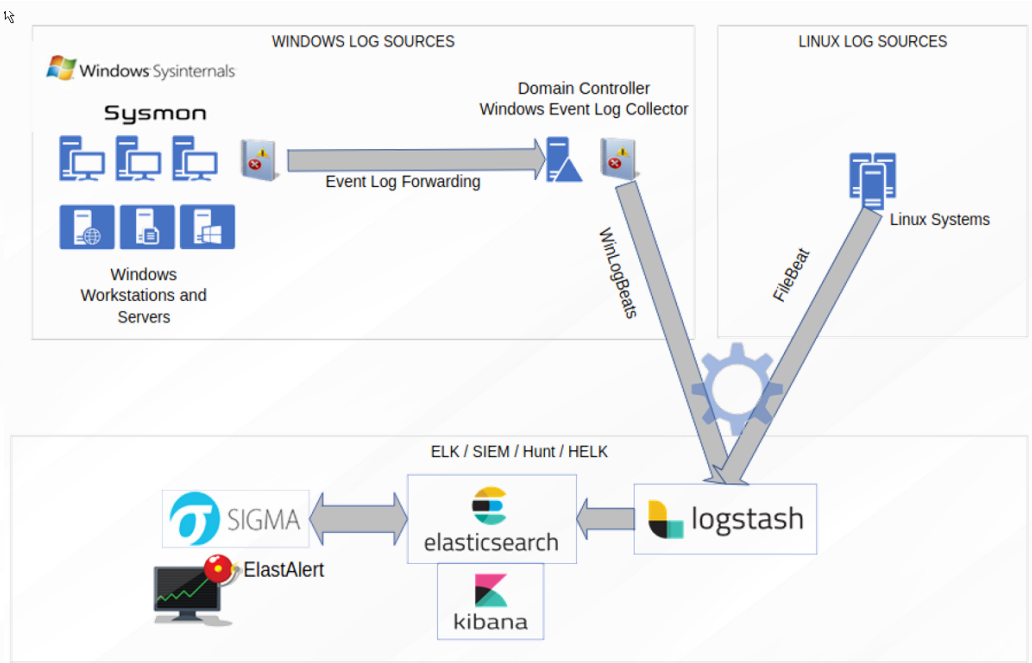
Applied Purple Teaming

Infrastructure, Threat Optics, and Continuous Improvement

June 6, 2020

LC0310

Endpoint Optics
Sysmon
Audit Policy



Sysmon – Assisting with Endpoint Logging

Biased opinion: Sysmon is the best free endpoint logging tool available.
Nuanced opinion: Sysmon can create a lot of noise.
Sysmon-modular: A configurable way to help parse and limit the noise.

- Also, as seen below, can help map events to MITRE techniques

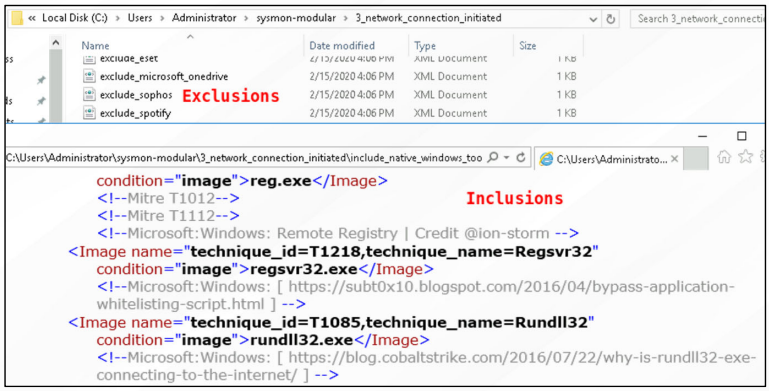
Sysmon v11.0

04/28/2020 • 13 minutes to read •

By Mark Russinovich and Thomas Garnier

Published: April 28, 2020

https://github.com/olafhartong/sysmon-modular
https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

