Mandiant

GOOGLE CHRONICLE INTEGRATION WITH SECURITY VALIDATION

This integration provides the following benefits:

- Validates that security tools are writing log events to Google Chronicle to ensure compliance with security policies and regulations
- Collects events generated by security tools that write to Google Chronicle to test the efficacy and configuration of security controls using Security Validation jobs

API calls

API	Usage
`/v1alpha/{instance}/legacy:legacyFetchUdmSearchView`	UDM search that returns matching events and alerting detections from Google Chronicle

Supported versions

Google Chronicle v1alpha

Before you begin

To configure this integration, you will need to provide the Auth Scopes when initializing your API client. Use the following scopes to initialize your Google API client:

```
https://www.googleapis.com/auth/cloud-platform
```

You may choose one of the following two authentication methods:

- **Direct service account authentication**
- **Service account impersonation**

Direct service account authentication

You will need a Google Developer Cloud Service Account JSON key file. The service account must have the necessary permissions for the Chronicle APIs. This will be provided to you by your Google Security Operations representative.

Service account impersonation

Service account impersonation is the recommended way of integrating with Google Cloud, which allows one identity to assume the permissions of another service account without using its credentials.

For that, instead of giving permissions to the service account, a source service account is created which impersonates an existing IAM.

1. Log into the Google Cloud Console
2. Navigate to the IAM & Admin section, then navigate to Service Accounts.
3. Click **Create Service Account**, fill in the form and grant the `Service Account Token Creator` role.
4. Generate the JSON keys that will be used for authenticating

After these steps, you can add an existing target account for accessing the service.

Authorization scopes

Requires the **cloud-platform** **(https://www.googleapis.com/auth/cloud-platform)** OAuth scope.

IAM Permissions

Requires the following IAM permission on the instance resource:

`chronicle.legacies.legacyFetchUdmSearchView`

Configure Security Validation

1. Go to **Settings > Integrations**.
2. From the Integrations table, click **Add Integration > Google Chronicle**.

   You can add this as either a Direct or Remote Integration.
3. Enter a meaningful **Integration Name**.
4. Optional: From the **Proxy** drop-down, choose a proxy profile if one is available. If one isn't available and all outbound connections go through a proxy, first, set up a **Proxy Rule** (https://docs.mandiant.com/home/msv-proxy-rules).
5. Optional: Change the **HttpProtocols** value to determine what protocol is used for requests (**Http** or **Https**).
6. Enter the **Host** value for the Google Chronicle Backstory instance as a hostname or IP address. The default is **chronicle.us.rep.googleapis.com**.
7. Enter a **Port** value. The default is **443**.
8. For the **Project Id**, enter the unique identifier for your Google Cloud project.
9. For the **Location**, enter the geographical region in Google Cloud where your Chronicle instance is located (for example, **us-central1** or **europe-west1**).
10. For the **Instance Id**, enter the specific identifier for your Chronicle instance.
11. Enter the **Service Account Info**, which is the contents of the Google Developer Service Account Credential and API Scope JSON file. The value for this field must be valid JSON.

    Alternatively, you can click **Browse** and select the JSON file.
12. Enter the **Impersonated Service Account Email**, which is the email of the Service Account that has the correct permissions to access the service.
13. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The default is **30** seconds.
14. Optional: Add or remove **Queries**, as needed. Default values are provided for **IP Query**, **Hostname Query**, **Domain Query**, and **Email Query**.
15. Optional: Change the **Max Results** value, if needed. This value is the maximum number of results that are returned for each query. The default is **1000**.
16. Optional: Modify the **Field Map** values, as necessary.

    - Each field map box can hold a JSON-formatted comma-separated list of columns returned by the API to be considered for each field when translating into the normalized event object format. Example: description could be configured to be 'msg_s' or 'SyslogMessage' in some environments. The field map tries both if set to: ['msg_s','SyslogMessage'] and whichever matches first is the column that is used.
    - When configuring an integration in Security Validation, you can assign additional host values in the Field Map settings. If none of the assigned fields return a valid host name, Network Actions may miss matched events from the third-party technology. Additional hosts values helps ensure the likelihood of a match between the two environments.
17. Optional: If necessary, configure **Alert Fields Map** values.
18. Optional: Expand **Advanced options** and update the information as necessary.
    a. Update **Query Time** and **Delay Time**.

> The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. 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, this configuration impacts the pass/fail results for AEDA monitors.

b. Update **Query Interval** (seconds).
c. If supported by your integration, configure correlation queries:
    i. Select **Correlation Query Enabled** and fill in the **Correlation Query**.
    ii. Modify the **Correlation Query Interval**, if necessary (minutes).
d. Select **Discover network devices automatically**, the default and recommended option.

> If unselected, reported events won't include product information for any matching network security technology.

e. Select **Save Suspicious Events**.
f. Modify the **Event Time Adjustment** (seconds). The default is **0**.
g. Modify the **Limit** value if you need to prevent a flood of results. This value is set to **10000** by default. This limit applies to both events and alerts individually, so if you set it to **10**, you can still see a maximum of 10 events and 10 alerts.

19. Click **Save**.

Verify connectivity

1. Go to **Settings > Integrations**.
2. From the Direct Integrations table, click ⋮ **> Test** to verify that:
    - The Director can communicate with the integration host on the port and protocol specified.
    - The integration credentials are valid and working.

For more information on setting up queries, see **Manage Integrations** (https://docs.mandiant.com/home/msv-managing-integrations).