LOGZILLA DOCUMENTATION

Microsoft Sysmon

LogZilla App Store application: Microsoft Sysmon

LogZilla App Store · Generated April 27, 2026 · logzilla.ai/docs/logzilla-appstore/microsoft—sysmon

Overview

Microsoft Sysmon (System Monitor) is a Windows system service and device driver that monitors and logs system activity to the Windows event log. Sysmon provides detailed information about process creations, network connections, file creation time changes, and other system events. Security teams use Sysmon for threat hunting, malware analysis, and incident response.

App Function

- Parse all 30 Sysmon event types from `Microsoft-Windows-Sysmon/Operational`
- Extract process execution details (command line, hashes, parent process)
- Extract network connection metadata (IPs, ports, protocols)
- Categorize events by type (Process, Network, File, Configuration, Service)
- Apply MITRE ATT&CK technique mappings for security analysis
- Apply compliance framework tags (PCI-DSS, HIPAA, SOX, NIST)
- Detect suspicious patterns (encoded commands, suspicious paths)

Vendor Documentation

- Sysmon Documentation (https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon)
- Sysmon Community Guide (https://github.com/trustedsec/SysmonCommunityGuide)

Supported Event IDs

ID	Description	Criticality	MITRE ATT&CK
1	Process Create	Medium	T1059
2	File creation time changed	Medium	T1070.006
3	Network connection	Low	T1071
4	Sysmon service state changed	Low	-
5	Process terminated	Low	-
6	Driver loaded	Medium	T1547.006

ID	Description	Criticality	MITRE ATT&CK
7	Image loaded	Medium	T1574
8	CreateRemoteThread	High	T1055
9	RawAccessRead	Low	T1006
10	ProcessAccess	High	T1003
11	FileCreate	Low	T1105
12	RegistryEvent (Object create/delete)	Medium	T1112
13	RegistryEvent (Value Set)	Medium	T1547.001
14	RegistryEvent (Key/Value Rename)	Medium	T1112
15	FileCreateStreamHash	Medium	T1564.004
16	ServiceConfigurationChange	Low	-
17	PipeEvent (Pipe Created)	Medium	T1559
18	PipeEvent (Pipe Connected)	Medium	T1570
19	WmiEvent (WmiEventFilter)	High	T1546.003
20	WmiEvent (WmiEventConsumer)	High	T1546.003
21	WmiEvent (WmiEventConsumerToFilter)	High	T1546.003
22	DNSEvent (DNS query)	Low	T1071.004
23	FileDelete (archived)	Medium	T1070.004
24	ClipboardChange	Low	T1115
25	ProcessTampering	High	T1055
26	FileDeleteDetected	Medium	T1070.004
27	FileBlockExecutable	Medium	-
28	FileBlockShredding	Low	T1561

ID	Description	Criticality	MITRE ATT&CK
29	FileExecutableDetected	Low	T1204
255	Error	Low	-

Device Configuration

Configure Windows hosts to forward Sysmon events to LogZilla:

Install Sysmon on Windows hosts using an appropriate configuration file
Install and configure LogZilla Windows Agent
Configure the Windows Agent to forward events from the `Microsoft-Windows-Sysmon/Operational` log
Restart the Windows Agent service

Verification

Generate test activity (create a process, make a network connection), then verify events appear in LogZilla with program name `Microsoft-Windows-Sysmon`.

Incoming Log Format

Sysmon events arrive via LogZilla Windows Agent in JSON format with `extra_fields` containing event-specific data.

Event 1: Process Create

```
Process Create:
RuleName: -
UtcTime: 2026-01-08 16:51:06.821
ProcessGuid: {370d727e-e07a-695f-eb5b-000000005b00}
ProcessId: 38044
Image: C:\Program Files\Microsoft OneDrive\FileCoAuth.exe
CommandLine: "C:\Program Files\Microsoft OneDrive\FileCoAuth.exe" -Embedding
User: DOMAIN\username
ParentImage: C:\Windows\System32\svchost.exe
Hashes: SHA256=9660F251B9D748F70A939B12DAE2FD735E854787DB54B9145865FC2D38165F54
```

Event 3: Network Connection

```
Network connection detected:
RuleName: -
UtcTime: 2026-01-08 16:50:42.736
ProcessGuid: {6eb69dd4-ee6b-693d-4c00-000000001e00}
ProcessId: 3668
Image: C:\Windows\System32\dns.exe
User: NT AUTHORITY\SYSTEM
Protocol: udp
SourceIp: 192.168.161.10
SourcePort: 53
DestinationIp: 192.168.150.119
DestinationPort: 53927
```

Event 5: Process Terminate

```
Process terminated:
RuleName: -
UtcTime: 2026-01-08 16:51:05.492
ProcessGuid: {f68d5927-e041-695f-3933-030000003700}
ProcessId: 15572
Image: C:\Windows\System32\RuntimeBroker.exe
User: DOMAIN\username
```

Parsed Metadata Fields

Tag Name	Example	Description
Vendor	Microsoft	Vendor name
Product	Sysmon	Product name
Event Class	Security	Event classification
Event Type	Process	Process, Network, File, Configuration, Service, Data
Compliance Framework	PCI-DSS	PCI-DSS, HIPAA, SOX, NIST
Sysmon EventID	1	Sysmon event ID

Tag Name	Example	Description
Sysmon Description	Process Create	Event description
Criticality	Medium	Event criticality level
MitreId	T1059	MITRE ATT&CK technique ID
MITRE Tactic	Execution	MITRE ATT&CK tactic
Process Name	C:\Windows\System32\cmd.exe	Process executable path
Process Args	cmd.exe /c dir	Command line arguments
Parent Process	C:\Windows\explorer.exe	Parent process path
User	DOMAIN\username	User account
Protocol	tcp	Network protocol
SrcIP	192.168.1.10	Source IP address
DstIP	192.168.1.20	Destination IP address
SrcPort	49152	Source port
DstPort	443	Destination port
Image Hash	SHA256=9660F251...	File hash
Integrity Level	Medium	Process integrity level

Log Examples

Suspicious PowerShell with Encoded Command

```
Process Create:
RuleName: -
UtcTime: 2026-01-08 16:51:06.821
ProcessGuid: {370d727e-e07a-695f-eb5b-000000005b00}
ProcessId: 38044
```

```
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
CommandLine: "powershell.exe" -EncodedCommand SGVsbG8gV29ybGQ=
User: DOMAIN\username
ParentImage: C:\Windows\System32\cmd.exe
Hashes: SHA256=9660F251B9D748F70A939B12DAE2FD735E854787DB54B9145865FC2D38165F54
```

Network Connection to External IP

```
Network connection detected:
RuleName: -
UtcTime: 2026-01-08 16:50:42.736
ProcessGuid: {6eb69dd4-ee6b-693d-4c00-000000001e00}
ProcessId: 3668
Image: C:\Program Files\Google\Chrome\Application\chrome.exe
User: DOMAIN\username
Protocol: tcp
SourceIp: 192.168.1.100
SourcePort: 49152
DestinationIp: 8.8.8.8
DestinationPort: 443
```

Triggers

Trigger	Description
`Sysmon: MITRE ATT&CK Threat Detected`	Any event with MITRE ATT&CK mapping
`Sysmon: Process Injection Detected`	CreateRemoteThread or ProcessTampering
`Sysmon: Credential Dumping Attempt`	ProcessAccess to LSASS
`Sysmon: WMI Persistence Detected`	WMI event subscription activity
`Sysmon: Encoded Command Detected`	PowerShell with encoded command
`Sysmon: Suspicious Pipe Activity`	Named pipe creation or connection