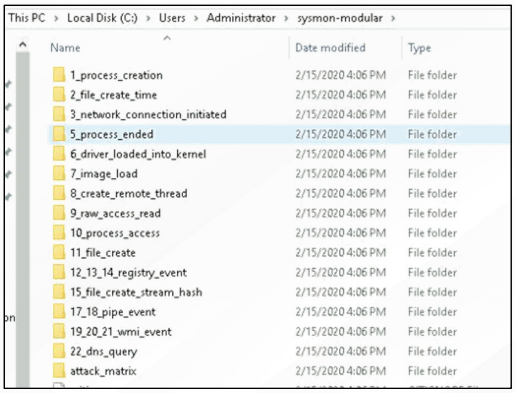


Sysmon – Assisting with Endpoint Logging

Create a configuration file using the sysmon-modular repository.
The containers to the right include configurable options.

The process below generates a custom config file for Sysmon.

- Parses directories as listed for includes/excludes
- It can be adjusted and re-installed easily




```
PS C:\Users\Administrator> cd .\sysmon-modular\
PS C:\Users\Administrator\sysmon-modular> Import-Module .\Merge-SysmonXml.ps1
PS C:\Users\Administrator\sysmon-modular> Merge-AllSysmonXml -Path ( Get-ChildItem '[0-9]*\*.xml') -AsString
  | Out-File sysmonconfig.xml
```

https://github.com/olafhartong/sysmon-modular

Sysmon – Assisting with Endpoint Logging

The install process is easy.

sysmon64.exe -accepteula -i sysmonconfig.xml

```
Z:\lab.defensiveorigins.com\CourseWare\Sysmon>sysmon64.exe -accepteula -i sysmonconfig.xml
System Monitor v10.42 - System activity monitor
Copyright (C) 2014-2019 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.22
Sysmon schema version: 4.23
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
Z:\lab.defensiveorigins.com\CourseWare\Sysmon>
```

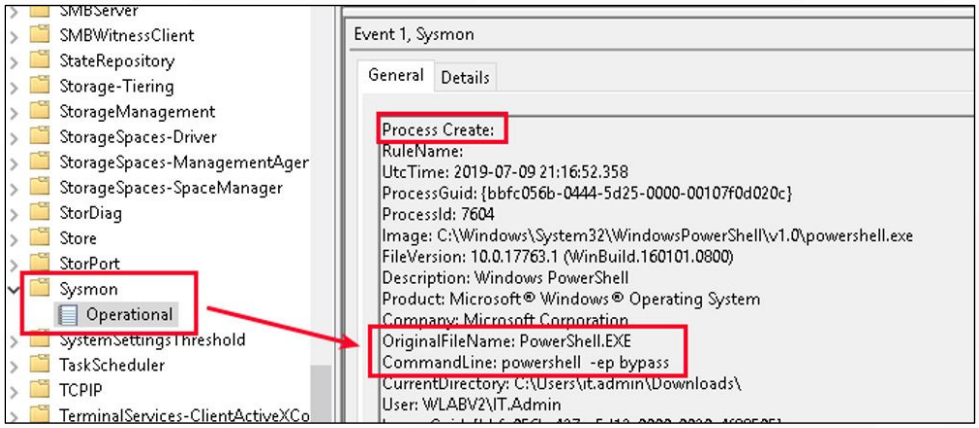
The config update process is easy too.
Update the config directory from the previous slide in accordance with lifecycle changes.
Re-generate the sysmonconfig.xml with the modular tool.

sysmon.exe -c sysmonconfig-update.xml

https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Sysmon – Assisting with Endpoint Logging

Catches things accurately.

