Microsoft: Windows event logs

Microsoft Windows event logs are a source of data that reports on state changes in the operating system, applications, and hardware. Data collected from these different elements are written to the Windows event log hosted within the operating system. These events are used by operations and development teams to troubleshoot and mitigate errors. Security and audit events are also written to the same place, but because they serve different use cases, they are covered in the Microsoft: Windows security data source article.

The Windows Event logs contain important events relating to applications, system services and the operating system. The events describe errors, warnings or information details about activity taking place on each system. This information is used to monitor and troubleshoot each system. In the Common Information Model, Windows event logs can be mapped to any of the following data models, depending on the field: Endpoint, Inventory, Updates, Change, Performance.

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: windows
- Source type: WinEventLog and XmlWinEventLog
- Input type: OS logs, forwarded WinEventLogs, and Script
- Add-on or app: Splunk Add-on for Microsoft Windows
- Sizing estimate: The best way to estimate sizing is to send the data to Splunk and use the monitoring console to get ingest sizing by index or sourcetype. Data ingest will vary widely, but an estimated baseline is 250/MB per day per item.

Validation

The first step in validating the logs is to run a search and confirm that the index is getting data in the proper time frame and that the source types and sources are as expected. Further validation is done by inspecting the events and making sure the needed fields are seen. A search similar to the following is a good starting point:

```
index=* earliest=-15m@ sourcetype=winEventLog OR sourcetype=XmlWinEventLog |stats count by sourcetype source index
```
Application

Security

- Maintaining Microsoft Windows systems
- Monitoring Windows account access
- Investigating a ransomware attack
- Deleting web shells automatically
- Terminating W3WP spawned processes
- Complying with General Data Privacy Regulation
- Creating a timebound picture of network activity
- Detecting the use of randomization in cyberattacks
- Identifying new Windows local admin accounts
- Recognizing improper use of system administration tools

Observability

- Managing printers in a Windows environment
- Recovering lost visibility of IT infrastructure