Micro Focus Security ArcSight Investigate

Software Version: 2.20

User's Guide

Document Release Date: June 28, 2018
Software Release Date: June 2018

Legal Notices

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

Document Revision History

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.

To check for recent updates or to verify that you are using the most recent edition of a document, go to the : ArcSight Product Documentation Community on Protect 724.

Document Changes

Date	Product Version	Description

Chapter 1: Introduction

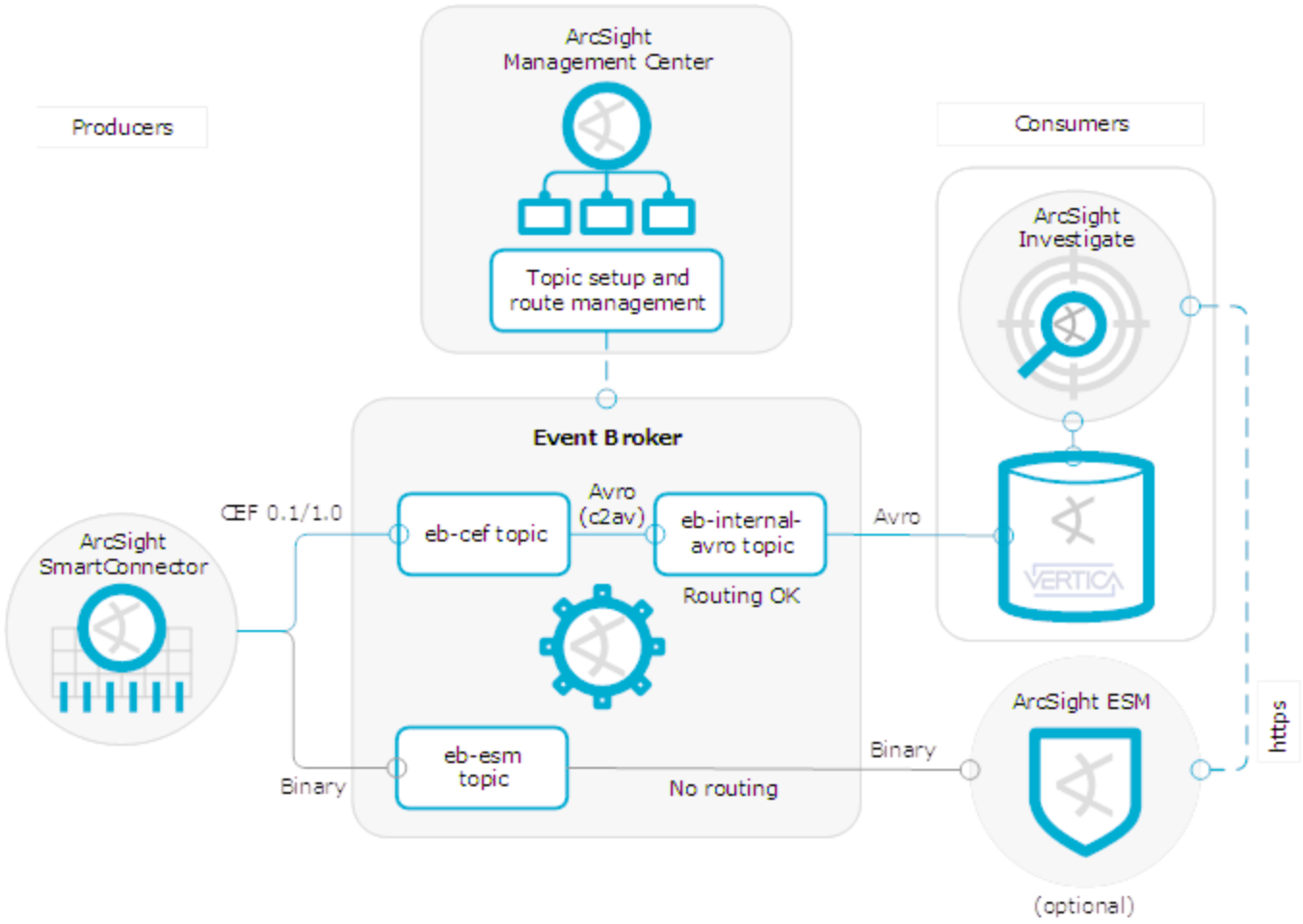
ArcSight Investigate enables you to search, analyze, and visualize machine-generated data gathered from such entities as websites, applications, sensors, and devices that comprise your IT infrastructure or business.

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

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 analyze 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 query input based on the data selected in the active channel.

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: View data visualization charts and text boxes for note-taking.
- Insights: View insights into specified security use cases, such as Host Profiler.
- Search: Perform searches on events and manage the search process.
- Configuration: Create and manage lookup lists.
- Admin : Set up users and establish user rights.

Roles and functions

- Security analyst

  Functions

  - Search events generated in your network (see "Searching events" on page 11).
  - Send an event from an ArcSight Enterprise Security Manager (ESM) channel to Investigate for further investigation (see "Searching events in ESM" on page 45).
  - Manage search-results fieldsets (see "Managing search-results fieldsets" on page 19)
  - Visualize search result data (see "Charting search-results data" on page 23).
  - Manage the display of search results information to better detect and analyze anomalies (see "Managing search results information" on page 37).
  - Manage dashboard widgets (see "Managing dashboard widgets" on page 54).

  Product access

  Investigate Console (Dashboard page and Search page)

- 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

Features and benefits

The following are the main features and benefits of ArcSight Investigate.

- **Search**

  Search is the primary way to navigate data in Investigate. The search is contextual and has auto-suggest capability to help you specify the query input. Therefore, there is no need to learn a complex query language or schema. This can boost the productivity of analysts. Using Vertica, information retrieval is extremely rapid. You can write a search to retrieve events from an index, use statistical commands to calculate metrics and generate charts, search for specific conditions within a rolling time window, identify patterns in your data, predict future trends, and so on. Data visualization charts can be added to a search in order to better understand search-results data. With Investigate supporting up to 100 concurrent queries, there can be 10 active searches and 40 saved searches per user. You can export a search either as a CSV or PDF file.

- **Indexing**

  Investigate indexes machine data. This includes data streaming from packaged and custom applications, application servers, web servers, databases, networks, virtual machines, telecoms equipment, operating systems, sensors, and so on, that make up your IT infrastructure. The maximum indexing volume depends on the Investigate license.

- **Data Analysis**

  Investigate enables you to conduct a security investigation by filtering, comparing, visualizing, and analyzing event data dynamically. You are able to expedite the investigation process with quick and easy data analysis, deriving insights without any complexity. Investigate provides precise investigation outcomes through pre-defined queries (and fieldsets) for security use cases; therefore, improving SOC efficiency and reducing threat posture.

- **Charting**

  You can graphically represent search-results data using the chart editor. This editor enables you to map attributes defined by data-model objects to a chart data visualization without having to write the searches to generate them.

  ArcSight Investigate offers two ways to build visualizations:

  (1) built-in security analytics provides pre-defined visualizations that are configured for specific security use cases, and

  (2) user-defined visualizations where you can define all of the elements of the visualization, including the type, fields, and functions used.

  Charts are saved with the search, and can also be independently added to a dashboard.

- **Dashboard**

  The dashboard can be comprised of search-results charts or text panels, or a combination of these.

  A chart can either have a fixed start and end date, where data cannot be refreshed, or a chart can have a "canned" date range. For example, for a last-30-minutes "canned" date range, data is updated upon refresh based on the most recent 30 minutes.

- **Host Profiler**

  Host Profiler is a predefined dashboard where you can monitor event traffic for a specified host using visualization widgets. The traffic displayed is for the five most active host ports and communication paths related to other systems. This information can enable you to better analyze events. This is available from the Insights section in the left navigation pane.

- **DNS Analytics**

  Pre-set visualizations enable you to monitor *Domain Generating Algorithm* (DGA) activity, often seen in malware.

Workflow summary

As a security analyst, you need to search event data as part of an ad-hoc analysis and investigation of security incidents and threats. Below, is a summary of this workflow and how ArcSight Investigate can help you in this effort.

Typically, the workflow originates from the Search page. However, there could be alternative starting points in the workflow, such as the Dashboard page.

Open Investigate.

1. Launch Investigate from an approved browser using the URL (see "Supported browsers" in the *MicroFocus Security ArcSight Investigate Deployment Guide*):

   `https://<master_node_IP>`
2. From the Login page, specify your credentials.

   From the welcome email that you received, a link was provided for you to create a password.

View event traffic from most active ports and communication paths.

In your investigation, you may want to do host profiling for a specifed host. Host profiling displays event traffic for the five most active host ports and communication paths related to other systems. Event traffic appears in visualization widgets.

Location: Left navigation > Insights > Host Profiler > Host Profiler page

3. Specify the time range in which you will profile a desired host.
4. From the search field, specify the host you want to profile and then click **Profile**.

See "Viewing event traffic" on page 48.

Create a search.

Some commonly used search queries are available as "canned" queries (see "Searching events" on page 11).

Location: Left navigation > Configuration

5. To extend searches with lookup lists, click **Lookup Files** and then upload the desired file(s) (see "Adding a lookup list to extend searches" on page 42).

   - Fields from a lookup file can be used to create a fieldset. This fieldset can be comprised entirely of lookup file fields or added to fields from the schema.
   - You can use a lookup file as search criteria in a search query.
   - ArcSight Investigate stores a lookup file as a table in the Vertica database.

Location: Left navigation > Search

6. Click **New Search** and then accept the default search name or rename it (see "Searching events" on page 11).

   - Investigate automatically assigns a name to a new search in the format of `Search x + 1`.
   - To save your work throughout the search procedure, click **Save** from the task bar.

Specify the query input.

The context of a search is twofold: (1) Investigate an alert or incident and (2) gather and compile data for analysis (see "Searching event data" on page 11).

Location: Left navigation > Search button > Search page

7. From the **Search** field, specify the desired query input (see "Searching events" on page 11).

   - The query can either be full text, natural language, or contextual.
   - An event search consists of specifying query input, search-result fields, and the time period to search within.
   - You can filter search results for more specific information.
   - To use "canned" queries, type # and then select the desired query.

8. To find authenticated users, right-click on an IP or host-name value in the Events table and then choose **Get Authenticated User** (see "Finding authenticated users" on page 41).

Make search-result fields available.

The default fieldset contains the 52 most common event fields. These fields are available for creating data visualization charts and for viewing in the Events table. Each field (column) in this table can provide the 10 most and least common values.

Location: Left navigation > Search button > Search page

9. To create a fieldset, click the fieldset button and then specify the desired fields (see "Creating a fieldset for search results" on page 19).
10. To edit a fieldset, click the fieldset button, select **Edit this set** from the drop-down, and then specify the desired fields (see "Editing a fieldset for search results " on page 20).
11. To delete a fieldset, click the fieldset button, select **Edit this set** from the drop-down, and then click **Delete** (see "Deleting a fieldset for search results " on page 21).

    - If only a single search is using the fieldset, then the fieldset will be deleted and the default fieldset used in its place.
    - If two or more searches are using the fieldset, then the fieldset cannot be deleted.

Specify the search time period.

By default, the time range is for the last 30 minutes (current time minus 30 minutes).

Location: Left navigation > Search button > Search page

12. From the time drop-down, specify the time period to be searched (see "Searching events" on page 11).

    The Quick Ranges feature provides a convenient way to select common search periods ranging from the past minute up to a year ago—or the whole time range where events occurred.

13. Click **Search**.

    To cancel the search, click **X** in the **Search** field.

To narrow your search, do any necessary filtering.

Filtering search results can be accomplished by creating a filter, specifying a time segment in the Timeline, and by adjusting the time range to be searched.

Location: Left navigation > Search button > Search page

14. Click **Filter** and then make the appropriate selections from the **Select** drop-downs (see "Searching events" on page 11).

    To add another filter, click **Add Filter**.
    Other filtering methods:

    - Drag and drop a statement from the Events table to the "Filter" area.

      Upon drop, the "Filter" area hightlights.

    - Right click a data cell in the Events table and then choose **Use As A Filter**.

    For both cases, Investigate adds a new filter (row) to the "Filter" area.

15. From the "Timeline" area, ensure that the range selector is on and then specify the desired time range (see "Viewing search results for a time range" on page 22).

    - This filter applies to the original search results and displays a smaller data set.
    - The new results are reflected in any data visualization and the Events table.

To better understand search-result data, represent it graphically.

You can create up to 10 data visualization charts for a search.

Location: Left navigation > Search button > Search page > Visualize

16. To chart search-result data, expand the "Visualize" area and then select the desired chart type (see "Charting search-results data" on page 23).

    - You can chart using standard or predefined security analytics charts.
    - Use  to delete or rename a chart or to add it to the Dashboard.
    - To edit a chart, click  and then **Edit Chart**.

To view select search results, organize data in the Events table.

Investigate lists search-result events in the Events table. The various fields of the event records are represented by the table column headers. Event-table columns are determined by the fieldset being used and the Show Columns feature.

Location: Left navigation > Search button > Search page > Events area > Events table

17. To find authenticated users, right-click on the desired field value and choose **Get Authenticated User** (see "Finding authenticated users" on page 41).
18. To view the most and least common values for an event field, right-click and specify to view these values from the desired field column header (see "Viewing the most and least common values for an event record field" on page 37).

    The most and least common values for an event record field translates into the count and percentage of hits for the field value.

19. To help compare the column values against those of other columns, make the desired column sticky (see "Pinning field columns to help analyze events" on page 38).
20. To view all the fields of an event, click the arrow at the beginning of the row (see "Viewing all fields of an event" on page 38).

    This feature enables you to quickly view the details of a single event without having to add all the fields of the fieldset.

21. To isolate an event for viewing, click the desired event row and specify view only (see "Viewing

select event data" on page 39).

Use the shift and control keys to select multiple events.

22. To limit the display of field columns, click  and then deselect undesired fields.
23. To reorder field columns, click and drag desired columns to new positions.
24. To sort values for a field column, click the appropriate arrow in the desired column heading.

    A single click in the column heading sorts values in ascending order while a double click sorts values in descending order.

25. To add a field value to the query, right-click on the desired value and select **Search For**.

To view search results outside of Investigate, export the data.

Investigate can export search results to a CSV file, which can be read by such applications as Microsoft Excel and Apple Numbers. The data appears in data-table format. Investigate can also export charts to a PDF file.

26. To export search results, click either 

or **Export to PDF**, depending on your preference (see "Exporting search results" on page 40).
    - Exporting to a CSV file includes only Events table data.
    - Exporting to a PDF includes search results along with any charts.
27. To export Dashboard charts, click **Export to PDF** from the Dashboard page.

Save the search.

The query input and results are saved along with any data visualization charts you created. If you refresh the browser without saving the search, then recently made changes are not saved.

Note: The event count reflected in saved searches does not account for filters.

28. Click **Save** from the task bar.

Editing my profile

About

Your profile includes the following:

- Personal details (name and email).
- Your roles and permissions.

- Fields to which you have access.
- Groups to which you belong.

Procedure

Location: Left navigation > [your name] > My Profile

- Make desired changes and then click **Save**.

Chapter 2: Searching event data

ArcSight Investigate helps you search event data as part of an ad hoc analysis and investigation of security incidents and threat context. The context of a search is twofold:

- Investigate an alert or incident from ArcSight Enterprise Security Manager (ESM) or ArcSight Command Center (ACC). Or, an investigative search can originate from a manual notification regarding a particular entity such as a user, server, or IP address.
- Gather and compile data for analysis and reporting on large-scale (billions of events) data. From a generated time-line chart, and table of events, you can detect anomalies in search responses that point to a security threat.

