Carbon Black

Carbon Black is a source for endpoint protection that can be forwarded into Splunk for correlation with other security indicators and for alerting on detections of attacks. The Carbon Black event data is forwarded to Splunk by universal forwarders in JSON format. Carbon Black provides fields and tags in the endpoint security domain focusing on intrusion detection, system changes used for malware detection, and investigation. It also monitors network traffic, does protocol analysis, and tracks and alerts on application behavior. In the Common Information Model, Carbon Black can be mapped to any of the following data models, depending on the field: Alerts, Intrusion Detection, Change, Network Traffic, Endpoint. Any use cases that leverage these data models could work directly or with minor adjustments.

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: bit9:carbonblack:json
- Input type: monitor://<path_of_the_directory_containing_json_file>
- Add-on or app: Splunk Add-on for Carbon Black
- Sizing estimate: The best way to calculate sizing is to measure it in your environment by sending it to Splunk in a lab. A baseline could be 150 MB/day per Carbon black instance and 5 MB/day from each endpoint. This is a rough estimate and can vary widely. It is best to measure with Splunk or to inspect the log sizes directly.

Validation

Validation is done by searching the index and validating timestamp, sourcetype, and field extractions. A search similar to the following is a good starting point:

```
index=* earliest=-15m@ sourcetype=bit9:carbonblack:json
|stats count by sourcetype source index
```

Application

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

- Monitoring for signs of Windows privilege escalation attacks
- Recognizing improper use of system administration tools
- Detecting data exfiltration activities
- Detecting host redirection attacks