Overview

Overview

Cisco Cyber Vision monitors the industrial network using sensors which analyze industrial protocols and forward useful properties to a central appliance, the Center. The Center processes this data to generate a model of the current view of the installation, which can then be compared to previous states and serves as a base for cybersecurity analysis.

During this analysis, events can be generated to warn the administrator of significant happenings: for example, a PLC being reprogrammed is considered to be unusual activity and generates a new event. Events are categorized based on their type and associated data (e.g. a network component or a flow) and are usually presented as a timeline in Cisco Cyber Vision. They can also be exported by the Center using syslog to external servers like log aggregation platforms, SIEMs, and automated event correlation tools.

For example, logs can be emitted when the following events occur:

- Init: new industrial communications being established
- Start CPU: a PLC is being started
- Stop CPU: a PLC is being stopped
- Exception: an exception has been detected in an industrial connection
- Program Download: a PLC program is being downloaded
- Program Upload: a PLC program is being uploaded
- New Communication: a new communication flow is detected
- New Properties: new industrial properties have been detected on the network
- New Component: a new component has been identified on the network
- Protocol Decode Failure: a received packet has generated a decoding error