Searching event data is based on the following general workflow:

Specify a fieldset to determine what search results fields are available for creating data visualization charts and what data columns appear in the Events table.

Extend the search query Specify any lookup lists

Searching events

About

- An event search consists of specifying query input, search-result fields, and the time period to search within.
- A search query can either have a fixed start and end date, where data cannot be refreshed, or a search can have a "canned" date range. For example, for a last-30-minutes "canned" search, data is updated upon re-executing the search based on the most recent 30 minutes.
- You can filter search results for more specific results.
- ArcSight Investigate supports up to 10 session searches and up to 40 saved searches.
- If an event does not have data for a schema field, this absence of data (null) is represented in various ways in the Search page.

Search field	`Null`, `NULL` and `null` query formats are supported
Events table	Empty cell
Charts	*(Null)*
Empty field from ESM (`name=''`)	`name = '', NULL`

- Refreshing the browser as you update a search does not save your changes. Changes are only saved by clicking **Save** from the task bar or by auto save if you navigate away from the search.

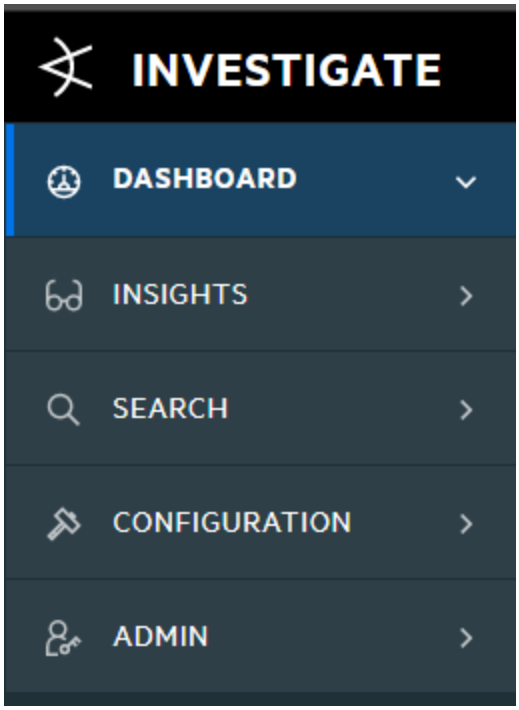
For a search that was created in a different timezone, Timeline will convert the time segments to local times. If there is a time attribute in a chart or the Events table, it will also be converted to local time. The aggregation for all these, however, will reflect that of the original timezone. For example, if Timeline has seven bars in the original timezone, the number of bars could be more or less now to reflect the current timezone.

- For a summary of search commands, see the ArcSight Investigate Query Quick Reference Guide, available from Protect724.

Procedure

Location: Left navigation > Search button > Search page

1. Click **New Search** in the left navigation area.
   - The search appears in a new tab in the left navigation.
   - To use an existing search:
     - Session search — From the left navigation, open the desired search from the list of session searches.



     - Saved search — From the left navigation, click **Saved Results** and open the desired search.

Note: For a search that was created in a different timezone, Timeline will convert the time segments to local times. If there is a time attribute in a lookup list, chart, or the Events table, it will also be converted to local time. The aggregation for all these, however, will reflect that of the original timezone. For example, if Timeline has seven bars in the original timezone, the number of bars could be more or less now to reflect the current timezone.

To modify any of these searches, continue with this procedure.

2. Accept the default search name or rename the search.

   Investigate automatically names a new search in the format of `Search x + 1`.

   Examples

   `Search 1`

   `Search 2`

   `Search 3`

3. To search for fields with data, specify the desired query input from the **Search** field.

   - The query input determines the search type (full text, natural language, or contextual).

     Examples

     - `Source Address = 192.10.11.12 and Destination Address less than 192.10.11.12`

       During search input, Investigate suggests the search items (`Source Address`, `Destination Address`) and operators (=, and, `less than`).

   - A drop-down appears below the field suggesting applicable input.

     In some cases where many options are available, you can click the more button (...) to view additional options.

   - Search items are case insensitive.
   - You can copy and paste in the **Search** field.
   - Investigate auto completes search items based on a schema data dictionary.
   - To use "canned" queries, type # and then select the desired query.

     - There are eight "canned" queries, indicated by the **preset** label.
     - To view the query input for the "canned" query, hover over the "canned" query in the **Search** field.

   - You can enter various combinations of search items and values.

     Investigate treats a comma (,) between search items and values as an `or` operator.

     Examples:

     - `Destination Address = 192.214.133.85, 192.211.201.91`

       Same as: `Destination Address = 192.214.133.85 or 192.211.201.91`
     - `Source Address, Destination Address = 192.214.133.85`

       Same as: `Source Address or Destination Address = 192.214.133.85`

- `IP = 192.214.133.85, 192.211.201.91, 192.215.101.77, 192.218.151.87 and agt = 15.214.130.65 and ahost = n15-214-130-h65.arst.usa.hp.com`

  Same as: `IP = 192.214.133.85 or 192.211.201.91 or 192.215.101.77 or 192.218.151.87 and agt = 15.214.130.65 and ahost = n15-214-130-h65.arst.usa.hp.com`

- From the Events table, you can specify query information to find authenticated users (see "Finding authenticated users" on page 41).
- You can search on IP address ranges and subnets.

  IPv4, IPv6, and MAC addresses are stored in a format that enables you to do the following:

  - Compare IP address with optimum performance
  - Specify a range of IP addresses
  - Use abbreviated input search notation

  Also, IP addresses in the Events table are listed in numerical order.

  See "IP address ranges and subnets as query input" on page 17.
- To remove a search item, use the backspace key.
- To join a lookup table to the 176-field schema table available for queries, use the `in list` operator.

  Example

  ```
  Agent Address in_subnet 15.* and Agent Address not equal 1.1.1.1 and Source Address in list l1_srcAddr
  ```

- See the *ArcSight Investigate Query Quick Reference Guide*.

4. To search for a field without data, use the `null` field value in the **Search** field.
   - The `Null`, `NULL` and `null` query formats are also supported.
   - An empty field is represented as *(NULL)* in the Search page, and an empty cell in the Events table.
   - See the *ArcSight Investigate Query Quick Reference Guide*.
5. Accept the default fieldset for search result events, or change the fieldset by clicking **Default Fieldset**.
   - Depending on your data access permissions, you may not see all the possible fields for an event.

     From the user page (**Left navigation > [user] > My Profile > Data Access > My Profile**), you can view event fields for which you have access.

See

- "Managing search-results fieldsets" on page 19
- "Creating a fieldset for search results" on page 19
- "Editing a fieldset for search results " on page 20
- "Deleting a fieldset for search results " on page 21

6. From the time drop-down accept the default time range (**Last 30 minutes**), or specify a different time range to be searched.

   - The **Quick Range** feature provides a convenient way to select common search periods ranging from the past minute up to a year ago.
   - A **Quick Range** selection appears in the **Custom Range** fields, where you can edit this information.
   - By default, the **Custom Range** fields contain the **Quick Range** time range for the last 30 minutes (current time minus 30 minutes).

7. Click **Search**.

   - If results are found, Timeline and the Events table are populated with data. Also, the **Filter** button and **Create Visualization** button appear.
   - To cancel the search, click **X** in the **Search** field.

     This will not remove the search conditions that you originally specified.
   - To change the search, edit the query input in the **Search** field and then click **Search**.

     The original search stops and the new query begins.
   - After the search executes, you can change the fieldset.

     Click **Search** again to fetch the desired fields. Any existing data visualization charts adjust to the fieldset change, along with the Events table. However, if a certain field from an original visualization is not present in the new fieldset, then the affected visualization is removed from the search after a warning message appears.
   - If millions of events are retrieved, the search could pause. To resume, click the play button (▶) from the progress bar.

     - The search pauses to indicate that the number of search results returned may impact the search performance. You may want to refine the search criteria and/or re-execute the search for a smaller time range.
     - Results are presented consistently for searches that include the same criteria. This means each time the same search criteria is used, the Events table populates the same, the Timeline reflects the search period the same, and any data visualization charts render the same.

- Search results are ordered by date, so a result set with millions of total records will bring back the same million records in subsequent searches. The result set will be ordered by device receipt time, with the newest events returning first.

- The data retention default is 90 days. You can specify a different data retention value, with the minimum being one day and the maximum being 366 days. See the *ArcSight Investigate Deployment Guide* for details.

8. To filter the search results:
   a. Click **Filter** and then **Add Filter**.
   b. Make the appropriate selections from the **Select** drop-downs.
   c. To add another filter, click **Add Filter**.
   d. Click **Apply** or **Apply all**, depending on your filter usage.

      - The updated search results are reflected in "Timeline", any data visualizations, and Events table.
      - Investigate list filters in abbreviated form.

        Examples

        ```
        IP = "208.202.19.230"
        Username = bob
        Rt = 1445077926551
        ```

        To see the whole filter, click the desired abbreviation.

   Other filtering methods:

   - Drag and drop values from Event Table to the "Filter" area.
   - Right click a data cell in the Events table and then choose **Use As A Filter**.

   For both cases, Investigate can add a new filter (row) or modify an existing one in the "Filter" area.
9. To view search results graphically, expand the "Visualization" area and then create the desired chart (see "Charting search-results data" on page 23).
10. To view and manage search result data, use the various options in the “Events” table to organize event data (see "Managing search results information" on page 37).
11. Click **Save** from the task bar.

    - The query input and results are saved along with any data visualization charts you created.
    - If you reach the limit of session searches (10), you will have to delete one in order to create a new search.

12. To export search results, either click 

from the "Events" area or **Export to PDF** from the task

bar, depending on the desired output (see "Exporting search results" on page 40).

13. To do another search, either create a new one or open an existing one.

    - An existing search can be either a session or saved search
    - Investigate supports up to 10 session searches and up to 40 saved searches.

      If total session searches is at the limit of 10, delete a session searches in order to create a new search.
    - You can open or create a new search before the current one finishes.

      Switching to another search does not interrupt the execution of the original search. The current search will run until complete.
    - To complete a new search, repeat steps 1 — 13.

See Also

- "Searching events in ESM" on page 45

IP address ranges and subnets as query input

About

IPv4, IPv6, and MAC addresses are stored in a format that provides more flexibility and better performance when performing a search. These benefits include the following:

- Compare IP address with optimum performance

  Example:

  ```
  Agent Address > 192.10.11.12
  ```

- Specify a range of IP addresses

  Examples:

  - `Agent Address in_between 192.2.13.1 and 192.2.13.11`
  - `Source Address greater_equal_than 192.10.11.12 and Destination Address less_than 192.112.98.33`

- Use abbreviated input search notation

  Examples:

  - `Agent Address in_subnet 192.*`

    For this IPv4 address, this input specifies IP addresses in the subnet starting with 192.
  - `Agent Address in_subnet 192.0.0.0/8`

For this IPv4 address, this input specifies an agent address in a subnet that uses CIDR notation in its address. The first 8 bits are the network part of the address, leaving the last 24 bits for specific host addresses.

- `Agent Address in_subnet 2001:0db8:0000:0000:0000:ff00:0042:8329/24`
  For this IPv6 address, this input specifies an agent address in a subnet that uses CIDR notation in its address. The first 24 bits are the network part of the address, leaving the last 40 bits for specific host addresses.

- IP addresses in the Events table sort in numerical order.

Supported address formats

Regular formats:

- `aa:aa:aa:aa:aa:aa`
- `aa-aa-aa-aa-aa-aa`
- `aaaa.aaaa.aaaa`

MAC address

Specifying a MAC address in an IPv4 or IPv6 field generates a warning.

MAC addresses in IPv6 EUI-64 format (see RFC2373)

- `fe80:0000:0000:0000:aaaa:aaff:feaa:aaaa`
- `FE80::aaaa:aaff:feaa:aaaa`

MAC addresses are converted to IPv6 when stored.

Example:

`B9:0D:78:10:40:DA` becomes `fe80:0000:0000:0000:bb0D:78ff:fe10:40DA`

In this case, when looking for the MAC address you can use either `B9:0D:78:10:40:DA` or `fe80:0000:0000:0000:bb0D:78ff:fe10:40DA`, or the short version of the latter.

IPv4 address format

`a.b.c.d`

Examples:

- `Agent Address in_subnet 192.*`
  This input specifies IP addresses in the subnet starting with 192.
- `Agent Address in_subnet 192.0.0.0/8`
  This input specifies an agent address in a subnet that uses CIDR notation in its address. The first 8 bits are the network part of the address, leaving the last 24 bits for specific host addresses.

IPv6 address formats in full form and canonical form (see RFC5952)

- `2001:0db8:0000:0000:0000:ff00:0042:8329`
  Full form.
- `2001:db8:0:0:0:ff00:42:8329`
  Canonical form without leading zeroes in each group.
- `2001:db8::ff00:42:8329`
  Canonical form without consecutive sections of zeroes.

IPv4 address format in_subnet:

- `a.*`
- `a.b.*`
- `a.b.c.*`
- `a.b.c.d/8`
  A full address is required in the CIDR format .
  Example: `Agent Address in_subnet 192.0.0.0/8`

IPv6 address format in_subnet

Any IPv6 in the format stated above plus any usage of CIDR

Examples:

`2001:0db8:0000:0000:0000:ff00:0042:8329`

`2001:0db8:0000:0000:0000:ff00:0042:8329/24`

`2001:db8::/32`

The above two command uses CIDR notation.

For `2001:db8::/32`, you can omit part of the IPv6 address, depending of the subnet that you are querying.

Managing search-results fieldsets

The default fieldset contains the 63 most common event fields. These fields are available for creating data visualization charts and for viewing in the Events table. Each field (column) in this table can provide the 10 most and least common values.

Creating a fieldset for search results

About

The fieldset determines what search results fields are available for creating data visualization charts and what data columns appear in the Events table.

A fieldset can be shared in many searches.

You can modify a fieldset for individual searches, making it a custom version of the original fieldset, and then re-execute the search with your new fields.

Custom fieldset changes will not be propagated to the original fieldset . To update the original fieldset with your custom changes, click the edit link and then **Save**.

Procedure

Location: Left navigation > Search button > Search page

1. Click the fieldset button.
   - For a new search, the button defaults to **Default Fieldset**.
   - For an existing search, the button name is that of the last selected fieldset, or **Default Fieldset** if no selection was made.
2. From the Fieldset Lists dialog, select **Create a new set** from the drop down.
3. Select and deselect any necessary fields.

   To quickly locate a desired field, use the **Filter** field.
4. To add lookup list fields to the fieldset, click **Lookup Lists** and then select the desired field or fields.
5. Accept the default fieldset name or rename it.
6. Click **Save**.

See Also

- "Editing a fieldset for search results " below
- "Deleting a fieldset for search results " on the next page

Editing a fieldset for search results

About

The fieldset determines what search results fields are available for creating data visualization charts and what data columns appear in the Events table.

There are a possible of 176 fields in a fieldset. To manage the display of this data, you may want to limit the number of fields in a fieldset.

Procedure

Location: Left navigation > Search button > Search page

1. Click the fieldset button.

   The button name is that of the last selected fieldset, or **Default Fieldset** if no selection was made.
2. To select a different fieldset, use the drop-down in the Fieldset Lists dialog.
3. From the drop-down, select **Edit this set**.

