Hewlett Packard
Enterprise

HPE Security ArcSight Investigate

Software Version: 1.0

User's Guide

May 24, 2017

Chapter 1: Introduction

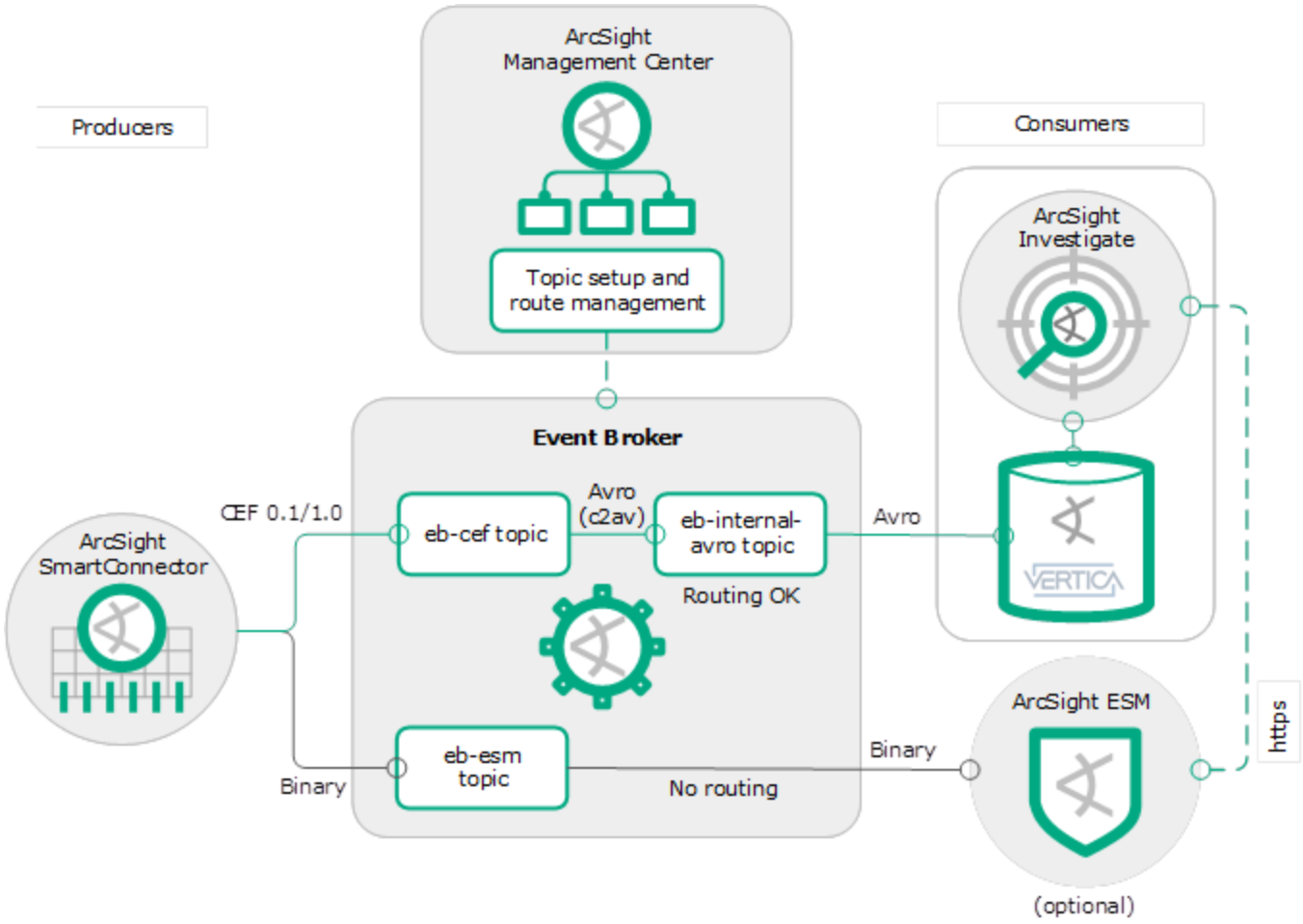
ArcSight Investigate enables you to search, analyze, and visualize machine-generated data gathered from such entities as websites, applications, sensors, and devices that comprise your IT infrastructure or business.

After Investigate ingests the data stream of individual events from Event Broker, you can view and search.

You can use the English-like search language to create searches.

How ArcSight Investigate works

ArcSight Investigate is a high-capacity, threat-investigation solution that enables you to search through and analysis (not just search) vast amounts of event data for anomalies associated with such entities as users, IP addresses, and network assets. Information yielded from a search can help you detect and investigate breaches before substantial damage can be done to your organization. From this, you can also discover contextual information regarding these entities and the effectiveness of security policies and rules, and security applications.



ArcSight Event Broker and ArcSight SmartConnectors are essential parts of the Investigate solution. Connectors send normalized and categorized CEF events to the ArcSight Event Broker topic (`eb-cef`). Events are transformed to Apache Avro format and then consumed by the Vertica Kafka scheduler and then loaded to the HPE Vertica database.

The Vertica scheduler pulls events from a topic and then loads the events into the Vertica database. Investigate reads the events from the Vertica database and then displays them in the Search page.

Investigate can extend the ArcSight Enterprise Security Manager (ESM) application in order to further investigate events in an active channel. ESM generates a URL that opens Investigate, with search criteria based on the data selected in the active channel.

The Search function makes it possible for you to investigate security incidents. It uses a microservices-based architecture, where it is possible to isolate different components (microservices) using docker container technology. This technology enables you to install and configure complex software and package it in an isolated environment—a container, then deploy these containers in any environment making it possible to maintain multiple servers even at a customer-controlled host or the cloud. Even though the microservices are isolated in containers, they still need to interact with each other in order for the application to run as a whole. This interaction is usually done by REST calls between the different microservices.

The Search function is composed of four basic components:

- Search UI

  The Search page is where you start an investigation. It is composed of the Search field, Filter field, Timeline, data visualization charts, and Events table:

- Search backend

  The Search backend saves searches, user preferences, and proxy search requests to Search engine. The REST API is used to implement this.

- Search engine

  Search engine is a scalable server-side application that is responsible for executing and caching large search queries in the Vertica database.

- Vertica database

  The database serves as the main data store, as well as a cache.

Investigate pages

- Dashboard — Where you view data visualization charts and text boxes for note taking.
- Search — Where you perform searches on events and manage this process.
- Admin — Where you set up users and establish user rights.

Roles and functions

- Security analyst

  Functions

  - Search events generated in your network (see "Searching events" on page 27).
  - Send an event to ArcSight Enterprise Security Manager (ESM) to see how it correlates with other events, some of which may be suspicious (see "Searching events in ESM" on page 31).
  - Manage search-results fieldsets (see "Managing search-results fieldsets" on page 35)
  - Visualize search result data (see).
  - Manage the display of search results information to better detect and analyze anomalies (see "Managing search results information" on page 50).
  - Manage dashboard widgets (see "Managing dashboard widgets" on page 25).

  Product access

  Investigate Console (Dashboard page and Search page)

- Security architect

  Functions

  - Can operate as a security analyst.

  Product access

  Investigate Portal (Admin page) and Investigate Console

- Security engineer

  Functions

  - Can operate as a security analyst.

  Product access

  Investigate Portal (Admin page) and Investigate Console

- System admin

  Functions

  - Can operate as a security analyst.
  - Installs and deploys Investigate.
  - Can add and remove analysts and architects.

  Product access

  Search, Dashboard, and Admin pages