Check Point

The Check Point Log Exporter is an easy and secured method for exporting Check Point logs in few standard protocols and formats. The Check Point App for Splunk allows you to respond to security risks immediately and gain network true insights. You can collect and analyze millions of logs from all Check Point technologies and platforms across networks, cloud, endpoints, and mobile. This app uses the Check Point Log Exporter to seamlessly send logs from your Check Point log server to your Splunk server. In the Common Information Model, Check Point can be mapped to any of the following data models, depending on the field: Alerts, Change, Intrusion Detection, Malware, and Network Traffic.

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:

- Source type: cp_log or cp_log:syslog
- Input type: Syslog
- Add-on or app: Check Point App for Splunk and Splunk Add-on for Check Point Log Exporter

Application

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

- Complying with General Data Protection Regulation