   You can also select **edit** from the **Create new or edit to save changes** link.
4. Specify the desired fieldset fields.

   - To quickly locate a field, use the **Filter** field.
   - To conveniently manage the selection of fields in a fieldset, use the **Select all**, **Unselect all**, and **View all** buttons.

   Note: If you remove a field from a fieldset, Investigate will remove all the filters and charts that use that field.
5. To specify lookup list fields for the fieldset, click **Lookup Lists** and then make the appropriate selection(s).
6. To change the fieldset name, use the **Fieldset Name** field.
7. Click **Save**.

   The saved fieldset updates the global fieldset.

See Also

- "Creating a fieldset for search results" on page 19
- "Deleting a fieldset for search results " below

Deleting a fieldset for search results

About

- The fieldset determines what search results fields are available for creating data visualization charts and what data columns appear in the Events table.
- If two or more searches are using a particular fieldset, then the fieldset cannot be deleted.

Procedure

Location: Left navigation > Search button > Search page

1. Click the fieldset button.

   The button name is that of the last selected fieldset, or the default fieldset if no selection was made.
2. To select a different fieldset, use the drop-down in the Show Fields dialog.

3. From the drop down, select **Edit this set**.
4. Click **Delete**.

See Also

- "Creating a fieldset for search results" on page 19
- "Editing a fieldset for search results " on page 20

Viewing search results for a time range

About

- A Timeline selection focuses on the search results for a specific time range within the specified time period.
- The results of a Timeline selection are reflected in any data visualization and the Events table.

Procedure

Prerequisite

"Searching events" on page 11

Location: Left navigation > Search button > Search page > Timeline area

1. Ensure that the Timeline chart is visible.
2. Ensure that the **Range Selector** is enabled.

   With the range selector off, you can hover over a sparkline and view the specific time range and number of events for the sparkline.
3. Position the pointer in the time line and using the double-arrow cursor, drag in the desired time range.

   - The time scale for a large specified time range may have large increments.
   - To aid in your selection, the exact desired time range appears above the chart.
   - The event counts for the specified time period and selected time range appear above the chart.
   - If you turn off the **Range Selector**, and turn it back on again, the specified time range will still be selected.
4. To remove a specified time range, click **X** at the end of the "Timeline" time range.
5. To save the time range selection, click **Save**.

   The filter and data visualization is also saved.

See Also

- "Charting search-results data" below

Charting search-results data

To better understand search-results data, you can represent it graphically. From the Search page, data visualization enables you to add up to 10 charts.

ArcSight Investigate provides data comparison charts and non-comparisons data charts. Data comparison charts include line, column, bar, and area. Non-comparisons data charts include pie and scatter plot.

Charts (widgets) can be added from the Search page to the Dashboard (see "Adding a widget to the Dashboard" on page 54).

Charting search-results data using predefined security analytics charts

About

ArcSight Investigate enables you to chart search-results data using standard charts or predefined security analytics charts.

Investigate provides the following predefined charts:

Authentication activity		
	Login by Destination Address Over Time	
	Login by Destination Username Over Time	
	Login by Username	
	Login Over Time	
Source Activity		
	Bytes Out by Source Address	
	Destination Hostname by Source Address - Detailed	
	Destination Hostname by Source Address - Summary	
	Destination Port by Source Address - Detailed	
	Destination Port by Source Address - Summary	
	Source Antivirus Activity	
	Top Source Addresses	
Destination Activity		
	Bytes In by Destination Address	

	Bytes Out by Destination Address	
	Bytes Out by Destination Hostname	
	Bytes Out by Request URL	
	Destination Antivirus Activity	
	Destination Port by Destination Address	
	Source Address by Destination Address - Detailed	
	Source Address by Destination Address - Summary	
	Top Destination Addresses	
	Top Destination Hostname	
Port & Protocol Activity		
	Bytes In by Destination Port	
	Bytes Out by Destination Port	
	Secure Communication Ports-Bytes Out by Destination Hostname	
	Secure Communication Ports-Bytes Out By Source Address	
	Top Destination Ports	
General		
	Authorization Changes by Destination Address	
	Bytes In by Destination Username	
	Bytes In Over Time	
	Bytes Out by Destination Host and Source Username	
	Bytes Out by Device Vendor	
	Bytes Out by Source Username	
	Bytes Out Over Time	
	Events Count Over Time	
	Top Device Vendors	
DNS Analytics		
	DNS Analysis Over Time	
	Top Hosts by DNS Events Sum Bytes Out	
	Top Hosts by Number of Unique DGA Domains	
	Top Unique DGA Domains by Number of Hosts	

Procedure

Location: Left navigation > Search button > Search page > Visualize area

1. Expand the "Visualize" area.
2. Click **Create Visualizations**.
3. From the Add Visualization dialog, click the desired predefined analytics chart.

   - You can modify a predefined analytics chart that can be shared in many searches.
   - **Create New** is for using standard charts (see "Creating line, bar, column, and area charts" below, "Creating a pie chart" on page 30, and "Creating a scatter plot chart" on page 32).

Creating line, bar, column, and area charts

About

- Line, bar, column, area and scatter plot are data-comparison charts. For these charts, you can create up to six series of data comparisons.
- The first chart series sets the X- and Y-axis parameters, which remain set for any subsequent series.
- Any ordering specified in the first chart series applies to any subsequent series.
- For any subsequent chart series, you can specify different fields for **Filter By** and set aggregate functions for the X- and Y-axis parameters.
- Parameters that can accept the field highlight upon field drag and drop.
- Parameters that cannot accept the field turn red upon field drag and drop.
- X- and Y-axis options

Field type	X-axis function	Y-axis function
Time	minute (default) hour week month year value itself count count distinct	count Example: Count the number of events for the time period.

String	value itself (default) count count distinct (bar charts)	count (default) count distinct value itself (scatter chart and bar chart)
Number	actual number (default)	count count distinct sum (default) average max min Number value itself (only for scatter plot) **Note:** For the average function, the default is the arithmetic mean. Example: For bytes out, the average will be sum (Bytes Out) / number of events (that contains bytes out). If you selected **Group By User**, then ArcSight Investigate uses the formula: (sum (Bytes Out (only for events when `user!=Null`)) / distinct number of users (without `Null`)

For bar-type charts, what is stated above is reversed for the x- and y-axis.

- When dragging a discrete-value field to a continuous-value parameter, Investigate converts the field to a continuous-value field.

  Example

  For **File Name**, Investigate applies the applies the `count()` function.

- Within a parameter, fields appear in the following formats:
  - Single key/value pair — `<field>:<value>`

    Example

    ```
    department:sales
    ```

  - Single key with multiple values — `<field>:<value1>,<value2>,...`

    Example

    ```
    user:johnny, bob,...
    ```

  - Aggregate function — `<function>(<field>)`

    Example

    ```
    - sum(Bytes Out)
    - month(Event Time)
    ```

Procedure

Location: Left navigation > Search button > Search page > Visualize area

1. Expand the "Visualize" area.
2. Click **Create Visualizations**.
3. From the Add Visualization dialog, click **Create New** and then select the desired data comparison chart type.

   - Line, bar, column, and area are data-comparison charts.
   - **Predefined Templates** is for using ArcSight-defined charts (see "Charting search-results data using predefined security analytics charts" on page 23).

4. To change available fields for parameter selection, click **Default Fieldset** (see "Editing a fieldset for search results " on page 20).
5. Drag the desired field to **X-Axis**.

   - The parameter can receive a field with a continuous value .
   - Investigate applies the `sum()` aggregate function to any continuous-value field.
   - Investigate convert a discrete-value field to a continuous value by applying the `count()` aggregate function to the field.
   - The field specified for this parameter remains for any subsequent chart series. You can change the aggregate function for the parameter in a subsequent chart series.

   To change the aggregate function for the parameter

   a. Click the field in **X-Axis**.
   b. From the X-Axis dialog, select the desired value type from the **Aggregate values using** drop down.

      Only aggregate functions that can be applied to continuous-value fields are enabled.

6. Drag the desired field to **Y-Axis**.

   - The parameter can receive any discrete-value field.
   - Investigate applies the `count()` aggregate function to any continuous-value fields.
   - When dragging a field to **Y-Axis**, the scale and data labels of the axis appear.

     The label for **Y-Axis** is in the form, `<function>(<field>) or <field>`.
   - The field specified for this parameter remains for any subsequent chart series. You can change the aggregate function for the parameter in a subsequent chart series.

   To change the aggregate function for the parameter

   a. Click the field in **Y-Axis**.
   b. From the Y-Axis dialog, select the desired value type from the **Aggregate values using** drop-

down.

Only aggregate functions that can be applied to discrete-value fields are enabled.

7. To compare event field data against the whole dataset, drag the desired field to **Filter By**.

   - The parameter can receive multiple discrete fields.
   - The parameter is enabled when both the X- and Y-Axis parameter are set.
   - By default, all values for a field are applied in the **Filter By** parameter.

   To change field values for filtering

   a. Click the field in **Filter By**.
   b. From the Filter By dialog, specify desired field values for filtering.

      Select all and **Unselect all** are convenient for a field with many values where you want to selectively pick values.

8. To specify the field by which records should be ordered, click **Order by**.

   - The parameter is enabled when the **X-Axis** parameter is set.
   - The parameter orders the bars in the Y-Axis
   - Sort orders are dependent on the field used for the Y-Axis.
   - Records appear in ascending order by default.

9. For a Stacked Bar Chart, specify any segmenting of Y-Axis bars by dragging the desired field to **sub-categories**.

   A sub-category enables you to specify a secondary discrete-value field. Each bar in the Y-axis is segmented by this secondary category.

10. To view values in the chart, choose **Preview > Data Labels**.
11. To set a baseline for which to compare chart data, choose **Preview > Plot Line** and then specify baseline value in the adjacent field.

    A dotted black line appears in the chart at the specified value.

12. To create another data segment comparison, click **Add Series** and specify any new parameters and aggregate functions.

    - The **X-Axis** and **Y-Axis** parameters specified in the first chart series are inherited in this series. You can specify a different Y-axis parameter for any or all chart versions in the series (see procedure below).

- The aggregate functions for parameters in the first chart series are inherited in this series.
- To hide a chart object (line, bar, or column), click the color of the chart object in the chart legend. Undo this hide by clicking on the appropriate grayed color in the chart legend. This feature is especially useful if a chart object overlaps another.

To specify data for a subsequent series chart

a. To change the aggregate function for **X-Axis**, click in this parameter and then make the appropriate changes in the X-Axis dialog (see "To change the aggregate function for the parameter" on page 27).

b. To change the aggregate function for **Y-Axis**, click in this parameter and then make the appropriate changes in the Y-Axis dialog (see "To change the aggregate function for the parameter" on page 27).

c. To change the value for **Y-Axis**, drag the desired field to the parameter.

You can change the **Y-Axis** value for any or all chart series.

d. Drag the desired field to **Filter By**.

If you change **Order By** for any series, all chart series are affected.

e. For a bar chart, to segment Y-Axis bars by a secondary category, see step 10.

13. To add the chart to the Dashboard, choose  > **Add to Dashboard** from the chart panel.

- It is not necessary to save the search before adding the chart to the Dashboard.

Investigate auto-saves the search when add a chart to the Dashboard.

To remove the chart from the Dashboard

- Choose  > **Delete** from the chart panel.

14. To enlarge the chart, click  .

- Any other charts are hidden until your return the chart to its original size.

To return the chart to its original size

- Click the left-pointing arrow in the chart title bar.

15. To name (rename) the chart, choose  > **Rename** from the chart panel.

- The default name is the **X-Asis** parameter field name combined with the **Y-axis** parameter field name.

Example

BYTES OUT BY AGENT ADDRESS, AGENT SEVERITY BY DESTINATION USERNAME

- If you previously added the chart to the Dashboard, the new chart name will also appear for that chart.

16. Click **Done** and then **Save** in the task bar.
17. To add another chart, click ✚ and repeat steps 3 - 18.

Creating a pie chart

About

- Charts (widgets), including a pie chart, can be added from the Search page to the Dashboard.
- Parameters that can accept a field highlight.
- Parameters that cannot accept a field turn red.

Procedure

Location: Left navigation > Search button > Search page > Visualize area

1. Expand the "Visualize" area.
2. Click **Create Visualizations**.
3. From the Choose Visualizations dialog, select **PIE CHART**.
4. Drag the desired field to **Measure**.

   - This parameter takes a continuous-value field.
   - The field-supported aggregate function is applied.
   - Discrete-value fields are automatically converted to a continuous-value field with the `count()` aggregation function.
   - The parameter determines the size of the pie slice.

   To change the aggregate function for the parameter

   a. Click the field in **Measure**.
   b. From the Measure dialog, select the desired value type from the **Aggregate values using** drop down.

      Only aggregate functions that can be applied to continuous-value fields are enabled.

5. Drag the desired field to **Label**.

   - This parameter takes a discrete-value field. Events are grouped by unique values for the

specified field.

To change the aggregate function for the parameter

a. Click the field in **Label**.
b. From the Label dialog, select the desired value type from the **Aggregate values using** drop down.

Only aggregate functions that can be applied to discrete-value fields are enabled.

6. Drag the desired field to **Filter By**.

The parameter can receive multiple Discrete-value fields.

To change the aggregate function for the parameter

a. Click the field in **Filter By**.
b. From the Filter By dialog, deselect unwanted field values.

7. To add the chart to the Dashboard, choose ... > **Add to Dashboard** from the chart panel.

- It is not necessary to save the search before adding the chart to the Dashboard
- Investigate places the chart in the last position in the Dashboard.

To remove the chart from the Dashboard

- Choose ... > **Delete** from the chart panel.

8. To enlarge the chart, click  .

- Any other charts are hidden until your return the chart to its original size.

To return the chart to its original size

- Click the left-pointing arrow in the chart title bar.

9. To name (rename) the chart, choose ... > **Rename** from the chart panel.

If you previously added the chart to the Dashboard, the new chart name will not appear in the Dashboard.

10. Click **Done** and then **Save** in the task bar.
11. To add another chart, click ✚ and repeat steps 3 - 11.

See Also

- "Creating line, bar, column, and area charts" on page 25

- "Creating a scatter plot chart" below
- "Adding a widget to the Dashboard" on page 54

Creating a scatter plot chart

About

Charts (widgets), including a scatter plot chart can be added from the Search page to the Dashboard.

- Parameters that can accept a field highlight.
- Parameters that cannot accept a field turn red.

Procedure

Location: Left navigation > Search button > Search page > Visualize area

1. Expand the "Visualize" area.
2. Click **Create Visualizations**.
3. From the Choose Visualizations dialog, select **SCATTER PLOT**.
4. Drag the desired field to **X-Axis**.
   - The parameter can receive a field with a continuous value.
   - Investigate applies a field-supported aggregate function to any continuous-value field.
   - Investigate convert a discrete-value field to a continuous value by applying the `count()` aggregate function to the field.
5. Drag the desired field to **Y-Axis**.
   - The parameter can receive any discrete-value field.
   - Investigate applies the `count()`aggregate function to any continuous-value fields.

   To change the aggregate function for the parameter

   a. Click the field in **Y-Axis**.
   b. From the Y-Axis dialog, select the desired value type from the **Aggregate values using** drop down.

      Only aggregate functions that can be applied to discrete-value fields are enabled.
6. When dragging a field to **Y-axis**, the scale and data labels of the axis appear.