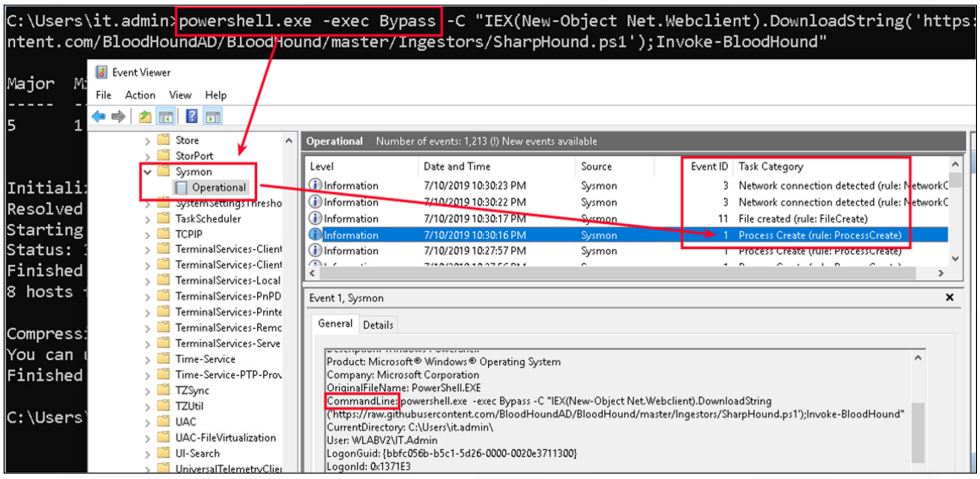


https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Sysmon – Assisting with Endpoint Logging

Catches things accurately.

https://github.com/olafhartong/sysmon-modular



Windows Audits the CLI and PowerShell Natively, Right?

Wrong.

Domain controllers? Nope.

Workstations? Nope.

Anything? Nope.

https://github.com/olafhartong/sysmon-modular

Audit Policy

The command prompt way.

- auditpol.exe /set /Category:* /success:enable
- auditpol.exe /set /Category:* /failure:enable
- auditpol.exe /get /Category:*

```
PS C:\Users\Administrator> auditpol.exe /get /Category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               Success and Failure
  System Integrity                        Success and Failure
  IPsec Driver                            Success and Failure
  Other System Events                     Success and Failure
  Security State Change                   Success and Failure
Logon/Logoff
  Logon                                   Success and Failure
  Logoff                                  Success and Failure
  Account Lockout                         Success and Failure
  IPsec Main Mode                         Success and Failure
  IPsec Quick Mode                        Success and Failure
  IPsec Extended Mode                     Success and Failure
  Special Logon                           Success and Failure
  Other Logon/Logoff Events               Success and Failure
  Network Policy Server                   Success and Failure
  User / Device Claims                    Success and Failure
Object Access
  File System                             Success and Failure
  Registry                                Success and Failure
  Kernel Object                           Success and Failure
  SAM                                     Success and Failure
  Certification Services                  Success and Failure
  Application Generated                   Success and Failure
  Handle Manipulation                     Success and Failure
  File Share                              Success and Failure
  Filtering Platform Packet Drop          Success and Failure
  Filtering Platform Connection           Success and Failure
  Other Object Access Events              Success and Failure
  Detailed File Share                     Success and Failure
  Removable Storage                       Success and Failure
  Central Policy Staging                  Success and Failure
Privilege Use
  Non Sensitive Privilege Use             Success and Failure
  Other Privilege Use Events              Success and Failure
  Sensitive Privilege Use                 Success and Failure
Detailed Tracking
  Process Creation                        Success and Failure
  Process Termination                     Success and Failure
  DPAPI Activity                          Success and Failure
  RPC Events                              Success and Failure
  Plug and Play Events                    Success and Failure
Policy Change
  Authentication Policy Change            Success and Failure
  Authorization Policy Change             Success and Failure
  MPSSVC Rule-Level Policy Change         Success and Failure
  Filtering Platform Policy Change        Success and Failure
  Other Policy Change Events              Success and Failure
  Audit Policy Change                     Success and Failure
Account Management
  User Account Management                 Success and Failure
  Computer Account Management             Success and Failure
  Security Group Management               Success and Failure
  Distribution Group Management           Success and Failure
  Application Group Management            Success and Failure
  Other Account Management Events         Success and Failure
DS Access
  Directory Service Changes               Success and Failure
  Directory Service Replication           Success and Failure
  Detailed Directory Service Replication  Success and Failure
  Directory Service Access                Success and Failure
Account Logon
  Kerberos Service Ticket Operations      Success and Failure
  Other Account Logon Events              Success and Failure
  Kerberos Authentication Service         Success and Failure
  Credential Validation                   Success and Failure
PS C:\Users\Administrator>
```

