Sysmon for Linux

Introduction

The Sysmon for Linux integration allows you to monitor the Sysmon for Linux, which is an open-source system monitor tool developed to collect security events from Linux environments.

Use the Sysmon for Linux integration to collect logs from linux machine which has sysmon tool running. Then visualize that data in Kibana, create alerts to notify you if something goes wrong, and reference data when troubleshooting an issue.

NOTE: To collect Sysmon events from Windows event log, use Windows sysmon_operational data stream instead.

- Sysmon for Linux - https://github.com/Sysinternals/SysmonForLinux
- Windows sysmon_operational data stream - https://docs.elastic.co/en/integrations/windows#sysmonoperational

Assumptions

The procedures described in Section 3 assumes that a Log Collector has already been setup.

Requirements

Setup

For step-by-step instructions on how to set up an integration, see the Getting started guide.

- https://www.elastic.co/guide/en/welcome-to-elastic/current/getting-started-observability.html

Data streams

The Sysmon for Linux log data stream provides events from logs produced by Sysmon tool running on Linux machine.

Sysmon for Linux Integration

Please provide the following information to CyTech:

Collect Sysmon for Linux logs (Enable Yes/No)

1. Paths - /var/log/sysmon*

Revision #2
Created 23 April 2024 10:01:33
Updated 19 June 2024 06:54:01