   The label for **Y-axis** is in the form, `<function>(<field>) or <field>`.
7. Drag the desired field to **Category**.
   - This parameter takes a discrete-value field.

- Each unique value for that field is represented by a different color point.

8. To add the chart to the Dashboard, choose ... > **Add to Dashboard** from the chart panel.
   - It is not necessary to save the search before adding the chart to the Dashboard
   - Investigate places the chart in the last position in the Dashboard.

   To remove the chart from the Dashboard

   - Choose ... > **Delete** from the chart panel.
9. To enlarge the chart, click  .
   - Any other charts are hidden until your return the chart to its original size.

   To return the chart to its original size

   - Click the left-pointing arrow in the chart title bar.
10. To name (rename) the chart, choose ... > **Rename** from the chart panel.

    If you previously added the chart to the Dashboard, the new chart name will not appear in the Dashboard.
11. Click **Done** and then **Save** in the task bar.
12. To add another chart, click ✚ and repeat steps 3 - 12.

See Also

- "Creating line, bar, column, and area charts" on page 25
- "Creating a pie chart" on page 30
- "Adding a widget to the Dashboard" on page 54

Editing search-results charts

About

Charts (widgets) can be added from the Search page to the Dashboard.

Procedure

Location: Left navigation > Search button > Search page > Visualize area

1. Ensure that the "Visualize" area is expanded.
2. To rename the chart, choose ... > **Rename** from the chart panel.

- The default name is the **X-asis** parameter field name combined with the **Y-axis** parameter field name.

  Example

  BYTES OUT BY AGENT ADDRESS, AGENT SEVERITY BY DESTINATION USERNAME

- If you previously added the chart to the Dashboard, the new chart name will also appear for that chart.

3. To expand a chart for editing, click  and then **Edit**.

   To return to the normal viewing mode, click the left-pointing arrow in the upper left corner.

4. To replace a parameter field:
   a. Hover over the parameter and then click **X**.
   b. Drag the new field to the parameter.

      - Parameters that can accept a field highlight.
      - Parameters that cannot accept a field turn red.

5. To change the aggregate function for the **X-Axis**, **Y-Axis**, **Measure**, and **Label** parameter fields:
   a. Click the parameter field.
   b. From the dialog, select the desired value type from the **Aggregate values using** drop-down.
   c. Click **Close**.
6. To change field values for filtering:
   a. Click the field in **Filter By**.
   b. From the Filter By dialog, specify desired field values for filtering.
7. To change the field by which records should be ordered, click the **Order By** parameter field.

   - This parameter field applies only to data-comparison charts (Line, bar, column, and area).
   - The parameter is enabled when both **X** and **Y-Axis** parameters are set.
   - The parameter orders the bars in the Y-Axis
   - Sort orders are dependent on the field used for the Y-Axis.
   - Records appear in ascending order by default.

8. To change the segmenting of Y-Axis bars in a bar chart:
   a. Hover over the **sub-categories** parameter field and click **X**.
   b. Drag the desired field to the parameter field.

A sub-category enables you to specify a secondary discrete-value field. Each bar in the Y-axis is segmented by this secondary category.

9. To view values in the chart, choose **Preview > Data Labels**.
10. To set a baseline for which to compare chart data, choose **Preview > Plot Line** and then specify baseline value in the adjacent field.

    A broken black line appears in the chart at the specified value.

11. To create another data segment comparison for data-comparison charts, click **Add Series** and specify any new parameters and aggregate functions.

    - The **X-Axis** and **Y-Axis** parameters specified in the first chart series are inherited in any subsequent series.
    - The aggregate functions for parameters in the first chart series are inherited in any subsequent series.
    - To hide a chart object (line, bar, or column), click the color of the chart object in the chart legend. Undo this hide by clicking on the appropriate grayed color in the chart legend. This feature is especially useful if a chart object overlaps another.

    To specify data for a subsequent series chart

    a. To change the aggregate function for **X-Axis**, click in this parameter and then make the appropriate changes in the X-Axis dialog (see step 5).
    b. To change the aggregate function for **Y-Axis**, click in this parameter and then make the appropriate changes in the Y-Axis dialog (see step 5).
    c. Drag the desired field to **Filter By**.

       If you change **Order By** for any series, all chart series are affected.

    d. For a bar chart, to segment Y-Axis bars by a secondary category, see step 8.

12. To specify the number of data points for a chart, choose ... **> Points to plot** from the chart panel.

    - The default number of data points is 15, potentially allowing for multiple chart pages for a data-intense chart.
    - If the chart is data intense, you can increase the number of data points in order to reduce the chart page count. The more data points that you specify, the more condense the chart, resulting in less pages.
    - If you add the chart to the Dashboard (see next step), the chart in the Dashboard will not reflect the data-point count that you specify here.

13. To add the chart to the Dashboard, choose

... > **Add to Dashboard** from the chart panel.

- Investigate places the chart in the last position in the Dashboard.

To remove the chart from the Dashboard

- Choose ... > **Delete** from the chart panel.

14. Click **Done** and then **Save** in the task bar.

See Also

- "Charting search-results data" on page 23

Deleting search-result charts

Procedure

Location: Left navigation > Search button > Search page > Visualize area

1. Ensure that the "Visualize" area is expanded.
2. For the desired chart, choose ... > **Delete**.

   If you added the chart to the Dashboard, the deleted chart will remain in the Dashboard.

   - To delete the chart from the Dashboard, see "Deleting a widget from the Dashboard" on page 55.
   - If you delete a chart from the Dashboard, the deleted chart is not removed from the search in the Search page.

Zooming in and out on charts

About

Investigatecharts support clustering and group data points. You can drill down on an individual data point in a chart to view all the grouped data points.

Procedure

Location: Left navigation > Search button > Search page > Visualize area

- Click the desired data point.
  - This allows you to drill down further and view the data points grouped under that point.
  - Clicking on the zoom out icon takes you one level up from where you drilled down.
  - The home button takes you to the top most zoom level with at least two data points.
  - You can drill down until you have the single-value data point.

- Hover over a data point enables you to view the X and Y value of the data point.
- **Data Labels** enables you to view individual data point along with the count of grouped data points.
- By default, the data point grouping is an average value of group data points.
- You can select the data points by sum.

  Example: Bytes out by Source Address, when data points are grouped by subnet, you may want to display the sum of outgoing traffic or average outgoing traffic per subnet.

Managing search results information

ArcSight Investigate lists search-result events in the Events table. The various fields of the event records are represented by the table column headers. Field columns are determined by the fieldset being used and the Show Columns feature.

To manage data in the Events table, Investigate enables you to view the most and least common values for an event record field, pin field columns to better compare values, view all fields of an event, and view select event data.

Viewing the most and least common values for an event record field

About

To help you filter for data security threats, ArcSight Investigate enables you to quickly display the most and least common values for a field. This translates into the count and percentage of hits for the value. For example, the **devicevendor** field could have a top value of "bluecoat" with a count of 3,000 hits, which is 30% of 10,000 results.

Procedure

Prerequisite

"Searching events" on page 11

Location

Left navigation > Search button > Search page > Events area

1. Ensure that the Events table is visible.
2. From the desired field column header, right click and then select **Preview Top/Least**.

   The default view in the dialog is the greatest data values in descending order.
3. To view the least common data values, click **View bottom 10** from the dialog.

See Also

- "Viewing all fields of an event" on the next page

- "Viewing select event data" on the next page

Pinning field columns to help analyze events

About

It can be helpful to pin a field column—to make a column horizontally stationary, in order to better compare the column values against those of other columns.

Procedure

Prerequisite

"Searching events" on page 11

Location

Left navigation > Search button > Search page > Events area

1. Ensure that the Events table is visible.
2. From the desired column header, right click and select **Make Sticky**.
   - The column moves to the extreme left in the Events table.
   - The sticky columns will not scroll horizontally.
   - You can make multiple columns stationary.
   - If there is an existing stationary column, the new stationary column is positioned to the right of that one.
3. To release a stationary column, right click the column header and then select **Unstick**.

Viewing all fields of an event

About

- ArcSight Investigate enables you to expand an event record and view all the record fields. Using this feature, you can quickly view the details of a single event without having to add all the fields of the fieldset.
- Depending on your data access permissions, you may not see all the possible fields for an event. From the user page (**Left navigation > [user] > My Profile > Data Access > My Profile**), you can view event fields for which you have access.

Procedure

Prerequisite

"Searching events" on page 11

Location

Left navigation > Search button > Search page > Events area

1. Ensure that the Events table is visible.
2. Click the arrow of the desired agent address.

   All the fields that are part of field set display, but are grouped in different categories. Not all the event fields display.

3. To view information about a field, click the arrow of the desired field.

   You can have multiple fields open at the same time.

See Also

"Viewing the most and least common values for an event record field" on page 37

Viewing select event data

About

From Events table, you can specify how event-record data is displayed.

- View only a select event or events
- Limit the display of field columns
- Sort values for an event field
- Arrange event records based on a common field value

Procedure

Prerequisite

"Searching events" on page 11

Location: Left navigation > Search button > Search page > Events area

1. Ensure that the Events table is visible.
2. To view a selected event, click in the event row and then click **Only show selection**.

   Use the shift and control keys to select multiple events.

3. To limit the display of field columns, click  and then deselect undesired fields from the Show Columns dialog.

   - When using a fieldset of more than 20 fields, it may be easier to quickly hide and reveal field

columns, rather than scrolling left and right, or rearranging the column order.

- To find a field, you can use the filter feature.
- To directly hide a field column in the Events table, right click the desired column header and then select **Hide Column**.
- To reveal a hidden field column in the Events table, click  and then select the hidden field column.

4. To reorder field columns, click and drag desired columns to new positions.
5. To sort values for a field column, click the appropriate arrow in the desired column heading.
   - The default order is descending.
   - Click the column header for ascending and descending orders.
6. To view all the event data based on a particular field value, right click on the desired field value and then select **Search For**.

   Below the selected event record, Investigate lists all the event records with a matching field value.

See Also

- "Viewing the most and least common values for an event record field" on page 37
- "Pinning field columns to help analyze events" on page 38

Exporting search results

About

- ArcSight Investigate can export search results to:
  - CSV file, which includes only Events table data. The data appears in data-table format and can be read by such applications as Microsoft Excel and Apple Numbers.
  - PDF file, which will contain details about the search conditions and any charts.
- Exported data is based on the fieldset specified for the search. Filtering has no impact on exported data. If you edit the fieldset, this is reflected in the fields available for the events.
- Hidden columns are exported.

Procedure

Location: Left navigation > Search button > Search page > Events

1. Click either 

from the "Events" area or **Export to PDF** from the task bar.

   Exporting
2. Open the downloaded file in an appropriate application.

See also

- "Viewing select event data" on page 39
- "Pinning field columns to help analyze events" on page 38

Finding authenticated users

About

This feature enables you to find the users who have successfully authenticated and are tied to a particular IP address or host name in the last 24 hours. This time range cannot be changed.

Procedure

Left navigation > Search button > Search page > Events area

1. Ensure that the Events table is visible.
2. Right-click on the desired field value and choose **Get Authenticated User**.

   Note: The fieldset for the original search must include `deviceReceiptTime` as one of the attributes. (The original search is the search that produced the search results in the Search page, including the Events table from which you executed the Get Authenticated User command.)

   - Depending on your field value choice, the address appears in the search query field in the following format:

     ```
     Source Address = <address> and Category Behavior=/Authentication/Verify and Categroy Outcome=Success
     ```

     ```
     Source Hostname = <hostname address> and Category Behavior=/Authentication/Verify and Categroy Outcome=Success
     ```

   - Search results are updated in the Search page.
   - The new search appears in the left navigation in the format of `<original search name>-user logins`
   - ArcSight Investigate auto saves the search if authenticated users are found. The saved search appears in the left navigation in the format of `<original search name>-user logins`
   - If Investigate finds no search results, the search is not auto saved and appears in the left navigation in the format of `<original search name x+1>`

Managing lookup lists

The lookup list feature enables you to create additional tables with different fields in the Vertica database. These additional lookup list fields can be used in the search query along with the other 176

schema fields.

Adding a lookup list to extend searches

About

- You can use a lookup list as search criteria in a search query. The lookup list is joined with the fields of the schema table that is part of ArcSight Investigate.
- Fields from a lookup list can be used in a fieldset. This fieldset can be comprised entirely of lookup list fields or combined with fields from the schema table.
- You can join multiple lookup list to the schema table.
- You can append fields from multiple lookup lists to a fieldset.
- If you attempt to append the schema table with a lookup list where there is a duplicate key field, the operation will fail. Other fields in a lookup list may have duplicate values.
- Investigate stores a lookup list as a table in the Vertica database.

Procedure

Location: Left navigation > Configuration > Lookup Lists > Lookup Lists page

1. Click **Add**.

   The lookup list needs to be a CSV file with the following requirements:

   - File extension must be `csv`
   - First row must be a comma separated list of column or field names. These are the columns/fields of the lookup list.
   - Rest of the rows in the file must be comma separated values for the columns specified in the first row.
   - All rows must have the same number of values, which must match the number of columns specified in the first row.
   - You need to select one of the columns as the key field
   - Values of the key field must be unique.
   - File may not have more that 2 million rows (excluding the first row)
   - File size may not exceed 150 MB.
   - File may not contain more than 25 columns/fields
   - Names of the columns/fields (names in the first row) may not exceed 40chars. They must start with an alphabet and contain alphanumeric characters and the '_' character only.

   If any requirements are not met, the add operation will fail.

2. From the Lookup Lists / Add New Lookup List page, specify the desired CSV file.
3. Specify a user-friendly lookup list name in the **Lookup List Name** field.
   - Lookup list name can be no more than 20 characters long. The name must start with an alphabet character and may contain only alphanumeric and '_' characters.
   - In the fieldset, the lookup file name displays on the top and the fields display underneath. You can click on the field check boxes to make them part of the fieldset.
   - ArcSight Investigate displays all the fields of the lookup list, each with the default value type of `text`.
4. Specify the key field and either accept the value type for this field or specify a different one.

   The key field identifies which field can be used for the `in list` operator in a query search.
5. Specify the value type for each lookup list field or accept the default.
   - The default value type is `domain`.
   - Possible value types:

domain	
float	For a number whose radix point can be placed anywhere relative to the significant digits of the number.
hostname	
int	Integer value
ip4	IPv4 address
ip6	IPv6 address
mac	
short text	Text that not exceed 1K of space
long text	Text that not exceed 4K of space
time	Timestamp
url	Does not exceed 4K
username	A string type

   - View the CSV file to help you determine the best value type for the lookup list fields.
6. Click **Upload** to save any specified field value types and to save the file as a table in the Vertica database.
   - The lookup list appears in the table on the Lookup List page.

- From the Lookup List page, you can click on the entry of a list to view its contents and replace the entire contents of the list. You can click on the check box against a specific list to display the delete icon on the top right, to delete the list. (see "Editing a lookup table" on page 1 or "Deleting a lookup list" below, respectively).
- If there is a time attribute in a lookup list, it will be converted to local time.

See also

- "Creating a fieldset for search results" on page 19
- "Searching events" on page 11
- "Searching events in ESM" on the next page

Replacing a lookup list

About

- This operation truncates (removes all content) from an existing lookup list and populates it with content from a new CSV file.
- Search queries that use the original lookup list are not affected by the truncation.
- While you can change the contents of the lookup list, you cannot change the list name.