Configurable via GPO

- More difficult, settings in a few different places
- BUT – granular controls are nice

```
Account Management
  Computer Account Management             No Auditing
  Security Group Management               Success and Failure
  Distribution Group Management           No Auditing
  Application Group Management            No Auditing
  Other Account Management Events         Success and Failure
  User Account Management                 Success and Failure
```

Windows Event Collection - Command Line Logging is ~~Easy~~

Max log file size is small by default.
Command line logging is off by default.

“To see the effects of this update, you will need to enable two policy settings”

- Admin. Templates > System > Audit Process Creation
- Policies > Windows > Security > Advanced Audit > Detailed Tracking

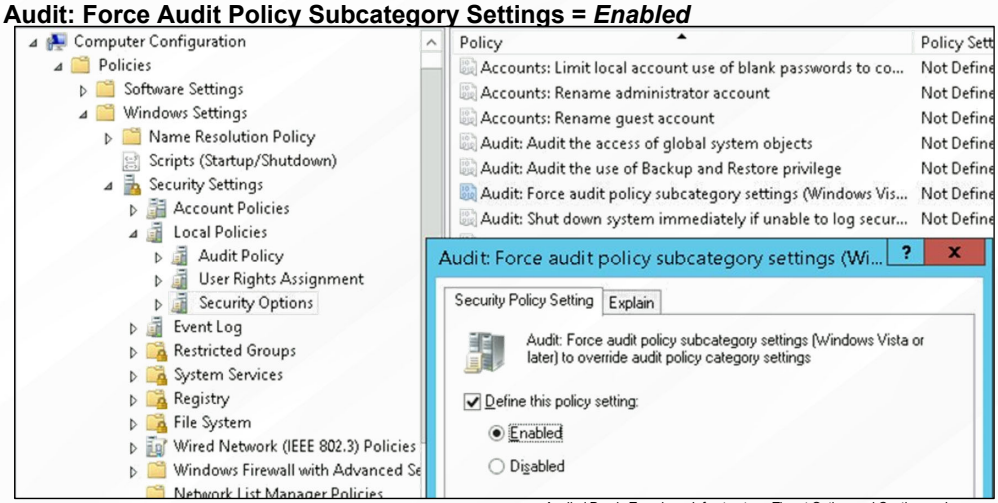
Yeah, and one last thing: The second setting may be overwritten.

> When you use Advanced Audit Policy Configuration settings, you need to confirm that these settings are not overwritten by basic audit policy settings. Event 4719 is logged when the settings are overwritten.

Windows Event Collection - Command Line Logging is ~~Easy~~

To avoid the overwriting of Advanced Audit settings, a *third* setting is required.
Computer Configuration > Policies > Windows Settings > Security > Local > Security

- Setting – **Audit: Force Audit Policy Subcategory Settings = *Enabled***



Windows Event Collection - PowerShell Logging is ~~Easy~~

The PowerShell way to turn on auditing:

