3. Sysmon Installation & Setup

Sysmon records detailed process creation, network events, and registry changes. This telemetry powers detection logic in Wazuh.

Steps:

1. Download Sysmon from Microsoft Sysinternals.
2. Download Olaf's or SwiftOnSecurity's Sysmon configuration file.
3. Extract Sysmon files.
4. Install Sysmon using Administrator PowerShell:

Command to install (written clean for Docs):
sysmon64.exe -accepteula -i sysmonconfig.xml

5. Verify operation:
    - Open Event Viewer
    - Navigate to Applications and Services Logs > Microsoft > Windows > Sysmon > Operational
    - Events should populate

Sysmon is now installed and generating telemetry.