Mandiant

BETTER STACK LOGS INTEGRATION WITH SECURITY VALIDATION

This integration provides the following benefits:

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

API Calls

API	Usage
`https://in.logs.betterstack.com`	Used to test REST API connectivity and authentication settings
`https://logs.betterstack.com/api/v1/query`	Query for events in Better Stack Logs

Supported Versions

Better Stack Logs API v1

Before You Begin

To configure this integration:

1. Create a free-tier account in Better Stack Logs using the URL **https://uptime.betterstack.com/users/sign-up**.
2. Create a **Direct API token** within the **Configure team** tab under **Team members**.
3. Use the **Direct API token** for Authorization as **Bearer $TEAM_TOKEN**; also, you can use a team member's **Direct API token**.
4. To generate the logs, use the **Live tail** tab.
5. If no data shows, select **Presets** data to kick off the Live tail logs.
6. You can see the Live tail logs in the terminal also using cmd `curl https://logs.betterstack.com/<DATA_LOGS_NAME>/<SOURCE_TOKEN> | bash` from **Sources** tab and then edit the sample realtime data logs.
7. After getting Live tail data in the terminal, stop the live data logs using `CTRL + C` or `CMD + C` and you can test the data in msi-thunder or Postman.
8. When sending the payload, Better Stack Logs accepts a range of 50-1000. Default: 100 rows in **runtime_config** for the **page_size** attribute.

Configure Security Validation

1. Go to **Settings > Integrations**.
2. From the Integrations table, click **Add Integration > Better Stack Logs V1**.

   

   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** for the Better Stack Logs instance. The default is **logs.betterstack.com**.
7. Enter a **Port** value. The default is **443.**
8. Optional: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
9. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The

default is **30** (seconds).

10. Enter the **Bearer Team Token** value that you generated.
11. Optional: Modify **Queries**, as needed. Defaults are provided for **Hostname Query**, **IP Query**, **DNS Query**, and **Email Query**.
12. Optional: Modify the **Page Size** to change the request for the upstream server. The default is **500**.
13. 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.

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)**.