Procedure

Location: Left navigation > Configuration > Lookup List

1. Select the desired lookup list and then click **Replace**.
   Only one list can be updated at a time.
2. From the Upload File dialog, choose the CSV file you want to use to replace the contents of the selected lookup list.
   - The requirements for the CSV file are the same as those for the Add operation (see "Adding a lookup list to extend searches" on page 42). Additionally, the column/field names specified in the first row for the CSV file must be identical to ones already in the lookup list.
   - If there is a time attribute in the lookup list, it will be converted to local time.

Deleting a lookup list

About

- For a saved search query that uses a deleted lookup list, the query will fail.
- For a saved field set that uses a deleted lookup list, operations using the fieldset will fail.
- If there is a time attribute in the lookup list, it will be converted to local time.

Procedure

Location: Left navigation > Configuration > Lookup Lists page

- Select the desired lookup list and then click  .

Searching events in ESM

About

- Using ArcSight Investigate, ArcSight Enterprise Security Manager (ESM) (Console or ArcSight Command Center (ACC)) enables you to investigate events from an ESM channel.
- From ESM, you can initiate a search in Investigate on a maximum of five fields.

  See the *ESM Release Notes* and depending upon your product, either the *HPE Security ArcSight Command Center User's Guide* or *HPE Security ArcSight ESM Administrator's Guide*.
- An event search consists of specifying query input, search-result fields, and the time period to search within.
- A search query can either have a fixed start and end date, where data cannot be refreshed, or a search can have a "canned" date range. For example, for a last-30-minutes "canned" search, data is updated upon re-executing the search based on the most recent 30 minutes.
- Within Investigate, you can filter ESM data for more specific results.
- If an event does not have data for a schema field, this absence of data (null) is represented in various ways in the Search page.

Search field	`Null`, `NULL` and `null` query formats are supported
Events table	Empty cell
Charts	*`(Null)`*
Empty field from ESM (`name=''`)	`name = '', NULL`

- Refreshing the browser as you update a search does not save your changes. Changes are only saved by clicking **Save** from the task bar or by auto save if you navigate away from the search.
- For a search that was created in a different timezone, Timeline will convert the time segments to local times. If there is a time attribute in a chart or the Events table, it will also be converted to local time. The aggregation for all these, however, will reflect that of the original timezone. For example, if Timeline has seven bars in the original timezone, the number of bars could be more or less now to reflect the current timezone.

Procedure

Prerequisite

New ESM user:

Run the configuration wizard (see "Using the Configuration Wizard" in the *HPE Security ArcSight ESM Installation Guide*).

Existing ESM user who upgraded to 6.11:

1. Login to the system and go to `/etc/bin` directory
2. Stop the manager.

   ```
   ./arcsight_services stop manager
   ```
3. `cd /opt/arcsight/manager/bin`
4. `./arcsight managersetup`
5. Enable Investigate as done in the configuration wizard for a fresh install.
6. Start the manager.

   ```
   ./arcsight start manager
   ```

ESM Console Location:	ESM > Event Detail (Inspect/Edit) panel
	ESM > Active Channel
ACC Location:	ESM > Event Detail
	ESM > Active Channel
	ESM > Visualize Events
	ESM > Active Channel
	ESM > Dashboards

1. Open an event viewer such as an active channel, or view event details in the Inspect/Edit panel.
2. Right-click a row and make the appropriate selection.

   Note: ESM fields that are not supported in Investigate searches appear disabled.

   For a list of supported fields, see "Running ArcSight Investigate Searches" under "Usage Notes" in the ESM 6.11 Release Notes. Also see the 6.11 *HPE Security ArcSight ESM Command Center User's Guide*.

   - To search on a specific value, select **ArcSight Investigate**.

     ESM generates a URL comprised of:

     - `query` equals `SELECTED COLUMN NAME = <title of column>`

       Example

       ```
       SELECTED COLUMN NAME = Employee
       ```

- `StartTime` equals `<time stamp>`
- `endTime` equals `<time stamp>`

- To search on one or more values, select **ArcSight Investigate (Multiple Fields)**.
  - From the dialog, select up to five fields for investigation. These fields are based on the columns that are available on the channel.
  - ESM generates a URL comprised with:
    - `query` equals `SELECTED COLUMN NAME = <title of column>`

      Example

      `SELECTED COLUMN NAME = Employee`
    - `StartTime equals <time stamp>`
    - `endTime equals <time stamp>`
- ESM opens a browser with the ESM-generated URL and creates a new search in Investigate.

  To modify this search, see "Searching events" on page 11.

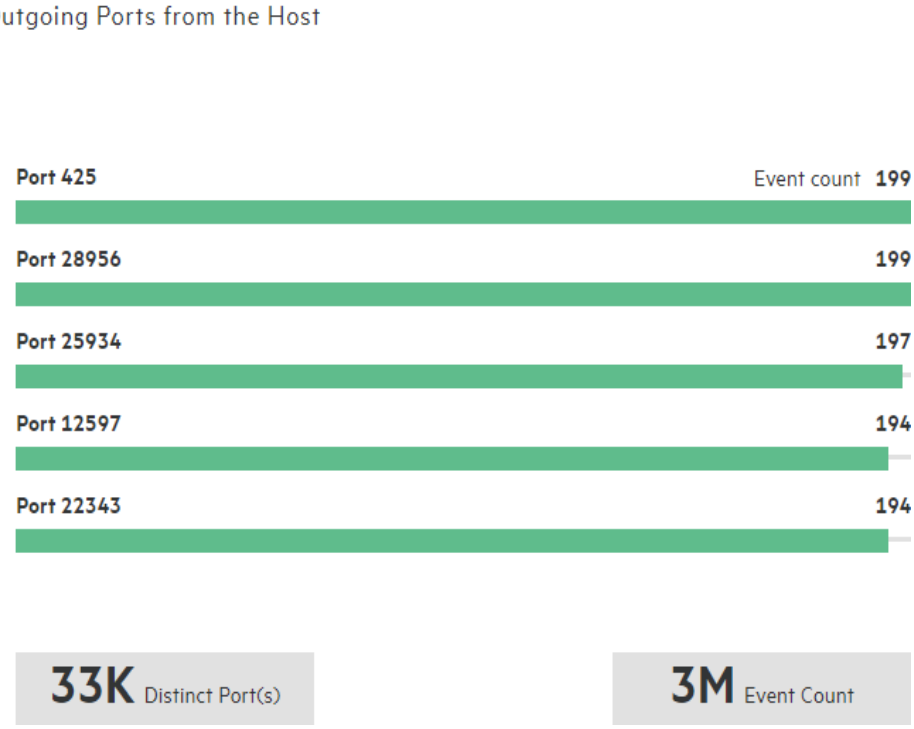
Chapter 3: Viewing event traffic

About

Host Profiler is a predefined dashboard where you can monitor event traffic for a specified host using visualization widgets. The traffic displayed is for the five most active host ports and communication paths related to other systems. Event traffic is charted for the following:

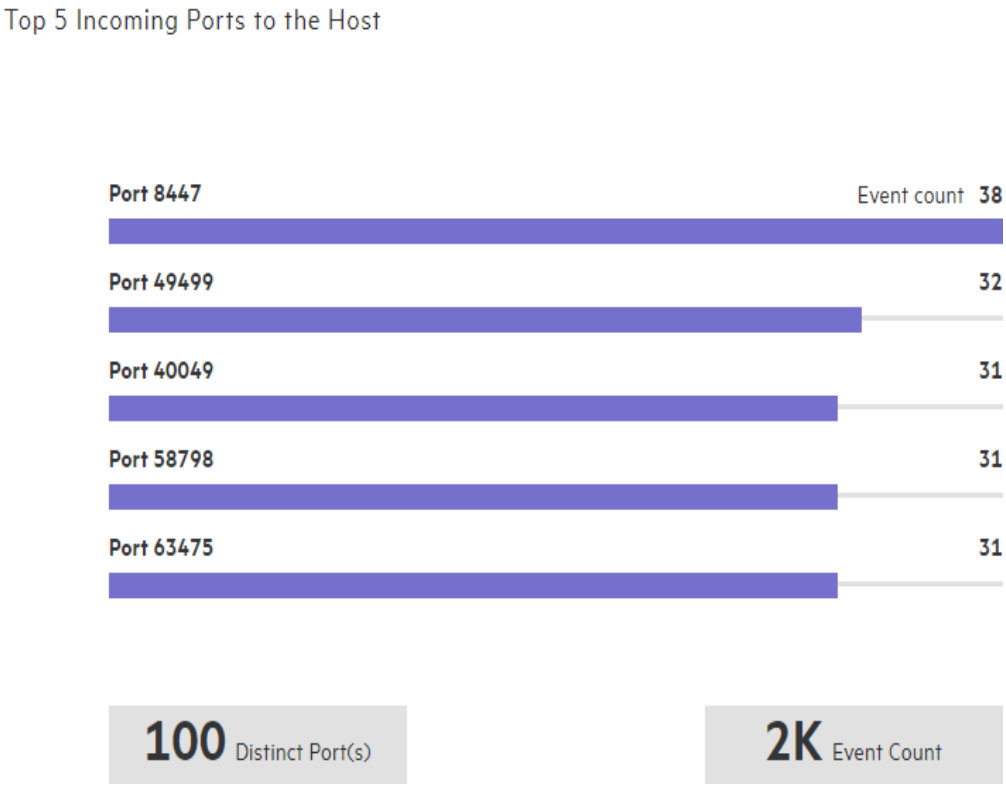
- Outgoing ports from a host
  - Ports of a specified host sending events to various systems. Five most active ports are represented in a bar chart.

    Example

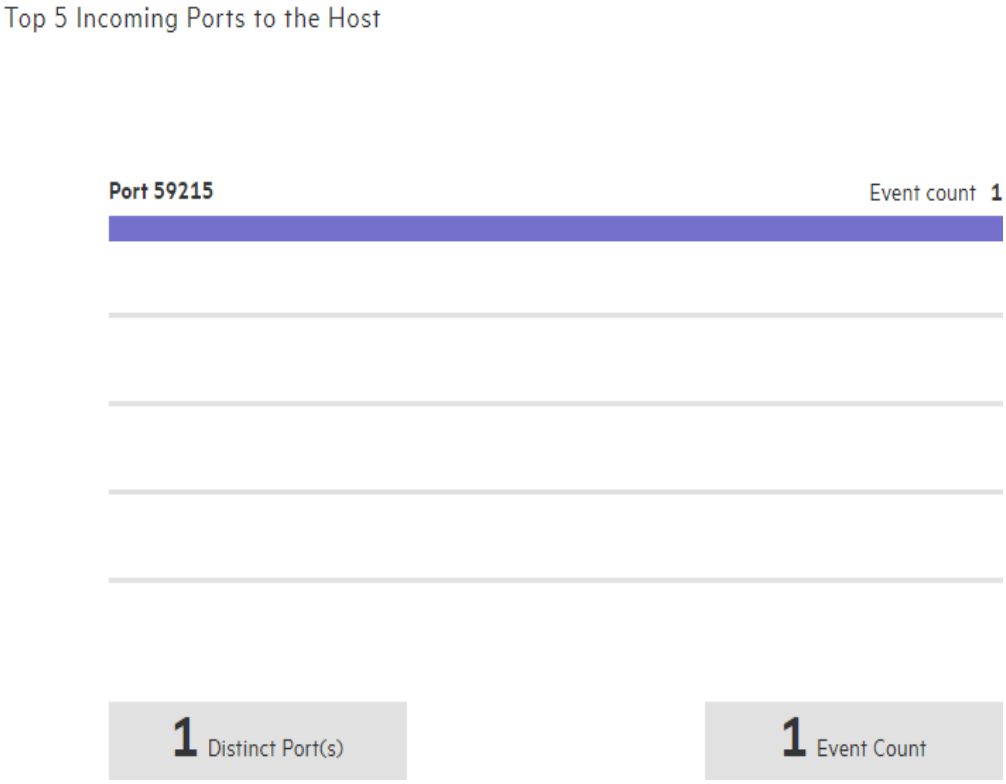
  - While Host Profiler lists the five most active ports in a visualization widget, the widget also displays the total number of events in the specified time range and the number of total ports involved. In this example, even though 983 events passed through the five most active ports, there were a total of three million events passing through thirty-three thousand ports in all.
  - Green bars are used to represent the event count on incoming ports.
- Incoming ports to a host
  - Ports of a specified host receiving events from various systems. Five most active ports are represented in a bar chart.

Example



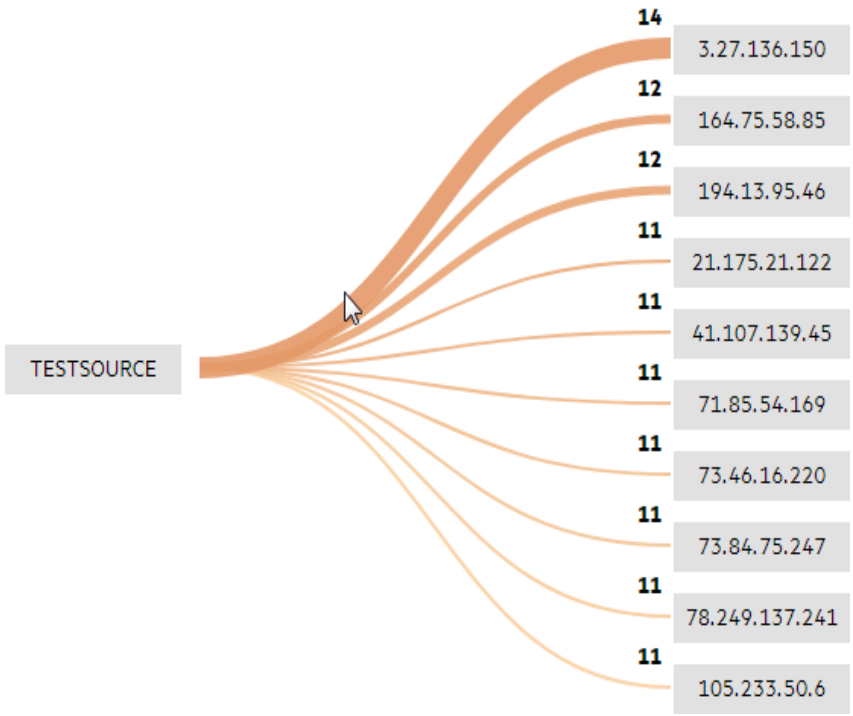
- In this example, even though 163 events passed through the five most active ports, there are a total of 2,000 events passing through 100 ports in all.
- There could be times when less than five ports are used by a specified host. In this case, the data in the bar element(s) will match what is given in the totals.

