Install Sysmon on Windows and Integrate with Wazuh

This document explains how Sysmon was installed on a Windows 10 endpoint and used to generate detailed security telemetry for analysis in Wazuh SIEM. Sysmon is widely used by SOC analysts for endpoint monitoring and threat detection.

Step 1: Download Sysmon

Download Sysmon from the official Microsoft Sysinternals website and extract the files into a folder such as C:\Sysmon.

Step 2: Download Sysmon Configuration

Download the SwiftOnSecurity Sysmon configuration file (sysmonconfig-export.xml) from GitHub and place it in the same folder as Sysmon64.exe.

Step 3: Install Sysmon

Open PowerShell as Administrator, navigate to the Sysmon folder, and run Sysmon64.exe -accepteula -i sysmonconfig-export.xml.

Step 4: Verify Sysmon

Verify the Sysmon service is running using Get-Service sysmon64 and confirm events are being generated in Event Viewer under Sysmon Operational logs.

Once installed, Sysmon logs are collected by the Wazuh Agent and analyzed in the Wazuh Dashboard, enabling real-world SOC-style endpoint monitoring.