CCP Architecture 2.0.1

Architecture

Date of publish: 2017-11-06

https://docs.cloudera.com/

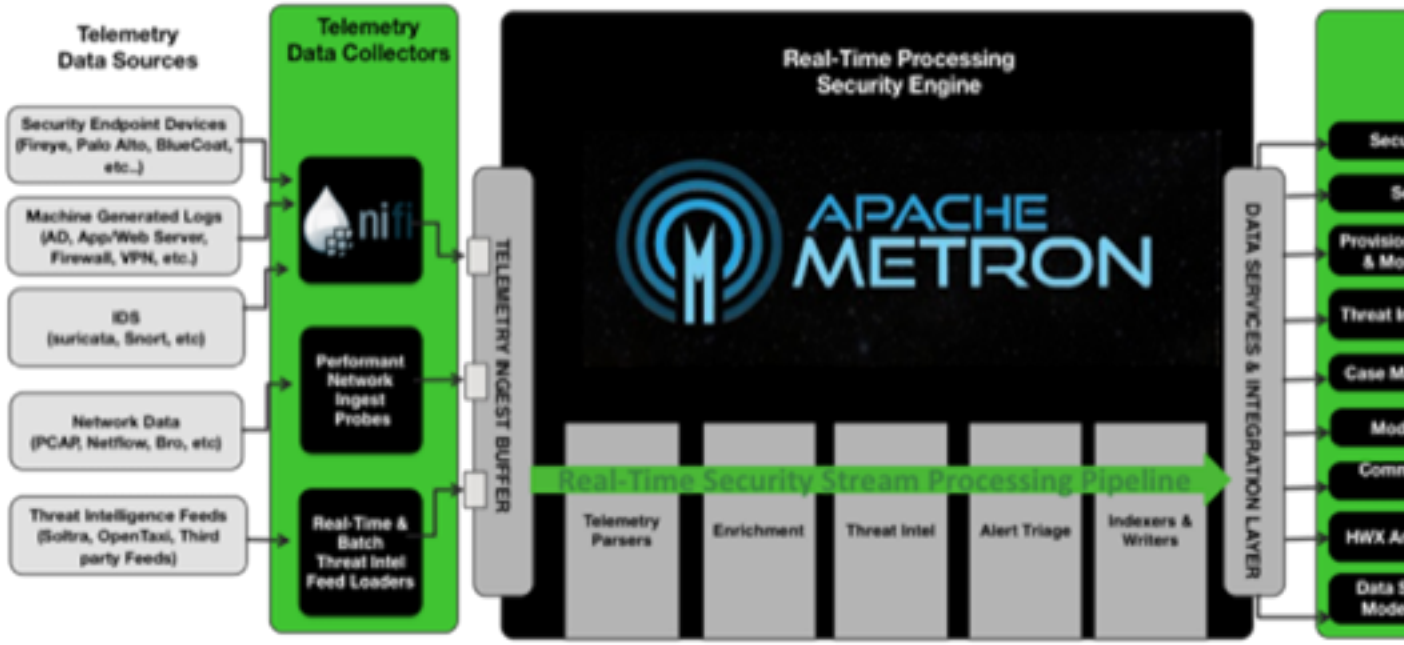
Legal Notice

Contents

Real-Time Processing Security Engine

The core of Cloudera Cybersecurity Platform (CCP) architecture is the Apache Metron real-time processing security engine.

The real-time processing security engine provides the ingest buffer to capture raw events, and, in real time, parses the raw events, enriches the events with relevant contextual information, enriches the events with threat intelligence, and applies available models (such as triaging threats by using the Stellar language). The engine then writes the events to a searchable index, as well as to HDFS, for analytics.



CCP High Level Architecture

Cloudera Cybersecurity Platform (CCP) is primarily backed by Storm and Kafka.

CCP also leverages the following components:

ZooKeeper	ZooKeeper provides dynamic configuration updates to running Storm topologies. This enables CCP to push updates to our Storm topologies without restarting them.
HBase	CCP uses HBase primarily for enrichments. But HBase is also used it to store user state for our UIs.
HDFS	HDFS uses HDFS for long term storage. Parsed and enriched messages land here, along with any reported exceptions or errors encountered along the way.
Solr and Elasticsearch (plus Kibana)	HDP uses Solr and Elasticsearch (plus Kibana) for real-time access. CCP provides out of the box compatibility with both Solr and Elasticsearch, and custom dashboards for data exploration in Kibana.

Zeppelin	Zeppelin provides dashboards to perform custom analytics.
Kafka	Information is pushed into Metron by setting up Kafka topics for parsers to read from. There are a variety of options for setting up Kafka topics, including, but not limited to: • Grok Kafka plugin • Fastcapa • NiFi

Telemetry Data Collectors

Telemetry data collectors push or stream the data source events into Apache Metron. Cloudera Cybersecurity Platform (CCP) works with Apache NiFi to push the majority of data sources into Apache Metron.

For high-volume network data, CCP provides a performant network ingest probe. And for threat intelligence feeds, CCP supports a set of both streaming and batch loaders that enables you to push third-party intelligence feeds into Apache Metron.

Data Services and Integration Layer

The data services and integration layer is a set of three CCP modules that provides different features for different SOC personas.

CCP provides three modules for the integration layer.

Security data vault	Stores the data in HDFS.
Search portal	The Metron dashboard.
Provisioning, management, and monitoring tool	A CCP-provided management module that expedites provisioning and managing sensors. Other provisioning, management, and monitoring functions are supported through Apache Ambari.