Microsoft: Sysmon

Microsoft Sysmon, a component of Microsoft’s Sysinternals suite of Windows utilities, is a powerful host-level tool that can assist you in detecting advanced threats on your network by providing intricate host-operation details in real time. In contrast to common Antivirus/Host-Based Intrusion-detection (HIDS) solutions, Sysmon performs system activity deep monitoring and logs high-confidence indicators of advanced attacks.

Sysmon is capable of producing extensive details that are useful in the early detection of malicious code execution or other nefarious behavior. These include:

- Process executions, including parent/child relationships, user that launched process, and hash data
- File creations
- File creation time changes
- Network activity, down to the process level
- Image loads
- Creation of remote threads
- Interprocess accesses
- Windows registry modifications
- NTFS alternate data stream (ADS) creations
- Pipe creations and connections
- WMI event monitoring

Configuration

Guidance for onboarding data can be found in the Splunk Documentation, Getting Data In (Splunk Enterprise) or Getting Data In (Splunk Cloud). Refer to the documentation, and note the following:

- Recommended index: epintel
- Source type: XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
- Input type: WinEventLog://Microsoft-Windows-Sysmon/Operational
- Add-on or app: Splunk Add-on for Microsoft Sysmon
- Sizing estimate: A properly configured Windows endpoint running Sysmon will result in 2-4MB of Sysmon data ingested in Splunk daily—sometimes much less. Particularly busy or compromised machines may generate more data. You may also select “critical” machines or machines owned by “most likely targets” and voluntarily increase the verbosity of logging on these systems. For example, the NetworkConnect (Event Code 3) and Image Load (Event Code 7) logging may be increased for these systems. Universal Forwarder operation can also result in significant process-execution events.

If you have already started ingesting data with a different sourcetype, we recommend that you switch over to the
standardized source types. If you have already started ingesting the data sources into another index, then you can usually proceed, though consider if you should separate sourcetypes into different indexes, based on who likely will need access or be prohibited access.

**Validation**

After proper configuration, run the following Splunk search:

```splunk
index=* source=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
```

You should see data coming into Splunk. Verify correct timestamps, event breaking, and field extraction.

**Application**

When your Splunk deployment is ingesting Sysmon data, you can use the data to achieve the following:

- Monitoring for signs of Windows privilege escalation attacks
- Recognizing improper use of system administration tools
- Monitoring command line interface actions
- Investigating a ransomware attack
- Reconstructing a website defacement
- Monitoring DNS queries
- Checking for files created on a system
- Visualizing processes and their parent/child relationships

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.