Qualys Context XDR (Extended Detection and Response)

Configuration of Microsoft Sysmon

June 20, 2022

Copyright 2022 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

Introduction

System Monitor (Sysmon) is a windows system service and device driver, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time along with many other attributes useful for threat hunting and detection. By collecting the events it generates using Windows Event Collection or SIEM agents and subsequently analyzing them, you can identify malicious or anomalous activity and understand how intruders and malware operate on your network

Overview of Sysmon Capabilities

Sysmon includes the following capabilities:

- Logs process creation with full command line for both current and parent processes.
- Records the hash of process image files using SHA1 (the default), MD5, SHA256 or IMPHASH.
- Multiple hashes can be used at the same time.
- Includes a process GUID in process create events to allow for correlation of events even when Windows reuses process IDs.
- Includes a session GUID in each event to allow correlation of events on same logon session.
- Logs loading of drivers or DLLs with their signatures and hashes.
- Logs opens for raw read access of disks and volumes.
- Optionally logs network connections, including each connection's source process, IP addresses, port numbers, hostnames, and port names.
- Detects changes in file creation time to understand when a file was really created. Modification of file create timestamps is a technique commonly used by malware to cover its tracks.
- Automatically reload configuration if changed in the registry.
- Rule filtering to include or exclude certain events dynamically.
- Generates events from early in the boot process to capture activity made by even sophisticated kernel-mode malware.
- For detailed information, please refer to the official Sysmon documentation at https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Suggested Open Source Sysmon Configuration File

This is a Microsoft Sysinternals Sysmon configuration file template with default high-quality event tracing. The file can function as a starting point for system change monitoring in a self-contained and accessible package. This configuration and results should give you a good idea of what's possible for Sysmon. Kindly note that this does not track all possible Windows events and should be tuned for your organization’s individual use case.

sysmonconfig-export.xml

Please note that this configuration file is not owned or maintained by Qualys, nor is the author affiliated with Qualys. It is recommended by Qualys Threat Research team based on the author’s expertise in threat hunting and incident response. SwiftOnSecurity, Olaf Hartong and Michael (HackerHurrican) are respected contributors to the infosec community and their sysmon configuration files are widely adopted due to their effectiveness and ease of customization.

Because virtually every line is commented and sections are marked with explanations, it can also function as a tutorial for Sysmon and a guide to critical monitoring of Windows systems.

- A more exhaustive, modular and detailed approach to Sysmon configuration can be obtained from: sysmon-modular by @olafhartong, which can act as a superset of sysmon-config.
- Sysmon is a complement to native Windows logging abilities, not a replacement for it. For additional advice on these configurations, see MalwareArchaeology Logging Cheat Sheets by @HackerHurricane.

Note: Exact syntax and filtering choices in the configuration are specific in what they target, and are tuned to minimize performance impact. Sysmon's filtering abilities are different than the built-in Windows auditing features, so often a different approach is taken than the normal static listing of paths.

Additional configuration files based on the original from SwiftOnSecurity

Usage

Install

Run with administrator rights

```
sysmon.exe -accepteula -i sysmonconfig-export.xml
```

Update existing configuration

Run with administrator rights

```
sysmon.exe -c sysmonconfig-export.xml
```

Uninstall

Run with administrator rights

```
sysmon.exe -u
```

Required actions

Prerequisites

We highly recommend Notepad++ to edit this configuration. It has better newline handling and performs XML syntax highlighting, that makes this process easier. We do not recommend using the built-in Notepad.exe.

Customization

It is strongly recommended to install and observe the results of the configuration in a test environment before deploying it widely. In your test environment ensure that proper anti-malware exclusions are in place for sysmon to prevent a negative performance impact and to prevent sysmon from monitoring and collecting anti-malware activities which are not useful for threat hunting and can produce a high volume of unwanted log data.

Your test environment should also include a cross section of representative systems across your standard software stack and include both workstation class systems and servers. Testing should also be performed across the Windows OS versions in place to ensure compatibility with all targeted systems before widespread adoption.

The configuration is commented with helpful hints and designed to be self-explanatory to assist you in this customization to your environment.

Design notes

It is strongly recommended to avoid software installations in the **`C:\Users`** folder which is subject to extra monitoring. Where possible, use the system-wide version of software, like Chrome. See the configuration file for more instructions. This is a scenario that should be reviewed during testing in an isolated environment with updates made to the configuration as needed to ensure minimal impact to your standard software stack.