to make it more verbose.

Configure Linux Logs:

- 1. Make sure the refuse manual stop is set to no in the .conf file of the auditd.
- Add the following audit rules in the paths: /etc/audit/audit.rules and /etc/audit/rules.d/audit.rules

| -a exit,always -F arch=b64 -F euid=0 -S execve |
|--|
| -a exit,always -F arch=b32 -F euid=0 -S execve |
| -w /etc/hosts -p r -k hosts_file_access |
| -w /etc/login.defs -p w -k password_policy_modified |
| -w /etc/pam.d/system-auth -p w -k password_policy_modified |
| -w /etc/sudoers -p w -k sudoers_file_modified |

3. Restart the auditd service. The path of the auditd service is in /usr/lib/system/system/auditd.service.

Other Linux Logs

There are also some commands run on Linux machines that cannot be monitored using auditd logs. Depending on the Linux Distribution, the logs are recorded in the appropriate output locations. Please refer to your Linux documentation for the exact output location path.

| anaconda | grubby_prune_debug | rhsm |
|-------------------|---------------------|------------------------|
| audit | httpd | |
| boot.log | lastlog | samba |
| boot.log-20230917 | libvirt | secure |
| boot.log-20230920 | maillog | secure-20230917 |
| boot.log-20230921 | maillog-20230917 | secure-20230924 |
| boot.log-20231006 | maillog-20230924 | secure-20231001 |
| boot.log-20231013 | maillog-20231001 | secure-20231008 |
| btmp | maillog-20231008 | speech-dispatcher |
| btmp-20231001 | mariadb | spooler |
| chrony | messages | spooler-20230917 |
| cron | messages-20230917 | spooler-20230924 |
| cron-20230917 | messages-20230924 | spooler-20231001 |
| cron-20230924 | messages-20231001 | spooler-20231008 |
| cron-20231001 | messages-20231008 | sssd |
| cron-20231008 | ntpstats | swtpm |
| cups | openlmi-install.log | tallylog |
| dmesg | pcp | tuned |
| dmesg.old | pluto | vmware-vgauthsvc.log.0 |
| gdm | qqq | vmware-vmsvc.log |
| glusterfs | qemu-ga | wtmp |

Fig 14

To increase the logging verbosity, install open-source tools like <u>Snoopy Command Logger</u> (not affiliated with Open Text). The snoopy logs can be monitored using a Syslog NG Deamon connector and by providing the appropriate path in the configuration. More details can be found in the <u>ArcSight SmartConnector documentation</u>.

Leveraging Windows ArcSight Connector

There are the following types of default Windows Event Logs:

- Application log, which tracks events that occur in a registered application.
- Security log, which tracks security changes and possible breaches in security.
- System log, which tracks system events.

Once you install the connector in your environment (refer to <u>ArcSight SmartConnectors documentation</u>), there are a few configuration changes that must be made, to monitor different types of logs under Windows connector.

1. Navigate to the connector path and then to the current\user\agent folder.

| > Tł | his PC > Local Disk (C:) > Connector > Windo | wsConnector > current > | > user > agent | |
|---------|---|---|--|-----------------------|
| | Name | Date modified | Туре | Size |
| * * * * | A acp agentdata aup avroschema certs checkpoint contrib fcp fips flexagent keys | Bate modified 8/4/2023 2:22 AM 10/14/2023 11:52 8/4/2023 2:26 AM 8/4/2023 2:22 AM 8/4/2023 2:22 AM 8/4/2023 2:22 AM 8/4/2023 2:22 AM 8/4/2023 2:22 AM 8/4/2023 2:22 AM | File folder File folder File folder File folder File folder File folder File folder File folder File folder File folder | Size |
| | IID map networkzones nfr nt winc 3Ow1evokBABCX8VB8GBwzzA== agent.properties connector_release_version | 8/4/2023 2:22 AM 8/4/2023 2:22 AM 8/4/2023 2:26 AM 8/4/2023 2:22 AM 8/4/2023 2:22 AM 8/4/2023 2:23 AM 8/4/2023 2:26 AM 10/10/2023 2:28 PM | File folder File folder File folder File folder File folder XML Document PROPERTIES File Text Document | 41 КВ 5 КВ 1 КВ |
| | desc | 8/4/2023 2:22 AM | Text Document | 1 KB |

