Sysmon For Linux

4 min read · Feb 5, 2024

Shreenkhala Bhattarai Follow

Sysmon for Linux is a powerful system monitoring tool designed to give deep insights into the processes and activities occurring in Linux settings. Sysmon provides an extensive range of logging and monitoring features, giving system administrators the means to ensure system security and integrity. Sysmon makes proactive threat identification and response possible by tracking important system events such as file modifications, network connections, and process creations. Administrators can obtain significant insight into system activity by utilizing Sysmon's real-time monitoring capabilities. This allows for the timely detection and mitigation of any suspicious actions.

Organizations strengthen their defenses against malware infections, unauthorized access, and other security threats by integrating Sysmon into their Linux systems. Sysmon's intricate logging methods make it possible to analyze system events in-depth, which helps with compliance audits and forensic investigations. Furthermore, Sysmon is a perfect fit for both small-scale deployments and big business systems because of its lightweight and efficient architecture, which guarantees little influence on system performance. Linux administrators may more effectively monitor, assess, and defend their systems against changing threats by using Sysmon, which also improves overall system security posture and resilience. It's essential to note the current limitations of Sysmon for Linux, as not all event types are supported at the time of release.

Installation & Configuration

1. Install and configure Sysmon for Linux

Installation instructions for a range of Linux distributions are available on the official Microsoft Sysmon for Linux GitHub.

In this example, I install on Ubuntu 22.04

```
# 1. Register Microsoft key and feed
wget -qO- https://packages.microsoft.com/keys/microsoft.asc | gpg --dearmor
sudo mv microsoft.asc.gpg /etc/apt/trusted.gpg.d/
wget -q https://packages.microsoft.com/config/debian/11/prod.list
sudo mv prod.list /etc/apt/sources.list.d/microsoft-prod.list
sudo chown root:root /etc/apt/trusted.gpg.d/microsoft.asc.gpg
sudo chown root:root /etc/apt/sources.list.d/microsoft-prod.list

# 2. Install SysmonForLinux
sudo apt-get update
sudo apt-get install apt-transport-https
sudo apt-get update
sudo apt-get install sysmonforlinux
```

Once installed you can use Sysmon as you would on a Windows platform, e.g.,

```
$ sysmon -h

Sysmon v1.3.1 - Monitors system events
Sysinternals - www.sysinternals.com
By Mark Russinovich, Thomas Garnier and Kevin Sheldrake
Copyright (C) 2014-2023 Microsoft Corporation
Licensed under MIT/GPLv2
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights
Usage:
Install:                  sysmon -i [<configfile>]
Update configuration:     sysmon -c [<configfile>]
Print schema:             sysmon -s
Uninstall:                sysmon -u [force]
  -c    Update configuration of an installed Sysmon driver or dump the
        current configuration if no other argument is provided. Optionally
        take a configuration file.
  -i    Install service and driver. Optionally take a configuration file.
  -s    Print configuration schema definition of the specified version.
        Specify 'all' to dump all schema versions (default is latest)).
  -u    Uninstall service and driver. Adding force causes uninstall to proceed
        even when some components are not installed.
  -btf Use the specified standalone BTF file.
```

```
The service logs events immediately and the driver installs as a boot-start
On Linux, events are stored in the Syslog, often found at /var/log/syslog.
Use the '-? config' command for configuration file documentation. More examp

Neither install nor uninstall requires a reboot.
```

In a similar fashion to the Windows version of Sysmon, we can use an XML configuration file during (or post) installation to tune as required.

💡 *Example configurations for Sysmon for Linux can be found on MSTIC Sysmon Resources:*

https://github.com/microsoft/MSTIC-Sysmon/blob/main/linux/configs/main.xml

In this example, I am using the default installation configuration.

```
$ sudo sysmon -i

Sysmon v1.3.1 - Monitors system events
Sysinternals - www.sysinternals.com
By Mark Russinovich, Thomas Garnier and Kevin Sheldrake
Copyright (C) 2014-2023 Microsoft Corporation
Licensed under MIT/GPLv2
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Right
Created symlink /etc/systemd/system/multi-user.target.wants/sysmon.service →
```

Sysmon for Linux will write to `/var/log/syslog Ubuntu`, and you can verify that logs are being generated by Sysmon by checking your `syslog` log:

```
sudo grep -i sysmon /var/log/syslog

Feb 04 8:26:35 debian sysmon: <Event><System><Provider Name="Linux-Sysmon" Gu
```

As the Sysmon for Linux logging is written by default to the generic OS log, it will require using Regex Filtering while forwarding logs to any Syslog collector.

Event ID Numbers

As we may have noticed from the previous config snippet, there aren't quite as many event IDs as there are in Windows, however, this is in the Similarities section. The similarities exist on the Event IDs that have been used from Windows keep the same Event IDs, meaning that a file creation is the same event ID across architectures. The table below shows the Event IDs which are used between Sysmon for Windows and Sysmon for Linux.

Sysmon for Windows Event IDs		Sysmon for Linux Event IDs
Event ID 1: Process creation	Event ID 14: RegistryEvent (Key and Value Rename)	Event ID 1: Create Process
Event ID 2: A process changed a file creation time	Event ID 15: FileCreateStreamHash	Event ID 3: Network Connect
Event ID 3: Network connection	Event ID 16: ServiceConfigurationChange	Event ID 4: Service State Change
Event ID 4: Sysmon service state changed	Event ID 17: PipeEvent (Pipe Created)	Event ID 5: Process Terminate
Event ID 5: Process terminated	Event ID 18: PipeEvent (Pipe Connected)	Event ID 9: Raw Access Read
Event ID 6: Driver loaded	Event ID 19: WmiEvent (WmiEventFilter activity detected)	Event ID 11: File Create
Event ID 7: Image loaded	Event ID 20: WmiEvent (WmiEventConsumer activity detected)	Event ID 16: Service Configuration Change
Event ID 8: CreateRemoteThread	Event ID 21: WmiEvent (WmiEventConsumerToFilter activity detected)	Event ID 23: File Delete
Event ID 9: RawAccessRead	Event ID 22: DNSEvent (DNS query)	
Event ID 10: ProcessAccess	Event ID 23: FileDelete (File Delete archived)	
Event ID 11: FileCreate	Event ID 24: ClipboardChange (New content in the clipboard)	
Event ID 12: RegistryEvent (Object create and delete)	Event ID 25: ProcessTampering (Process image change)	
Event ID 13: RegistryEvent (Value Set)		

Cybersecurity Threat Hunting Sysmon Infosec Threat Detection

Follow

Written by Shreenkhala Bhattarai

137 followers · 26 following

SOC Team Lead @ CryptoGen Nepal