darkoperator / **Posh-Sysmon**

PowerShell module for creating and managing Sysinternals Sysmon config files.

BSD-3-Clause License

157 stars 29 forks

Star Watch

Code Issues Pull requests 1 Actions Projects Wiki Security Insights

master

darkoperator committed on 21 Sep 2018

View code

README.md

Posh-Sysmon

PowerShell 3.0 or above module for creating and managing Sysinternals Sysmon v2.0 config files. System Monitor (Sysmon) is a Windows system service and device driver that is part of the SysInternal tools from Microsoft. It is written by Mark Russinovich and Thomas Garnier to monitor a Windows system actions and log such actions in to the Windows Event Log. When the tool is installed on a system it can be given a XML configuration file so as to control what is logged and the same file can be used to update the configuration of a previously installed instance of the tool.

All functions in the PowerShell module include help information and example of usage that can be view using the Get-Help cmdlet.

Installation

For installation it is highly recomended that you install from the PowerShell Gallery using the Install-Module cmdlet.

On PowerShell v5 and above:

```
Install-Module -Name Posh-Sysmon
```

If you are running PS 3.0 to 4.0 you can use the PowerShell Gallery also following instruction in PowerShell Gallery Documentation

Change Log

Version 1.2

- Module only supports the last 2 Schema versions.**[Breaking Change]**
- Support for Sysmon 8.0 Schema version 4.1 RuleName
- Fixed issue when adding a filter for a none existing rule. It will properly error now.

Version 1.0

- Module only supports the last 2 Schema versions.**[Breaking Change]**
- Support for Sysmon 7.0 Schema version 4.0
- Added new fields for filtering introduced in Sysmon 7.0.
- Modified organization of functions in to their own files for better management while coding.
- Fixed typo in the enabling of rules in rule creation.

Version 0.7.6

- Support for Schema 3.4 of Sysmon v6.2
- New function New-SysmonWmiEvent.
- Updated Rule and Filter functions for WmiEvents.
- Fixed where some functions did not support PipeEvents.

Version 0.7.5

- Support for Schema 3.3 of Sysmon v6.
- New function New-SysmonPipeEvent for filtering for named pipeline cration and connection events.
- Support of PipeEvent in config creation and event type functions.
- Several bug fixes on filtering functions when give an array of values.

Version 0.7.3

- Several bug fixes when creating RawAccess and ProcessOpen rules.
- By default the new schema is 3.2 for the latest version of Sysmon 5.0
- New-SysmonConfiguration function has options to enable all logging for FileCreate, RegistryEvent and FileCreateStreamHash
- Get-SysmonEventData can now parse File Create, Registry and File Stream creation events.
- New function New-SysmonFileCreateFilter for creating file creation filters.
- New function New-SysmonRegistryEvent for creating registry event filters.
- New function New-SysmonFileCreateStreamHash for creating file stream hash event filters.
- Updated Get-SysmonRule, Set-SysmonRule, Remove-SysmonRule and Remove-SysmonRuleFilter for the new event type rules.
- Added Online Help option for all functions.

Version 0.7.2

- Added missing Event Types to Get-SysmonEventData.

Version 0.7.1

- Fixed issue with conditions with filters with space in them.

Version 0.7

- Added support for ProcessAccess filtering added in Sysmon 4.1
- Added function New-SysmonProcessAccess for creating ProcessAccess filters.

- Fixed issue where command was displayed and not ran with New-SysmonDriverLoadFilter.
- Added ProcessAccess type in Get-SysmonEventData and Get-SysmonRuleFilter.
- In verbose output it shows with what version of Sysmon the file will be compatible with after creating it.

Version 0.6

- Added support for Sysmon 4.0 XML schemea (Schema version 3.0)
- One can select the version of schema to support when creating the configuration file.
- All functions have been updated to support the use of more than one rule as per Schema 3.0

Version 0.5

- Added Get-SysmonEventData to get the Event Data information as custom object for selected Event Types.
- Added Get-SysmonRuleFilter to get all filters under a specific Event Type Rule.

Version 0.4

Version 3.0 is a full re-write om how rules work and new event types. This update is SysMon 3.0 only. If you wish to work on SysMon 2.0 rules I recommend you use version 0.3 version of the module.

- When creating a new sysmon rule it will allow you to enable logging of event types supported.
- Checks that it is only working with the proper XML schema for the rules.
- Can now create specific filter for CreateRemoteThread event type.
- Since Rules and Config got merger config functions (Get-SysmonConfigOptio, Set-SysmonConfigOption) where removed and replaced with Get-SysmonHashingAlgorithm and Set-SysmonHashingAlgorithm

Version 0.3

- Tons of fixes do to a bad re-facor.
- Filter creation is now done by specific funtions per event type.
- Filter creation functions are now in their own sub-module.