  Example



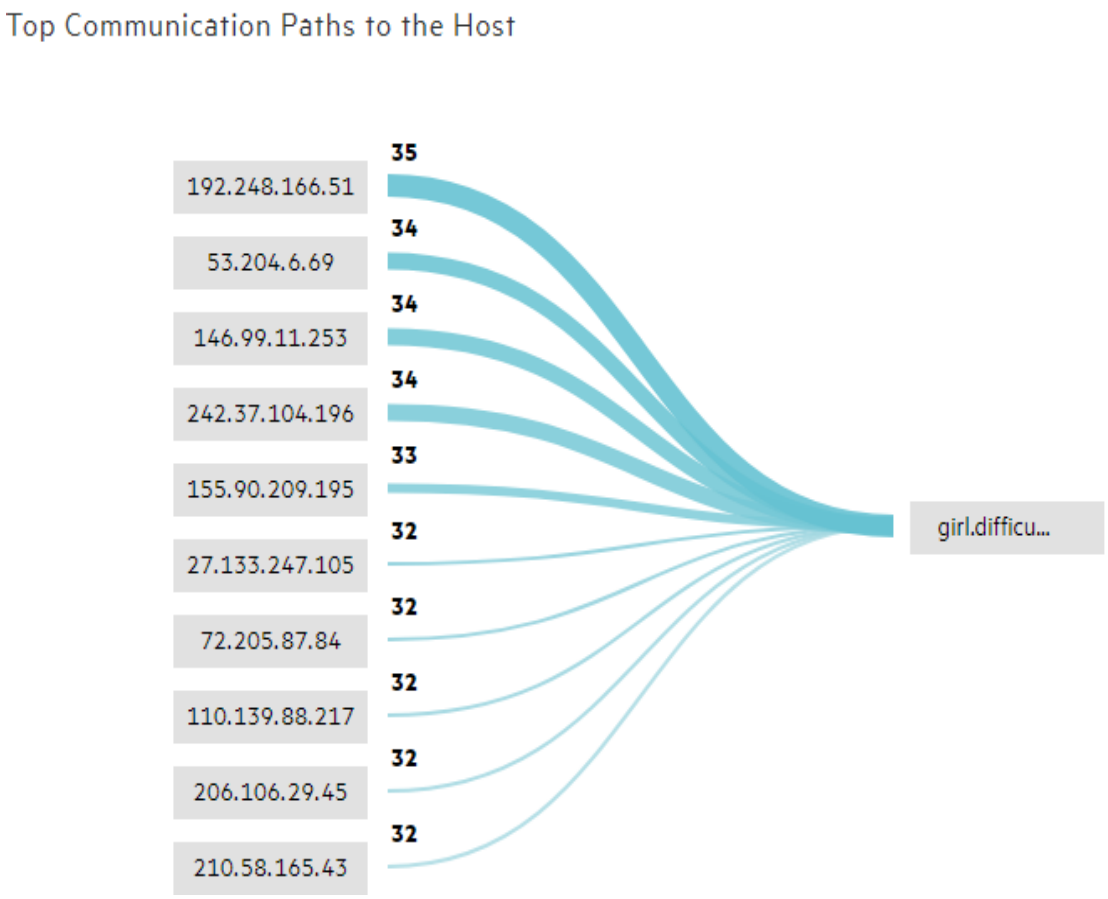
  - Blue bars are used to represent the event count on incoming ports.
- Communication paths from a host
  - Five most active system are represented in a Sankey chart.

    Example



  - Green lines represent paths from a specified host.
  - The number associated with each line is the number of events sent from a specified host.
- Communication paths to a host
  - Five most active system are represented in a Sankey chart.

    Example



- Blue lines represent paths from a specified host.
- The number associated with each line is the number of events sent to a specified host.

Procedure

Location: Left navigation > Insights > Host Profiler > Host Profiler page

1. Specify the time range in which you will profile a desired host.
   - Custom ranges are not provided, only quick ranges.
   - The default time range is 24 hours. The time range can be changed after the Host Profiler renders for the first time.
2. From the search field, specify the host you want to profile and then click **Profile**.
   - You can specify the desired host either by its IP address or host name.
   - Using the IP address, you can either type this address directly or use the `ip =` operator.
   - IPv4 and IPv6 addresses are supported, but not MAC addresses.
   - Using the host name, you can either type the name directly or use the `name =` operator.

- Host Profiler auto-suggests search input based on what you type in the search field. The suggested search input appears in a drop-down.
- If millions of events are retrieved, the search could pause. To resume, click the play button () from the progress bar at the top of the Host Profiler page.
  - The search pauses to indicate that the number of search results returned may impact the search performance. You may want to refine the search criteria and/or re-execute the search for a smaller time range.
  - Search results are ordered by date, so a result set with millions of total records will bring back the same million records in subsequent host profiles. The result set should be ordered by device receipt time, with the newest events returning first.

Depending on your environment, all four visualization widgets will display data or only two will display data, either for incoming ports and communication paths or outgoing ports and communication paths.

Chapter 4: Managing dashboard widgets

The Dashboard provides widgets to simultaneously monitor numerous event flows and create text boxes.

Dashboard widgets include a set of controls to pause or continue searches. If millions of events are retrieved, the search could pause. To resume, click the play button (▶

Adding a widget to the Dashboard

About

ArcSight Investigate provides for two types of widgets: Data visualization chart and text box. The former is added from the Search page and the latter is created in the Dashboard.

Procedure

Location: Left navigation > Dashboard button > Dashboard page

1. To add a text box widget to the Dashboard, click **Add Text Box** in the task bar.
   - Type text directly in the text box.
   - To delete the text box, choose ... > **Delete** from the text box panel.

Location: Left navigation > Search button > Search page

2. To add a chart to the Dashboard, open the desired search and then expand the "Visualize" area.
3. Choose ... > **Add to Dashboard** from the chart panel of the desired chart.
   - Repeat this step for each chart that you want to add to the Dashboard.
   - To change the chart before adding it to the Dashboard, see "Editing search-results charts" on page 33
   - To delete the chart from the Dashboard, in the Dashboard choose ... > **Delete** from the chart panel.

Location: Left navigation > Dashboard button > Dashboard page

4. To view the latest data for a chart associated with a real-time search, choose ... > **Refresh** from the chart panel.

Refresh a chart associated with a real-time search in order to see the latest data in the chart.

See Also

- "Creating line, bar, column, and area charts" on page 25
- "Creating a pie chart" on page 30
- "Creating a scatter plot chart" on page 32

Deleting a widget from the Dashboard

About

ArcSight Investigate provides for two types of widgets: Data visualization chart and text box. The former is added from the Search page and the latter is created in Dashboard.

Procedure

Location: Left navigation > Dashboard button > Dashboard page

- For the desired widget, choose ... > **Delete**.

  A deleted data visualization chart is removed from the Dashboard, but not from the originating search in the Search page.

See Also

- "Editing search-results charts" on page 33

Exporting Dashboard widgets to a PDF file

About

All the Dashboard widgets (charts and text boxes) are exported to a PDF file. You cannot pick and choose.

Procedure

Location: Left navigation > Dashboard button > Dashboard page

- Click **Export to PDF** from the task bar.

See also

"Exporting search results" on page 40

Chapter 5: DNS Analytics

Location: Insights> DNS Analytics

A *Domain Generating Algorithm* (DGA) is a program or subroutine, often seen in malware, that periodically provides new domains on demand or on the fly.

The following pre-set visualizations displaying DGA-related activity are shown on the **DNS Analytics** page. The visualizations display the results of the `#DGA Events` and `#DNS Events` queries.

If these visualizations do not show the desired results or data, you can create custom visualizations to accommodate your requirements.

Note: In order to track DGA activity, you must use and configure the MS-DNS tracelog connector on the MS-DNS server to send DGA events. Instructions for configuring the MS-DNS connector are given here.

If millions of events are retrieved for a visualization, the search could pause. To resume, click the play button (

Top Hosts by Number of Unique DGA Domains

Top Hosts by # of Unique DGA Domains shows a list of the top hosts reporting DGA domains, sorted by the number of unique domains.

Top Hosts by DNS Events Sum Bytes Out

Top Hosts by DNS Events Sum Bytes Out shows the top hosts reporting DNS events and the total bytes sent by each.

Top Unique DGA Domains by Number of Hosts

Top Unique DGA Domains by Number of Hosts shows the top DGA domains reporting DGA events, sorted by the number of reporting hosts.

DNS Analysis Over Time

DNS Analysis Over Time shows the a graph of the number of DNS and DGA events reported over time.

Configuring MS-DNS SmartConnector for DGA

In order to monitor DGA events, the MS-DNS Tracelog SmartConnector must be installed on your DNS server and then configured with the correct map files and whitelist file. Your SmartConnector may be a standalone connector or one managed by ArcMC.

These instructions assume you have already installed the MS-DNS SmartConnector on your MS DNS server. For more details on configuring SmartConnectors, see the SmartConnector User's Guide, available from Protect724.

Note: SmartConnector version GA 7.8.0.8070 is supported for DGA configuration.

Configuring Standalone SmartConnector

To configure a standalone MS-DNS SmartConnector:

1. In a text editor, create and save the following files. *Sample content* is shown here; your files should include content tailored to your own requirements.

File	Description	Sample Content
dga_ whitelist.txt	White list file. Includes all domains that are not scanned by the connector DGA detection.	google.com youtube.com facebook.com baidu.com wikipedia.org yahoo.com reddit.com google.co.in qq.com taobao.com amazon.com twitter.com
map.2.properties	Numbered connector map file, which calls the _domainWhitelist operation. This operation is a lookup for whitelisted domains in each event and will mark them as WHITELISTED, to be dropped by the filter later. **Note:** Adjust the sequence numbers of your new map files based on any existing map files. For example, if the last map file in the connector has the number 3, change the first new DGA map file to 4 and increment the rest of the files accordingly.)	!Flags,Overwrite+ set.expr (destinationHostName).event.deviceCustomFloatingPoint2Label __domainWhitelist(destinationHostName)

File	Description	Sample Content

map.3.properties	Numbered connector map file, which calls the dgaForbiddenTrigrams operation. This operation applies the forbiddenTrigrams DGA classifier on every event and returns 1 or 0 for each.
	Note: Adjust the sequence numbers of your new map files based on any existing map files. For example, if the last map file in the connector has the number 3, change the first new DGA map file to 4 and increment the rest of the files accordingly.)
		`!Flags,Overwrite+`
		`set.expr(destinationHostName).event.deviceCustomNumber1`
		`__dgaForbiddenTrigrams(destinationHostName)`

map.4.properties	Numbered connector map file, which calls the ForbiddenTrigramsHelper operation. This is a helper function that adds a label to the dga field in CEF.
	Note: Adjust the sequence numbers of your new map files based on any existing map files. For example, if the last map file in the connector has the number 3, change the first new DGA map file to 4 and increment the rest of the files accordingly.)
		`!Flags,Overwrite+`
		`set.expr (deviceCustomNumber1).event.deviceCustomNumber1Label`
		`__dgaForbiddenTrigramsHelper(deviceCustomNumber1)`

2. Copy the whitelist file and map files to the connector you are configuring, as follows:

File	Copy to...
dga_whitelist.txt	<ArcsightSmartConnector installation path>/current/user/agent/
x map.*.properties	<ArcsightSmartConnector installation path>/current/user/agent/map

3. Configure the connector to filter whitelisted domains. The whitelist filters both exact and suffix matches.
4. Restart the connector.

Configuring SmartConnectors managed by ArcMC

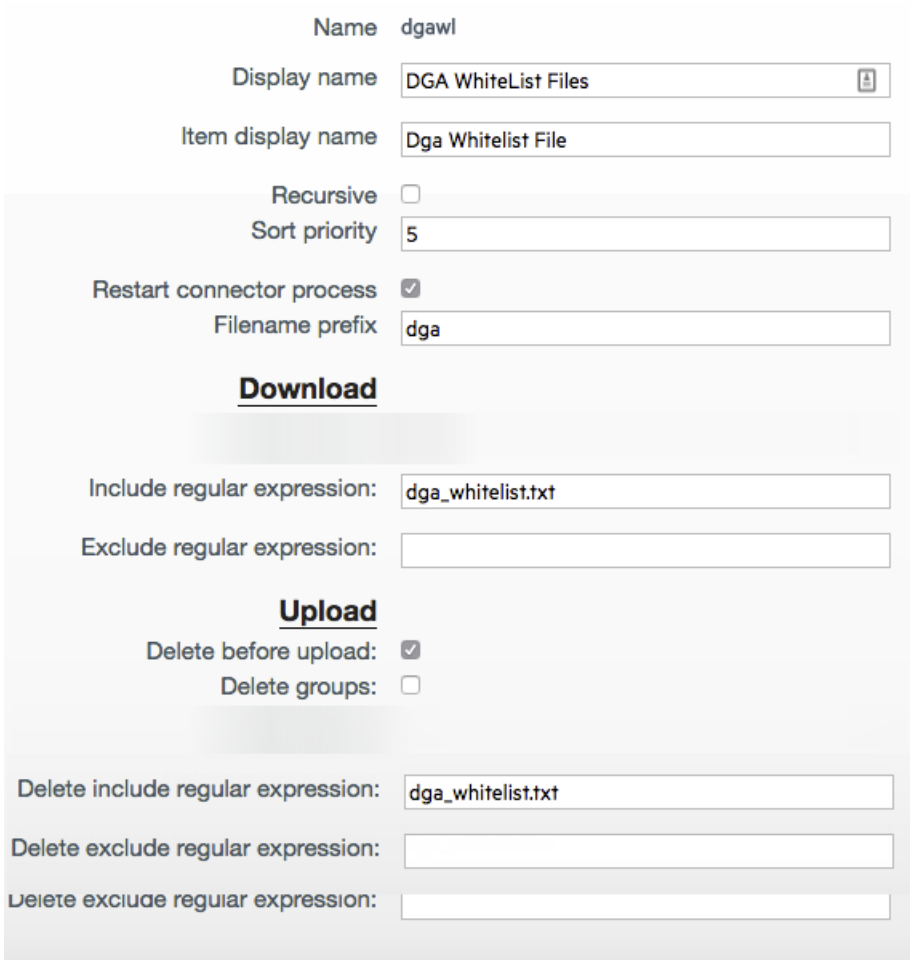
If your SmartConnector is managed by ArcMC, you can push the map files and whitelist files as configurations to the managed connector, as well as configure the whitelist filter.

Map Files

1. Under **Configuration Management > All Subscriber Configurations**, create a new subscriber or subscribers (the connector or connectors to be configured).
2. Use the **Import** option to add the DGA map files. Choose your connector and map file configuration type.
3. Click **Add Property** to add and upload your map files one-by-one. Alternatively, you can create the properties files and copy their contents into the Edit box.
4. Save your settings.
5. Restart each managed connector using **Node Management > Containers > Restart.**

Whitelist File

1. Select **Administration > Repositories**
2. Click **Create New Repository**, and fill in the settings as follows:



3. Choose **Upload To Repository** and follow the wizard to upload the new dga_whitelist.txt. The wizard will delete any existing list and replace it with the new one.

Configuring the Whitelist Filter

1. Click **Node Management > Connector** and select your MS-DNS connector.
2. Select **Runtime Parameters.**
3. Pick a desired destination, such as Kafka.
4. From the parameter groups list, select *zonebasedfiltering,*and then click **Next**.
5. In the **Filter Out** field, enter *deviceCustomFloatingPoint2Label deviceCustomFloatingPoint2Label EQ "WHITELISTED"*

Chapter 6: SOAR Application Integration

ArcSight Investigate supports integration with a selected SOAR (Security Orchestration, Automation and Response) application.

SOAR applications enable enterprises to automate their IT and security operations. When integrated with other applications and network devices, SOAR applications can orchestrate an automatic or manual response to an IT or security event in the enterprise network. SOAR applications provide a single-pane-of-glass view for the enterprise network operations personnel.

