Mandiant

GOOGLE BIGQUERY

This document applies to Classic/Legacy Integrations. You may continue to use these integration configurations. While no active development is happening for these integrations, we continue to provide Classic/Legacy Integrations in the product. You do not have to move to MSI Integrations. If your support engineer or TSC recommends or you choose to move to MSI Integrations, you can take advantage of the latest features and functionality. For more information, see the MSI Integration documentation in the **Integrations Overview** **(https://docs.mandiant.com/home/msv-integrations-overview)**.

This integration is not remote capable.

Update Google BigQuery

Identify or create the service account credentials to access BigQuery.

- BigQuery does not support API keys, you must use a service account.
- Authentication requires the json file for the service account for the BigQuery project.

The service account created must have a minimum of **Data Viewer role** **(https://cloud.google.com/bigquery/docs/access-control#bigquery.dataViewer)** permissions in order to complete the API call.

Update the Validation Platform

Prerequisites

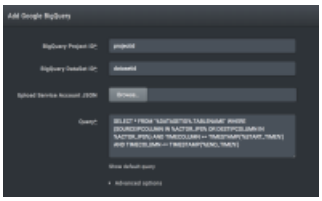
Information to gather before you start:

1. Identify the BigQuery project ID.
2. Identify the BigQuery data set ID.
3. Identify the table and schema used in the data set.
4. Identify the json file for the service account authentication.
5. Identify the field name mappings for the following:
    - Source IP
    - Destination IP
    - Source Port
    - Destination Port
    - Event Start Time (timestamp)
    - Event Unique ID
    - Event Signature ID
    - Event Description

Configuration

TO ADD THE GOOGLE BIGQUERY INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Google BigQuery**.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12dbc9cba0017c2f7e01/n/google-bigquery.png)

Google BigQuery Integration

3. Enter the **Project ID**, **DataSet ID**, and upload the json file for the service account.
4. Modify the **Query** with the appropriate columns for the table's schema.

   Do not change the words inside the percent (%) symbols

5. Expand **Advanced options**.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12dcc9cba0017c2f7e07/n/google-bigquery-adv.png)

Google BigQuery Integration (Advanced Options)

6. (Optional) Update **Query time** and **Delay time**.

   The **Query time** is the amount of time (minutes) before and after the query runs that the looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the query after a Job Action. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

   If your monitors are set to run more frequently than the query time, it will impact the pass/fail results for AEDA monitors.

7. (Optional) Select **Enable query for Malicious DNS Actions** and configure the **Query**. This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.
8. (Optional) Select **Enable query for Email Actions** and configure the **Query**. This query will be only be used when you run Email Actions.
9. Review the field name mappings and update as necessary.
   a. The field should only contain the name of the column in your table schema that maps to the given field name.
   b. Example: `Source IP: source_ip`
10. (Optional) Select **Discover network devices automatically**.

If this is not selected, new events processed by the integration will not have discovered or related network or endpoint security technologies.

11. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
12. (Optional) Assign a **Name**.
13. (Optional) Choose **Yes** to save suspicious events.
14. Click **Submit**.

Verify connectivity

TO VERIFY CONNECTIVITY TO GOOGLE BIGQUERY

Click **Test** to verify that:

- The Director can communicate with Google BigQuery, and the Project ID and DataSet ID are correct.
- The service account credentials provided can perform queries on the project, dataset, and table.

Run a Malicious or Captive DNS Action and then review the last run query to verify:

- The custom DNS query works as expected (if configured).