Version 0.2

- Validate that the file is an XML file and a valid Sysmon configuration file.

- Change option ConfigFile to Path and LiteralPath so as to match other cmdlets that work with files.
- Fixed typos on verbose messages and examples.
- Functions should work better now when passing files through the pipeline using Get-ChildItem.

Version 0.1

- Initial version for Sysmon 2.0 with XML Schema 1.0

Examples

Create a XML Configuration File

```
PS C:\> New-SysmonConfiguration -Path .\pc_marketing.xml -HashingAlgorithm IMPHASH,SH
VERBOSE: Enabling hashing algorithms : IMPHASH,SHA1
VERBOSE: Enabling network connection logging.
VERBOSE: Config file created as C:\pc_marketing.xml
```

Get configured Rules and Filters

```
PS C:\> Get-SysmonRule -Path .\pc_marketing.xml


EventType     : NetworkConnect
Scope         : Filtered
DefaultAction : Exclude
Filters       : {@{EventField=Image; Condition=Image; Value=C:\Windows\System32\svcho
                @{EventField=Image; Condition=Image; Value=C:\Program Files (x86)\Int
                @{EventField=Image; Condition=Image; Value=C:\Program Files\Internet
                @{EventField=Image; Condition=Image; Value=C:\Program Files (x86)\Goo



PS C:\> Get-SysmonRules -Path .\pc_marketing.xml | select -ExpandProperty Filters

EventField   Condition    Value
----------   ---------    -----
Image        Image        C:\Windows\System32\svchost.exe
Image        Image        C:\Program Files (x86)\Internet Explorer\iexplo...
Image        Image        C:\Program Files\Internet Explorer\iexplore.exe
Image        Image        C:\Program Files (x86)\Google\Chrome\Applicatio...
Image        Image        C:\Program Files (x86)\PuTTY\putty.exe
Image        Image        C:\Program Files (x86)\PuTTY\plink.exe
Image        Image        C:\Program Files (x86)\PuTTY\pscp.exe
```

```
Image        Image        C:\Program Files (x86)\PuTTY\psftp.exe
```

Create or Update a Rule and its Default Action

```
PS C:\> Set-SysmonRule -Path .\pc_marketing.xml -EventType ImageLoad -Verbose
VERBOSE: No rule for ImageLoad was found.
VERBOSE: Creating rule for event type with action of Exclude
VERBOSE: Action has been set.

EventType     : ImageLoad
Scope         : All Events
DefaultAction : Exclude
Filters       :
```

Remove One or More Filters

```
PS C:\> Get-SysmonRule -Path .\pc_marketing.xml -EventType NetworkConnect

EventType     : NetworkConnect
Scope         : Filtered
DefaultAction : Exclude
Filters       : {@{EventField=Image; Condition=Image; Value=C:\Windows\System32\svcho
                @{EventField=Image; Condition=Image; Value=C:\Program Files (x86)\Int
                @{EventField=Image; Condition=Image; Value=C:\Program Files\Internet
                @{EventField=Image; Condition=Image; Value=C:\Program Files (x86)\Goo


PS C:\> Remove-SysmonRuleFilter -Path .\pc_marketing.xml -EventType NetworkConnect -C
VERBOSE: Filter for field Image with condition Image and value of C:\Windows\System32
VERBOSE: Filter for field Image with condition Image and value of C:\Program Files (x
VERBOSE: Filter for field Image with condition Image and value of C:\Program Files\In
VERBOSE: Filter for field Image with condition Image and value of C:\Program Files (x
VERBOSE: Filter for field Image with condition Image and value of C:\Program Files (x
VERBOSE: Filter for field Image with condition Image and value of C:\Program Files (x
VERBOSE: Filter for field Image with condition Image and value of C:\Program Files (x
VERBOSE: Filter for field Image with condition Image and value of C:\Program Files (x


EventType     : NetworkConnect
Scope         : All Events
DefaultAction : Exclude
Filters       :
```

Remove Rule

```
PS C:\> Remove-SysmonRule -Path .\pc_marketing.xml -EventType ImageLoad,NetworkConnec
VERBOSE: Removed rule for ImageLoad.
VERBOSE: Removed rule for NetworkConnect.
```

Releases 3

Posh-Sysmon 1.2 Latest
on 21 Sep 2018

+ 2 releases

Contributors 2


darkoperator darkoperator


leechristensen leechristensen

Languages

- **PowerShell** 100.0%