The grouping of orchestration steps and the relationships between them is represented in graphic formats called playbooks or *workflows*. ArcSight Investigate SOAR integration will trigger playbooks in the SOAR applications from the Search Grid. A user's right-click action on an event displayed in the Search Grid will pass the entire context of the event to the SOAR application using the application's REST APIs. In turn, the REST API call will trigger a playbook in the SOAR application which will execute the sequence of steps to accomplish the action initiated by the user. Once the executions are complete, the final step in the playbook will send the results of the executions to Investigate using an API exposed by Investigate. These results are displayed in a new Investigate page, under the **Integrations** tab, called **SOAR Notification.**

Supported SOAR Apps

ArcSight Investigate only supports the integration of a single SOAR application at one time. Integration of a second SOAR application at the same time will replace any existing integration.

Currently, Investigate can be integrated with either Demisto, Operations Orchestration, or Siemplify Enterprise.

Configuring Investigate for SOAR integration

SOAR Application integration involves the following overall process:

1. **Create the necessary playbook triggers and playbooks in the SOAR Application:** Before integrating with ArcSight Investigate, you must create the desired playbook triggers and playbooks in your SOAR application. Please refer to the SOAR application's documentation for details.
2. **"SOAR Configuration Parameters" on the next page**Note that only one supported SOAR application configuration can be active in ArcSight Investigate. Configuring a new SOAR application will automatically delete the existing configuration and replace it with a new one.
3. **"Install and run the SOAR application proxy (optional)" on page 64**: This optional step is required only in environments where there is a firewall between the SOAR application and Arcsight Investigate.

4. **"Trigger a playbook" on the next page**: Right-click an event and execute an action in the Search Grid to trigger a playbook in the integrated SOAR application.
5. **"Viewing results" on page 65**: View the results of the playbook execution on the **Notifications** page.

SOAR Configuration Parameters

Location: Configuration > SOAR Configuration

In Investigate, navigate to the **SOAR Configuration** page and set these parameters for integration.

Configuration Parameter	Description	Value Constraints
Application Name	Select from the list of supported applications. Note that only one supported SOAR application configuration can be active in ArcSight Investigate.	Required.
Hostname/IP	The hostname or IP in URL format.	Required. Must start with `http/https`, no ending '/'
Port Number	Port number of the application.	2 or more digits, no leading zeroes.
Proxy	URL of the Proxy server, if one is required.	Same as Hostname/IP
API/Application Key	The special key provided by the application to access its REST APIs. This is generated by the SOAR application using its UI. Refer to the SOAR application documentation for steps to generate the key.	
API URI	The REST end point that will be used to trigger a playbook in the SOAR application.	Required. Must start with a '/', no ending '/'
Login URI	The REST end point that will be used to login in to the SOAR application.	Same as API URI
Flow URI	The REST end point that will be used to get the flows in Operations Orchestration (OO).	Required in OO only. Same as API URI
Application Username	Username to use to login in to the SOAR application.	
Application Password	Password corresponding to the username.	

Configuration Parameter	Description	Value Constraints
Supported Actions	Comma-separated list of Actions supported by this SOAR application. These strings will appear in the right-click cell context menu on the Search Grid. These strings must exactly match the corresponding playbook triggers configured in the SOAR application.	Required.
Verify Application Certificate	Enable/Disable verification of server certificates from the SOAR application.	
Configuration Enabled/Disabled	Enable/Disable the configuration. When disabled, the Supported Actions list will not appear in the right-click cell context menu on the Search Grid.	

Install and run the SOAR application proxy (optional)

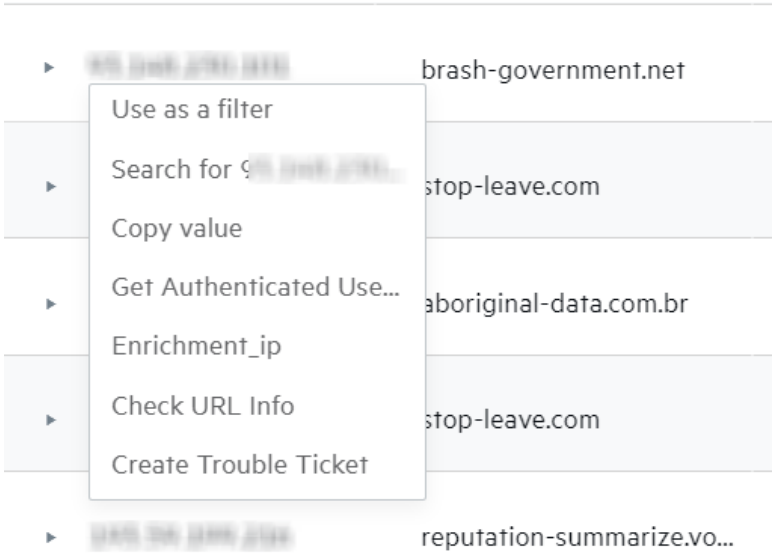
In environments with a firewall between the ArcSight Investigate and the SOAR application, a proxy provided by the corresponding SOAR application must be installed in the network that hosts Investigate. The requirements and steps for installing such a proxy are specific to the SOAR application. Refer to the SOAR application documentation for proxy setup intstruction.

Note: Investigate does not include a method for verifying connectivity to an integrated SOAR application.

Trigger a playbook

Once a SOAR application has been configured, and network requirements for the communication between the application and Investigate are met, you invoke the configured actions.

First, run a search and display the results of the search in the Search Grid. Then, right-click on a specific column of a specific event and select an action applicable to the column or event from the context menu.



In the above illustration, the user right-clicked on an IP address. The list of SOAR-related actions is displayed in the cell context menu. Select one of the actions, which will trigger a corresponding playbook in the SOAR application. You are redirected to the **SOAR Notification** page once an action is invoked.

Note: Actions configured for a SOAR application are not associated with any data type. As a result, all actions will be available for all data types, but some actions may not be applicable. For meaningful results, only right-click on actions appropriate and applicable for the column (data type).

Viewing results

SOAR actions invoked from the Search Grid will have an entry in **SOAR Notification Details** grid. Navigate to the SOAR Notification page from the **Integration** tab of the left navigation menu.

The **Status** column reflects the current status of the action as shown in the screenshot below.

- A *running* status indicates that the playbook has not yet completed execution.
- Once the playbook execution is complete, the results will be sent to Investigate and the status of the action will be marked as *done*.

The results of the action can be viewed by expanding the row in the **Notification Details** grid.

To delete an old entry from the **Notifications** grid, select the entry's checkbox and then click **Delete**.

Integrating with Demisto

Parameters required for integration with the Demisto platform are shown in the following table.

Parameter Type	Value	Description
Authentication	Application generated API Key	
Playbook Trigger	Incident Type	One Incident Type must be created for each configured Supported Action. The string must be an exact match.
API	/incident	The REST API URI used to trigger playbooks

Integrating with Operations Orchestration

Parameters required for integration with the Operations Orchestration platform are shown in the following table.

Parameter Type	Value	Description
Authentication	Userid and Password	
Flow Trigger	None	Flows are triggered by directly executing them using the API
API	/oo/rest/latest/executions	The REST API URI used to trigger flows

Integrating with Siemplify Enterprise

Parameters required for integration with the Siemplify Enterprise platform are shown in the following table.

Parameter Type	Value	Description
Authentication	Application generated API Key	
Playbook Trigger	Product Name	One Product Name must be created for each configured Supported Action. The string must be an exact match. Product Name is created when a playbook is created.
API	/api/external/v1/cases/CreateCase	The REST API URI used to trigger playbooks

Sample Python code snippet

Shown here is a snippet of Python code that shows the Investigate API and how it is used to send the results of playbook execution back to ArcSight Investigate. This code will either be part of an Integration script in the SOAR application that establishes the interface between that application and Investigate, or it may be the last step in the playbook that consolidates and sends the results to Investigate.

Note: The username and password used to invoke the REST API in the sample code are credentials to access ArcSight Investigate. This username requires Execute Search permission, so you can use a Guest account (or similar role) with Execute Search permission. Implementation details will vary, depending on which SOAR application you are integrating.

```
import requests

import os

# First remove the proxies, since this script will

# most likely execute inside the enterprise network

if 'http_proxy' in os.environ:

del os.environ['http_proxy']

if 'https_proxy' in os.environ:

del os.environ['https_proxy']

# These arguments must be passed as arguments to the script itself

# or as arguments to a method that will be invoked to send the

# results to Arcsight Investigate

host = <must be passed as argument>

protocol = <must be passed as argument>

username = <must be passed as argument>

password = <must be passed as argument>

# Action output is the info that the SOAR application wants to

# send to Arcsight Investigate. This could be the cumulative

# output of the previous steps in the playbook

actionOutput = <must be passed as argument>

##### IMPORTANT ######

# jobid is a string that will be sent by Arcsight Investigate

# in the original request that triggered the playbook. The SOAR application

# MUST send this ID back in the results for Arcsight Investigate to

# match the result with the right action.

jobid = <must be passed as argument>
```

```
if username and password:
# first login using the arcsight Investigate credentials
# to get the SESSIONTOKEN cookie
loginRes = requests.post("%s://%s/mgmt/login" % (protocol, host),
data={"username": username, "password": password},
verify=False)
# then call the API to send the results of the playbook execution
# with the SESSIONTOKEN cookie set
result = requests.put("%s://%s/api/soarAction/update/%s" % (protocol, host,
jobid),
# jobid and actionOutput are mapped as follows
# both the keys are case-sensitive
json = {"jobid": jobid, "actionOutput": actionOutput},
cookies={"SESSIONTOKEN": loginRes.cookies.get('SESSIONTOKEN') or None},
verify=False)
```

Appendix A: FAQs

Can I pin a field column in order to compare it against other field values?

Answer

In the Event table, Investigate enables you to pin a field column—to make a column horizontally stationary, in order to better compare the column values against those of other columns.

Related Topic

"Pinning field columns to help analyze events" on page 38

Can I export search-results data to an Excel file?

Answer

Yes. ArcSight Investigate enables you to output search results to any CSV file.

Related Topic

"Exporting search results" on page 40

How much search-result data can I view?

Answer

There are a possible of 176 pieces of data that can be returned from a search. This data takes the form of fields in a fieldset. The fieldset determines what search results data is available for creating data visualization charts and what data columns appear in the Events table.

To manage the display of search-result data, you can limit the number of fields in a fieldset.

Related Topic

"Editing a fieldset for search results " on page 20

Can I view the most and least common values for a search-results field?

Answer

To help you filter for data anomalies, ArcSight Investigate enables you to quickly display the most and least common values for a field. This translates into the count and percentage of hits for the value. For example, the **devicevendor** field could have a top value of "bluecoat" with a count of 3,000 hits, which is 30% of 10,000 results.

Related Topic

"Viewing the most and least common values for an event record field" on page 37

Can I use SQL to specify query input?

Answer

No. Support for SQL statements is planned for a future release.

Can I use a SIEM with ArcSight Investigate?

Answer

Currently, ArcSight Investigate only supports the ArcSight Enterprise Security Manager (ESM) SIEM. Support for other SIEMs is planned for a future release.

Related Topic

- "Features and benefits" on page 4
- "How ArcSight Investigate works" on page 1

Can I apply User Behavior Analytics to the Hadoop data lake used by ArcSight Investigate?

Answer

No. Support for HPE Security ArcSight User Behavior Analytics (UBA) and HPE Security ArcSight DNS Malware Analytics (DMA) to use the Hadoop data lake used by Investigate is planned for a future release.

Related Topic

"Features and benefits" on page 4

Appendix B: Debug Log Levels

You can set the log levels for each of Investigate micro-services: `search, search-engine`, and `user management`. Available log levels, in descending order of verbosity, are:

- error (most verbose)
- warning
- info (default value)
- debug
- trace (least verbose)

By default, log level is set to info.

To change the log level:

1. In a text editor, open the installer's product configuration file located at `/opt/arcsight/installer/arcsight-installer.properties.` The properties file will list the following log properties for Investigate, which are commen4 ted out by default:

```
## Log level for Investigate components

# search-log-level=info

# search-engine-log-level=info

# mgmt-log-level=info
```

2. Uncomment the log level property for the selected microservice and change the log level to one of the values listed above. For example, the following text would change the log level for `search` to trace.

```
## Log level for Investigate components

search-log-level=trace

# search-engine-log-level=info

# mgmt-log-level=info
```

3. Run the Update Properties script: `./update-arcsight-installer-properties.sh`
4. Redeploy the ArcSight Investigate pods in the ArcSight Installer.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on User's Guide (ArcSight Investigate 2.20)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arcsight_doc@microfocus.com.

We appreciate your feedback!

Glossary

A

Active channel
An active channel is a tool that monitors all the activity that ESM processes for your network. An active channel displays a stream of information defined by parameters set in the active channel editor. A channel could stream events, or show the status of some resources. A channel can be further fine-tuned using in-line filters. There are three types of active channels that display different types of data: - Live Channels continuously refreshed live event data - Rules Channels display replay events for testing rules - Resource Channels display the status of certain resources, such as the assets in your network model and open cases

Aggregate data
Data that refers to numerical or non-numerical information that is (1) collected from multiple sources and/or on multiple measures, variables, or individuals and (2) compiled into data summaries or summary reports, typically for the purposes of reporting or statistical analysis—for such purposes as examining trends, making comparisons, or revealing information and insights that would not be observable when data elements are viewed in isolation.

Aggregate function
In database management an aggregate function is a function where the values of multiple rows are grouped together as input on certain criteria to form a single value of more significant meaning or measurement such as a set, a bag or a list. Common aggregate functions include : Average() and Count().

Apache Avro
Avro is a remote procedure call and data serialization framework developed within Apache's Hadoop project. It uses JSON for defining data types and protocols, and serializes data in a compact binary format. Its primary use is in Apache Hadoop, where it can provide both a serialization format for persistent data, and a wire format for communication between Hadoop nodes, and from client programs to the Hadoop services.

Apache Kafka
Apache Kafka is an open-source stream processing platform. Kafka is a distributed publish-subscribe messaging system that is designed to be fast, scalable, and durable. Like many publish-subscribe messaging systems, Kafka maintains feeds of messages in topics. Producers write data to topics and consumers read from topics. Since Kafka is a distributed system, topics are partitioned and replicated across multiple nodes.

Apache Kafka broker
Each node in an Apache Kafka cluster is called a Kafka broker.

Apache Kafka topic
The container with which messages are associated. A consumer of topics pulls messages off of a Kafka topic while producers push messages into a Kafka topic.

ArcSight Command Center (ACC)
The ArcSight Command Center is a web-based user interface that enables you to perform many of the functions found in the ArcSight Console. ArcSight Command Center provides dashboards, several kinds of searches, reports, case management, notifications, and administrative functions for managing active channels, content, users, connectors, storage, archives, search filters, saved searches, peer configuration, and system logs.

ArcSight Enterprise Security Manager (ESM)
A comprehensive software solution—a SIEM that combines traditional security event monitoring with network intelligence, context correlation, anomaly detection, historical analysis tools, and automated remediation. It consolidates and normalizes data from disparate devices across your enterprise network in a centralized view.

ArcSight Event Broker
Event Broker centralizes event processing, helps you to scale your ArcSight environment, and opens up ArcSight events to ArcSight Investigate. It enables you to take advantage of scalable, high-throughput, multi-broker clusters for publishing and subscribing to event data.

ArcSight Logger
Logger is a log management solution that is optimized for extremely high event throughput, efficient long-term storage, and rapid data analysis. Logger receives and stores events; supports search, retrieval, and reporting; and can optionally forward selected events. Logger compresses raw data, but can always retrieve unmodified data on demand for forensics-quality litigation data.