Fig 15

2. Right-click on the agent.properties file and open with Notepad++ under administrator mode.

| | | 0.0000000000000000000000000000000000000 | 511 A 11 |
|------------------|---|---|-------------------|
| 📕 certs | | 8/4/2023 2:25 AM | File folder |
| checkpoint | | Open with | File folder |
| 📕 contrib | | Edit with Notepad++ | File folder |
| 📕 fcp | Ŕ | Share | File folder |
| 📕 fips | - | Bastera provious versions | File folder |
| 📕 flexagent | | Restore previous versions | File folder |
| 📕 keys | | Send to > | File folder |
| 📕 lib | | Cut | File folder |
| 📕 map | | Сору | File folder |
| networkzones | | Create chartest | File folder |
| 📕 nfr | | Create shortcut | File folder |
| 📕 nt | | Delete | File folder |
| 📕 winc | | Rename | File folder |
| 3Ow1evokBABCX8 | | Properties | XML Document |
| agent.properties | | 10/10/2023 2:28 PM | 1 PROPERTIES File |

Fig 16

3. Add the following line: Microsoft-Windows-Sysmon/Operational, Windows PowerShell, Microsoft-Windows-PowerShell/Operational, "Windows PowerShell" in the

agents[0].windowshoststable[0].eventlogtypes parameter and save it. Once completed, restart the connector.





Use Cases

The following use cases give specific examples of ArcSight Default Content resources that rely on verbose logging.

- Windows Use Case
- PowerShell Use Case
- Sysmon Use Case
- Linux Use Case

Windows Use Case

Scenario: The adversary is trying to modify the Registry and running the below commands.

| _ | | | | | |
|---|-------------------------|---|-----------------------|----|-----|
| I | The operation completed | successfully. | | | |
| Ŀ | _DWORD /d 1 /f | | | | |
| Ģ | C:\WINDOWS\system32≻reg | add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest | /v UseLogonCredential | /t | RE(|

Fig 18

In default content, we have a rule to detect the above activity. Rule Path: /All Rules/ArcSight Foundation/MITRE

ATT&CK/TA0005 Defense Evasion/T1112-Modify Registry/Registry Modified by Reg.exe (Fig 18).



Fig 19

In this rule, the condition uses 4688 Event ID, and to capture the specific event, the fields like Target Process Name and Device Custom String4 are used.

However, the Device Custom String4 field in the ESM will not be populated unless we configure verbose logging by enabling Detailed Tracking and Audit Process Creation events. This event won't have sufficient information and the rule can never trigger despite the registry being modified. Hence, its important to enable the appropriate settings as mentioned in <u>Windows Security Logs</u> section of this document. Fig 20 shows the details of the event recorded in the ESM.





PowerShell Use Case

Scenario: The adversary is obfuscating the content during command execution to impede detection and is running the below commands in PowerShell.

Import-Module ./Invoke-Obfuscation.psd1

Invoke-Obfuscation

In default content, we have a rule to detect this activity. Rule Path: /All Rules/Real-time Rules/Security Threat Monitoring/Host Monitoring/Command Obfuscation Using PowerShell (Fig 21)



This rule condition uses PowerShell event IDs like 800 and 4104. These event IDs are not logged in the event viewer unless enabled. Refer to the section <u>PowerShell Logging</u>. The below screenshot shows the details recorded for PowerShell event ID 4104 in windows event viewer (Fig 22).

| Event Properties - Event 4104, PowerShell (Microsoft-Windows-PowerShell) | | | | | | | | |
|--|-----------------------------|-----------------|--------------------------|--|--|--|--|--|
| General Details | | | | | | | | |
| | | | | | | | | |
| Creating Scriptblo | ck text (1 of 1): | | | | | | | |
| invoke-Obluseute | | | | | | | | |
| ScriptBlock ID: 4ff Path: | 00d58-99bd-4392-a79c-0b15d7 | 755eb2c | | | | | | |
| | | | | | | | | |
| 1 | | | | | | | | |
| Log Name: | Microsoft-Windows-PowerSh | ell/Operational | | | | | | |
| Source: | PowerShell (Microsoft-Windc | Logged: | 10/15/2023 11:54:34 PM | | | | | |
| Event ID: | 4104 | Task Category: | Execute a Remote Command | | | | | |
| Level: | Verbose | Keywords: | None | | | | | |
| User: | ۱ | Computer: | | | | | | |
| OpCode: | On create calls | | | | | | | |
| More Information: | Event Log Online Help | | | | | | | |
| | | | | | | | | |
| Fig 22 | | | | | | | | |

This in turn will populate the fields like Device Event Class ID, File Permission, and File Name in the ESM and trigger the rule (Fig 23).

