Syslog compatibility

Syslog compatibility

Cisco Cyber Vision uses the industry-standard *rsyslog* implementation internally and supports both UDP and TCP. The destination IP and port is to be set in Cisco Cyber Vision's admin page.

Syslog is a loosely defined format, that is there is very little standardization between vendors. The Cisco Cyber Vision Center follows best practices to format the exported data and make it easy to process.

Four syslog formats are available in Cisco Cyber Vision:

- Standard
- Standard/CEF
- RFC3164
- RFC3164/CEF

Standard and RFC3164 formats are available for historical reasons.

CEF (Common Event Format) is an open log management standard that improves interoperability of security-related information from different security and network devices and applications. CEF enables customers to use a common event log format so that data can easily be collected and aggregated for analysis by an enterprise management system.

In RFC3164 and RFC3164/CEF formats, a standard message header containing the date and time (i.e. a timestamp) is applied when a message is generated, as detected from the Windows event log, followed by the hostname and the message content. The value can either be RFC or RFC3164, as both values are equivalent.

RFC3164 provides nanoseconds information, whereas the standard format provides seconds.

For example, a timestamp with/without RFC3164 looks like:

- Timestamp with RFC3164: “2020-11-18T15:45:15.376781+00:00”
- Timestamp without RFC3164: “Nov 18 15:45:15”

Syslog compatibility