- WevtUtil gl "Windows PowerShell" (list configuration)
- WevtUtil sl "Windows PowerShell" /ms:512000000
- WevtUtil sl "Windows PowerShell" /rt:false
- WevtUtil gl "Microsoft-Windows-PowerShell/Operational" (list configuration)
- WevtUtil sl "Microsoft-Windows-PowerShell/Operational" /ms:512000000
- WevtUtil sl "Microsoft-Windows-PowerShell/Operational" /rt:false

```
PS C:\Windows\System32\WindowsPowerShell\v1.0> type .\profile.ps1
$LogCommandHealthEvent = $true
$LogCommandLifecycleEvent = $true
$LogPipelineExecutionDetails = $true
$PSVersionTable.PSVersion
```

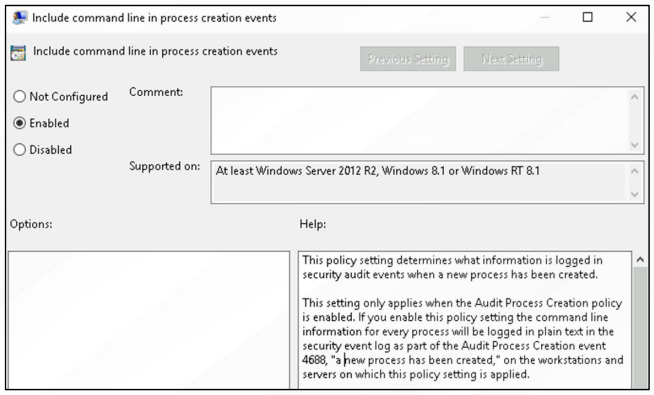
Can also configure the following via command line options.

- Module Logging
- Script Block Logging
- Script Execution Privileges (ie: signed / bypass / enforced)

Windows Event Collection - PowerShell Logging is ~~Easy~~

The Group Policy way to turn on PowerShell auditing:

Policies > Admin Templates > System > Audit Process Creation



Can also configure more granular things under the PowerShell config section.

Admin Templates > Windows Components > Windows PowerShell

- Module Logging
- Script Block Logging
- Script Execution Privileges (ie: signed / bypass / enforced)

Windows Event Collection
What About IIS Logging?

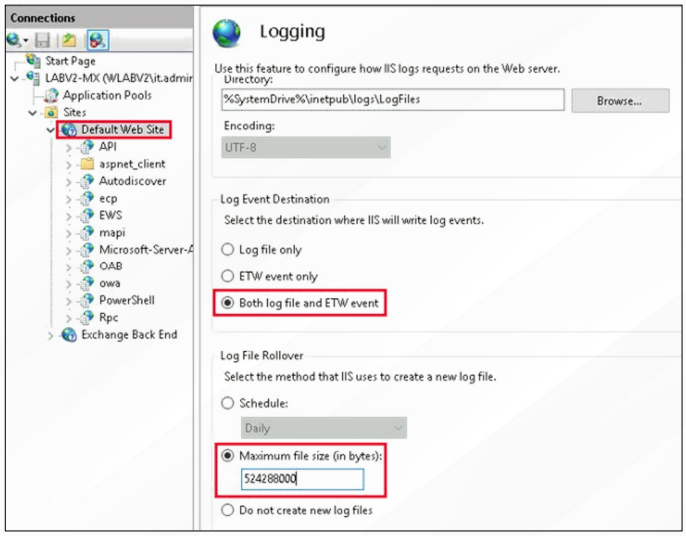
Yeah, that's not on by default either.
LogFiles (text) written by default…
Nothing to event log.

Enable:

- Both log file and ETW event
- Maximum file size

And then you can catch:

- MailSniper
- Burp Suite sprays
- Hydra
- Authentication interactions with Exchange



Windows Event Collection - Making Sense Out of it All.

1. Sysmon can help, a lot. This is not a silver bullet, nothing is.
2. Command line auditing should be configured to capture process creation events.
3. PowerShell module logging and transcription should be configured via Group Policy.
4. IIS doesn't log to Event Viewer without configuration.
5. Logging and auditing can be a challenge, and we're up to the task.