| Active Channel: | | | Total Events: 1 – Events: 1 – | | | |
|--|--|-------------------------|-------------------------------|-------------|-----------------------|--|
| Start Time: 15 Oct 2023 17:39:55 EDT | | | Very High: 0 | | | |
| End Time: 15 Oct 2023 19:39:55 EDT | | | | High: 1 | 😑 💋 Command Obfusc | ation Using PowerShell |
| Filter (File Path = "/All Rules/Real-time Rules/Secu | rity Threat Monitoring/Host Monitoring/Command C | bfuscation Using Power: | Shell" And Type = "Co | Medium: 0 | Creating Scrip | tblock text |
| Inline Filter: No Filter Verified Pulse: No Puls | | | | Low: 0 | | |
| | | | | Very Low. 0 | | |
| Radar | | | | | | |
| 1 | | | | | | |
| 0 | | | | | | |
| 💋 Manager Receipt Time ↑ 1End Time 🗢 🛛 Nar | me 🗢 🛛 🖸 | evice Event Class ID | File Name | Attack: 🧭 | | |
| 5 Oct 2023 19:37:12 EDT 15 Oct 2023 19:37:00 EDT Cor | mmand Obfuscation Using PowerShell | ule:102 | Script Block Text: Invoke- | DOSfucation | Event Details Anni | stations Payload |
| | | | | | II 18 | |
| | | | | | 12 Name | Value |
| | | | | | Device Severity | Verbose |
| | | | | | Device Receipt Time | 15 Oct 2023 19:37:00 FDT |
| | | | | | Device Event Class ID | Microsoft-Windows-PowerShell:4104 |
| | | | | | Device Host Name | WIN-RGJA9DHK0KS |
| | | | | | Device Address | 15.214.144.158 |
| | | | | | Device Zone | <Resource URI="/All Zones/ArcSight System/Public Addres</td> |
| | | | | | Device Zone ID | MX8HU5fsAABCCV7v-GNArfg== |
| | | | | | Device Zone URI | /All Zones/ArcSight System/Public Address Space Zones/He |
| | | | | | Device Zone External | Hewlett-Packard Company |
| | | | | | Device Zone Resource | Hewlett-Packard Company |
| | | | | | Device Zone Name | Hewlett-Packard Company |
| | | | | | Device Version | Windows Server 2019 |
| | | | | | Device Time Zone | America/Los Angeles |
| | | | | | Device Time Zone Of | -28800000 |
| | | | | | Device Vendor | Microsoft |
| | | | | | Device Product | PowerShell |
| | | | | | Destination | |
| | | | | | Destination User Name | Administrator |
| | | | | | Target | |
| | | | | | Target User Name | Administrator |
| | | | | | File | |
| | | | | | File Name | Script Block Text: Invoke-DOSfucation |
| | | | | | File ID | Script Block Id: 534ed87c-8119-4929-b680-ecf5d6870ef2 |
| | | | | | Old File | |
| | | | | | Old File Hash | UTF-8 |
| | | | | | | |



Sysmon Use Case

Scenario: The adversary is trying to gain access to credentials stored in group policy preferences in Windows and is trying to run the below commands to view the credentials.

findstr /S /I cpassword \\sysvol\policies*.xml

In default content, we have a rule to detect this activity. Rule Path: /All Rules/ArcSight Foundation/MITRE ATT&CK/TA0006 Credential Access/T1552-Unsecured Credentials/T1552.006-Group Policy Preferences/Credentials in Group Policy Preferences.



Fig 24

The rule contains a filter called 'process create' which in turn uses Sysmon event ID 1 in an either-or condition. Sysmon must be installed to record Sysmon events. Please refer <u>Sysmon Logging</u> for further reading. Fig 25 are the details recorded when the above Sysmon event is recorded in the windows event viewer.

Event Properties - Event 1, Sysmon General Details Process Create: RuleName: technique_id=T1059,technique_name=Command-Line Interface UtcTime: 2023-10-16 20:16:11.898 ProcessGuid: (4655bcad-9ceb-652c-0318-00000008200) ProcessId: 27968 Image: C:Windows\System 32/findstr.exe FileVersion: 10.0.1904.11 (WinBuild.160101.0800) Description: Find String (OGREP) Utility Product: Microsoft® Vindows® Operating System Company: Microsoft Corporation OriginalFileName: FINDSTR.EXE CommandLine: findstr /S cpassword \\<u>OTPRVDC1901\sysvol*.xml</u> CurrentDirectory: C:\WINDDWS\system 32\ User: OPENTEXT\sraviprasad LogonGuid: (4655bcad-1da5-652b-ab9d-1d000000000) LogonGuid: {4655bcad-1da5-652b-ab9d-1d000000000} LogonId: 0x1D9DAB TerminalSessionId lerminalsessionid: 1 InteqrityLevel: High Hashes: SHA1=FDC776E1297D6E6FB31F8EB0E85771D886A18DC2,MD5=804A6AE28E88689E0CF1946A6CB3FEE5,SHA256 = B298E6DA54121F5D930C545ECECCE26F30A7F209CE0D9AAEA8E00C27DDA27A2,IMPHASH=A27641A39DA5A6B0717E06BA00E56B7F ParentProcessGuid: (4655bcad-98b8-652c-a317-00000008200) ParentProcessId: 14316 ParentImage: C:\Windows\System32\cmd.exe ParentTage: C:\Windows\System32\cmd.exe Log Name: Microsoft-Windows-Sysmon/Operational Source: Logged: 10/15/2023 10:16:11 PM Sysmon Event ID: 1 Information Task Category: Process Create (rule: ProcessCreate) Level: Keywords: User: SYSTEM Computer: USravipras01.opentext.net OpCode: Info More Information: Event Log Online Help

