Mandiant

LOGRHYTHM CLOUD INTEGRATION WITH SECURITY VALIDATION

This integration provides the following benefits:

- Validate that security tools are writing log events to LogRhythm Cloud to ensure compliance with security policies and regulations
- Collect events generated by security tools that write to LogRhythm Cloud to test the efficacy and configuration of security controls using Security Validation jobs

API Calls

API	Usage
`/lr-alarm-api/alarms`	Retrieve a list of alarms from LogRhythm Cloud
`/lr-alarm-api/alarms/{alarmId}/events`	Retrieve the events from an alarm

Supported Versions

- LogRhythm Cloud Rest API 7.7+

Preparation

To configure this integration, you need to register the application.

1. Log in to the Client Console as a Global Administrator.
2. On the main toolbar, click **Deployment Manager**.
3. Click the **Third Party Applications** tab.
4. Right-click the blank area of the grid, and then click **New**. The Third Party Application Properties dialog box appears.
5. Type an Application Name and Description. The Application Name must be unique.
6. Click **OK**. The application is saved.
7. Right-click the newly created application, and then click **Properties**.
8. Optional: Change the number of days you want the token to be valid.
9. Click **Generate Token**. The Credentials dialog box appears.
10. Enter the password for the user, and then click **OK**. A Client ID, Client Secret, and token are generated for the application.
11. Copy the token and use it to configure the integration.

You will not be able to get back to this screen to copy the token. It appears only one time and, for security purposes, is not stored. If you do not copy and save the token, you will have to regenerate it later.

Configure Security Validation

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

   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 (**Https** or **Http**).
6. Enter the **Host** value (hostname or IP address) for the LogRhythm Cloud instance. The default is **httpbin.org**.

7. Enter a **Port** value. The default is **443.**
8. Enter the **API Token** value that you generated.
9. Optional: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
10. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The default is **30** (seconds).
11. 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.

12. Optional: Modify the **Page Size** to change the request for the upstream server. The default is **500**.
13. Optional: Modify the **Max Pages** value, which is the maximum number of API pages to query for events. The default is **5**.
14. 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. Select **Correlation Query Enabled** and fill in the **Correlation Query**.
    d. Modify the **Correlation Query Interval**, if necessary (minutes).
    e. 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.

    f. Select **Save Suspicious Events**.
    g. Modify the **Event Time Adjustment** (seconds). The default is **0**.
    h. 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.

15. 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)**.