ArcSight SmartConnector
The interface to the objects on your network that generate correlation-relevant event data. After collecting event data for ArcSight Investigate, the connectors normalize the data in two ways: normalizing values (such as severity, priority, and time zone) into a common format, and normalizing the data structure into a common schema. SmartConnectors can then filter and aggregate events to reduce the volume of events sent to the ArcSight Manager. See SmartConnector documentation for complete details.

Area chart
An area chart or area graph displays graphically quantitative data. It is based on the line chart. The area between the axis and line are commonly emphasized with colors, textures and hatchings. Commonly, one compares with an area chart two or more quantities.

B

Bar chart
A bar chart or bar graph is a chart or graph that presents grouped data with rectangular bars with lengths proportional to the values that they represent. The bars can be plotted vertically or horizontally. A vertical bar chart is sometimes called a Line graph.

C

CEF
Common Event Format (CEF) is an extensible, text-based, high-performance format designed to support multiple device types in the simplest manner possible. Various message syntaxes are reduced to one-matching ArcSight

Enterprise Security Manager (ESM) normalization. Specifically, CEF defines a syntax for log records comprised of a standard header and a variable extension, formatted as key-value pairs. This format contains the most relevant event information, making it easy for event consumers to parse and use them. Other standards target a single component of the security infrastructure or are designed for specific applications. These alternatives lack the ability to support today's high-performance, real-time security requirements. For Investigate, there is CEF to Avro conversion for CEF versions 0.1 and 1.0.

CIDR notation

Classless Inter-Domain Routing (CIDR) encompasses several concepts. It is based on the variable-length subnet masking (VLSM) technique allows the specification of arbitrary-length prefixes. CIDR introduced a new method of representation for IP addresses, now commonly known as CIDR notation, in which an address or routing prefix is written with a suffix indicating the number of bits of the prefix, such as 192.168.2.0/24 for IPv4, and 2001:db8::/32 for IPv6. CIDR introduced an administrative process of allocating address blocks to organizations based on their actual and short-term projected needs.

CLI

A command-line user interface (CLI), also known as a console user interface, and character user interface (CUI), is a means of interacting with a computer program where the user (or client) issues commands to the program in the form of successive lines of text (command lines). A program which handles the interface is called a command language interpreter or shell.

Cold data

Data that is accessed less frequently by an organization. Cold data is usually stored on lower performing and less expensive storage environments in-house or in the cloud.

Column chart

A column chart is a graphic representation of data. Column charts display vertical bars going across the chart horizontally, with the values axis being displayed on the left side of the chart.

Connector

An integration element to a certain software, device format, appliance, or function through use of the product. An Onboard Connector means software that resides on the HPE ArcSight appliance that communicates with other software data center. A Remote Connector is software that resides on a different computer that communicates with the HPE ArcSight appliance.

Containers as a Service (CaaS)

To deliver the consistent experience for developers and IT ops, teams began using Docker for Containers as a Service (CaaS). Containers as a Service is a model where IT organizations and developers can work together to build, ship and run their applications anywhere. CaaS enables an IT secured and managed application environment consisting of content and infrastructure, from which developers are able build and deploy applications in a self service manner.

Contextual search

A form of optimizing search results based on context provided to Investigate to execute the query. For example, Investigate knows what operators to provide in the search if an IP address is specified. Likewise, if an operator is specified in the search, Investigate knows what other related operators to provide. When entering query input, Investigate can suggest fields, operators, and searches. The technology understands basic search keywords based on security terminology, database content, and user history. The search is based on such criteria as time, IPs,

domains, device vendors, ports, protocols, EventCategory, and usernames. Example: Source Address = 192.10.11.12 and Destination Address less than 192.10.11.12 Investigate suggested the search items and operators.

Continuous data
Data that is not restricted to a specific value, but can occupy any value over a continuous range.

Cron job
The cron utility is a time-based job scheduler in Unix-like computer operating systems. Administrators who set up and maintain software environments use cron to schedule jobs (commands or shell scripts) to run periodically at fixed times, dates, or intervals. It typically automates system maintenance or administration—though its general-purpose nature makes it useful for things like downloading files from the Internet and downloading email at regular intervals. The origin of the name cron is from the Greek word for time, chronos.

CSV
In computing, a comma-separated values (CSV) file stores tabular data (numbers and text) in plain text. Each line of the file is a data record. Each record consists of one or more fields, separated by commas. The use of the comma as a field separator is the source of the name for this file format.

D

Data lake
A storage repository that holds a vast amount of raw data in its native format until it is needed. While a hierarchical data warehouse stores data in files or folders, a data lake uses a flat architecture to store data.

Data visualization
Data visualization is the graphical display of abstract information for two purposes: (1) Sense-making (also called data analysis) and (2) communication. Important stories live in data and data visualization is a powerful means to discover and understand these stories, and then to present them to others.

Dataset
A collection of related sets of information that is composed of separate elements but can be manipulated as a unit by a computer.

Discrete data
Data that can be numeric, such as the number of apples. It can also be categorical, like red or blue, or male or female, or good or bad.

Docker
Docker containers wrap a piece of software in a complete filesystem that contains everything needed to run: code, runtime, system tools, system libraries – anything that can be installed on a server. This guarantees that the software will always run the same, regardless of its environment. The Docker platform leverages Docker containers to enable IT operations teams and Developer teams to build, ship and run any application, anywhere. Docker containers are based on open standards, enabling containers to run on all major Linux distributions and on Microsoft Windows -- and on top of any infrastructure. Docker creates a common framework for developers and sysadmins to work together on distributed applications.

F

Fieldset
A select group of fields that determine the field information that displays in the search results for each event that matched the search query. Investigate provides a predefined, default fieldset.

Full-text search
Searches on all the tables. If you enter a string you don't know about you just search the entire columns in all the tables.

H

Hadoop
Apache Hadoop is an open source software platform for distributed storage and distributed processing of very large data sets on computer clusters built from commodity hardware. Hadoop services provide for data storage, data processing, data access, data governance, security, and operations.

Hadoop cluster
A special type of computational cluster designed specifically for storing and analyzing huge amounts of unstructured data in a distributed computing environment.

Hadoop data lake
A data management platform comprising of one or more Hadoop clusters used principally to process and store non-relational data such as log files , Internet clickstream records, sensor data, JSON objects, images and social media posts.

HDFS
The core of Apache Hadoop consists of a storage part, known as Hadoop Distributed File System (HDFS), and a processing part which is a map-reduce programming model. Hadoop splits files into large blocks and distributes them across nodes in a cluster.

Hot data
Data that needs to be accessed frequently. It is typically business-critical information that needs to be accessed quickly and is often used by a company for quick decision making. Hot data usually resides on the fastest storage -- typically flash in hybrid or tiered storage environments.

HPE Security ArcSight DNS Malware Analytics (DMA)
DMA is a scalable, cloud-based threat detector that monitors DNS traffic and rapidly identifies an infected system, enabling immediate remediation in real time. The application can function in a stand-alone configuration as well as in a Security Operations Center (SOC), using HPE - Security ArcSight Enterprise Security Manager (ESM) as the Security Information and Event Management (SIEM) tool.

HPE Security ArcSight User Behavior Analytics (UBA)
HPE Security ArcSight User Behavior Analytics (UBA) enables security analysts to minimize the risk and impact of cyberattacks in real time. Instead of solely focusing on events and log data, HPE ArcSight UBA detects unknown threats through purpose-built security analytics by creating a baseline of normal user and entity behavior and

identifying anomalies associated with users and entities as they occur. By aggregating activities and multiple indicators of compromise for users, entities, and their peer groups, HPE ArcSight UBA delivers insight into the highest risk users and entities—even when credentials are legitimate.

HPE Vertica
An advanced SQL database that can address the most demanding Big Data analytics initiatives. It introduces a unified architecture and advanced in-database analytics capabilities that enable users to conduct sophisticated analysis at industry-leading scale and speed, regardless of where their data resides.

I

Integration commands
Integration commands are a set of tools in the ESM Console that make it possible to invoke scripts and utilities from several places in the ArcSight Console, and to provide snap-in views of other applications, such as ArcSight Logger and third-party applications, within the ArcSight Console. This enables you to use the ArcSight Console as a central command hub for all security-related operations. Once integrated, the commands, tools, and applications can be launched on demand from within the Console, such as from a right-click context menu within an events grid.

IoT
The Internet of things (IoT) is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items—embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data.

K

Key field
A field in a record that holds unique data which identifies that record from all the other records in the file or database. Account number, product code, and customer name are typical key fields. As an identifier, each key value must be unique in each record.

Kubernetes
Commonly referred to as "K8s", this is an open-source container cluster manager originally designed by Google and donated to the Cloud Native Computing Foundation. It aims to provide a "platform for automating deployment, scaling, and operations of application containers across clusters of hosts". It usually works with the Docker container tool and coordinates between a wide cluster of hosts running Docker.

L

Line chart
A line chart or line graph is a type of chart which displays information as a series of data points called 'markers' connected by straight line segments. It is a basic type of chart common in many fields.

Lookup list
A CSV table.

M

MAC address
A media access control address (MAC address) of a device is a unique identifier assigned to network interfaces for communications at the data link layer of a network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet and Wi-Fi.

Microservices
Microservices is a specialisation of and implementation approach for service-oriented architectures (SOA) used to build flexible, independently deployable software systems. As with SOA, services in a microservice architecture (MSA) are processes that communicate with each other over a network in order to fulfill a goal. Also, like SOA, these services use technology-agnostic protocols. The microservices approach is a first realization of SOA that followed the introduction of DevOps and is becoming more popular for building continuously deployed systems. In a microservices architecture, services should have a small granularity and the protocols should be lightweight. A central microservices property that appears in multiple definitions is that services should be independently deployable. The benefit of distributing different responsibilities of the system into different smaller services is that it enhances the cohesion and decreases the coupling. This makes it easier to change and add functions and qualities to the system at any time. It also allows the architecture of an individual service to emerge through continuous refactoring, and hence reduces the need for a big up-front design and allows for releasing software early and continuously.

N

Natural-language search
A set of pre-defined operators. Complex search: Two or more terms Separation operators: 1. And 2. Not 3. = 4. OR 5. Connecting to 6. Equals 7. List (src =1.1.1.1, 1.2.4.5) This is an OR. Example: src = 1.1.1.1 or src = 1.2.4.5

NOC
Network Operations Centers (NOCs) are implemented by business organizations, public utilities, universities, and government agencies that oversee complex networking environments that require high availability. NOC personnel are responsible for monitoring one or many networks for certain conditions that may require special attention to avoid degraded service. Organizations may operate more than one NOC, either to manage different networks or to provide geographic redundancy in the event of one site becoming unavailable. In addition to monitoring internal and external networks of related infrastructure, NOCs can monitor social networks to get a head-start on disruptive events.

O

OT
Operational Technology (OT) is hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise.

P

Pie chart
A type of graph in which a circle is divided into sectors that each represent a proportion of the whole. A pie chart can be used to show percentages of a whole, and represent percentages at a set point in time.

R

REST
REST (REpresentational State Transfer) is an architectural style, and an approach to communications that is often used in the development of Web services. The REST architectural style describes six constraints: - Uniform Interface - Stateless - Cacheable - Client-Server - Layered System - Code on Demand (optional)

ROS
The Read Optimized Store (ROS) is a highly optimized, read-oriented, disk storage structure, organized by projection. The ROS makes heavy use of compression and indexing. You can use the COPY statement DIRECT and INSERT parameters (with /*+direct*/ hint) to load data directly into the ROS. Note: HPE Vertica allows optional spaces before and after the plus sign in direct hints (between the /* and the +).

RSS
RSS (Rich Site Summary; originally RDF Site Summary; often called Really Simple Syndication) uses a family of standard web feed formats to publish frequently updated information: blog entries, news headlines, audio, video.

Runbook
In a computer system or network, a runbook is a routine compilation of procedures and operations that the system administrator or operator carries out. System administrators in IT departments and NOCs use runbooks as a reference. Runbooks can be in either electronic or in physical book form.

S

Scatter plot chart
A scatter plot (also called a scatter graph, scatter chart, scattergram, or scatter diagram) is a type of plot or mathematical diagram using Cartesian coordinates to display values for typically two variables for a set of data. If the points are color-coded, one additional variable can be displayed.

Security analyst
The primary user of ArcSight Investigate. This user relies on the overall ArcSight log collection and search capabilities for successfully triaging security incidents. Ultimately, security analysts want to get actionable insights from a search.

Security architect
This user is responsible for determining the overall ArcSight deployment and how this product fits into the SIEM architecture of the organization. This includes integration with other systems such as Hadoop which may be used for storing additional log data.

Security engineer
This user is responsible for data sources and determining how security analysts can effectively triage security incidents and security threat.

Security posture
Your overall security plan – the approach your organization takes to security, from planning to implementation. It is comprised of technical and non-technical policies, procedures and controls, that protect you from both internal and external threats.

SIEM
In the field of computer security, Security Information and Event Management (SIEM) software products and services combine Security Information Management (SIM) and Security Event Management (SEM). They provide real-time analysis of security alerts generated by network hardware and applications. HPE Security ArcSight Enterprise Security Manager (ESM) is an example of a SIEM product.

SMTP
SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail.

SOC
An information security operations center ("ISOC" or "SOC") is a facility where enterprise information systems (websites, applications, databases, data centers and servers, networks, desktops and other endpoints) are monitored, assessed, and defended.

Sparkline
A small graphic designed to give a quick representation of numerical or statistical information within a piece of text, taking the form of a graph without axes.

Subnet
A logical subdivision of an IP network. Computers that belong to a subnet are addressed with a common, identical, most-significant bit-group in their IP address. This results in the logical division of an IP address into two fields, a network or routing prefix and the "rest" field or host identifier. The rest field is an identifier for a specific host or network interface.

System admin
This user is responsible for the deployment, administration and day to day operations of the product. They will need the necessary monitoring and administrative controls to ensure that the product is available and functioning with optimal performance for security analysts.

T

Text box widget
From the Dashboard, you can use this widget to create, edit, and delete a text note.

TLS
Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), both frequently referred to as "SSL", are cryptographic protocols that provide communications security over a computer network. In the case of

ArcSight Investigate, TLS is used between the user management, search interface, search engine, and Vertica database modules.

Truncate table
This removes all rows from a table, but the table structure and its columns, constraints, indexes, and alike remain.

Tuple
A tuple is a sequence of immutable Python objects. Tuples are sequences, just like lists. The differences between tuples and lists are, the tuples cannot be changed unlike lists and tuples use parentheses, whereas lists use square brackets. Creating a tuple is as simple as putting different comma-separated values.

V

Vertica
At its core, the HPE Vertica Analytics Platform from Hewlett Packard Enterprise is a column-oriented, relational database system built specifically to handle modern analytic workloads. The platform uses a clustered approach to storing big data, offering high-performance query and analytics functionality.

Z

ZooKeeper
Apache ZooKeeper is a distributed hierarchical key-value store, which is used to provide a distributed configuration service, synchronization service, and naming registry for large distributed systems. ZooKeeper was originally a sub-project of Hadoop. ZooKeeper's architecture supports high availability through redundant services. The clients can thus ask another ZooKeeper leader if the first fails to answer. ZooKeeper nodes store their data in a hierarchical name space, much like a file system or a tree data structure. Clients can read from and write to the nodes and in this way have a shared configuration service. Updates are ordered.