Linux Use Case

Scenario: The adversary is trying to discover information about remote systems using Linux commands.

In default content, we have rule to detect this activity. Rule Path: /All Rules/ArcSight Foundation/MITRE ATT&CK/TA0007 Discovery/T1018-Remote System Discovery/Suspicious Remote System Discovery Commands Entered on Linux (Fig 26).



Fig 26

Most of the Linux-based rules in Default Content depend on auditd logs. However, the target process name field is empty unless verbose logging is enabled in the Linux Machine. Refer to <u>Linux Logging</u> for more information. When the audit rules are enabled, the appropriate fields get populated, which in turn triggers the rule.

| Viewer | | | ۲ ? ۲ | Inspect/Edit | |
|---|---|---------------------|----------------------|-----------------------|---|
| Untitled Active Channel 2 | | | | Event Inspector | |
| Active Channel: | | | Total Events: 2 – | | |
| Start Time: 15 Oct 2023 21:20:31 EDT 🧭 | | | Very High: 0 | Events | |
| End Time: 15 Oct 2023 23:20:31 EDT Filter (File Path = "/All Rules/Real-time Rules | /Security Threat Monitoring /Host Monitoring /Suspicious Remote Syste | em Discovery Com | High: 0 Medium: 0 | Suspicious Remot | e System Discovery Commands i veleuccese |
| Inline Filter: No Filter | | | Low: 2 | | ine poccess |
| Verified Rules: No Rule | | | Very Low: 0 | | |
| Radar | | | | | |
| 2.0 - | | | | | |
| | | | | | |
| 0.0 | | | | | |
| | | | | 4 | |
| 💋 Manager Receipt Time ↑ 1End Time 🗢 | Name 🗢 | Target Process Name | Device Product 💠 📝 | | |
| 🔰 15 Oct 2023 23:20:27 EDT 15 Oct 2023 23:20:25 EDT | Suspicious Remote System Discovery Commands Entered On Linux | /usr/bin/host | auditd 🔺 | Event Details Ann | otations Payload |
| 15 Oct 2023 23:20:27 EDT 15 Oct 2023 23:20:13 EDT | Suspicious Remote System Discovery Commands Entered On Linux | /usr/sbin/arp | auditd | | |
| | | | | | |
| | | | | Name | Value |
| | | | | Device | |
| | | | | Device Event Category | SYSCALL lexecve lsuccess |
| | | | | Device Receipt Time | 15 Oct 2023 23:20:25 EDT |
| | | | | Device Event Class ID | SYSCALL execve success |
| | | | | Device Time Zone | America/Los_Angeles |
| | | | | Device Time Zone Of | -28800000 |
| | | | | Device Vendor | Unix |
| | | | | Device Product | auditd |
| | | | | Device Process Name | auditd |
| | | | | Source | |
| | | | | Source Process ID | 839 |
| | | | | Source User ID | |
| | | | | Destination | |
| | | | | Destination User ID | 1000 |
| | | | | Destination Process | /usr/bin/host |
| | | | | Destination Service | host |
| | | | | Attacker | |
| | | | | Attacker Process ID | 839 |
| | | | | Attacker User ID | |
| | | | | Target | 1000 |
| | | | | Target User ID | 1000 |
| | | | | Target Process Name | heet |
| | | | | rarget service Name | nost |



Conclusion

It's always a challenge to understand the level of verbosity needed in the logs to ensure the right and sufficient information is recorded. It is also important to strike a balance as to what needs to be enabled and disabled to keep the performance of the system unaffected. Hence, to ease some part of this detailed process, this document helps as an easy guide to set up the logs and make use of MITRE ATT&CK related default content in the most effective manner possible.

Useful Links:

- ESM Default Content ArcSight Marketplace
- <u>ArcSight Connectors Documentation</u>
- <u>MITRE Coverage in Default Content</u>
- <u>Contact Us</u>

Legal Notice

Copyright [2024] Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors ("Open Text") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.