ZEROFOX®

ZeroFOX Integrations

Sumo Logic Logging, Analytics and Dashboard

Last Updated: June 24, 2020

Integration Description

Software solutions with out-of-the-box integration seamlessly syncs data, and reduces the need for rekeying and multi-system management. With Sumo Logic, users can pull information from several different operational or security platforms into one consolidated dashboard for customized insights at-a-glance. Integrate ZeroFOX alert data directly into Sumo Logic to leverage a full suite of logging, analytics and dashboards.

The ZeroFOX Sumo Logic integration comes with a great set of pre-built queries and dashboards. This pre-built integration can be set up in minutes to provide an automated, continual stream of alert data into Sumo Logic. Once the integration is complete, Sumo Logic users can utilize the default dashboard and queries or create their own custom dashboards.

Log Types

The ZeroFOX Cloud App uses JSON-formatted alert data that can be integrated directly into your Sumo Logic instance. For more information on the specific alert format, see ZeroFOX Alert documentation at https://api.zerofox.com/1.0/docs/.

Collect Logs From the ZeroFOX Cloud

This page provides instructions for adding a setting up webhook events in ZeroFOX and an HTTP source in Sumo Logic. The specific steps to be addressed are as follows:

Collection Process Overview

Step 1: Set up an HTTP Source for ZeroFOX Cloud
Step 2: Get Your ZeroFOX API Key
Step 3: Enable Webhooks from ZeroFOX Cloud
Step 4: Verify ZeroFOX Alert Log Collection

Collection Process Overview

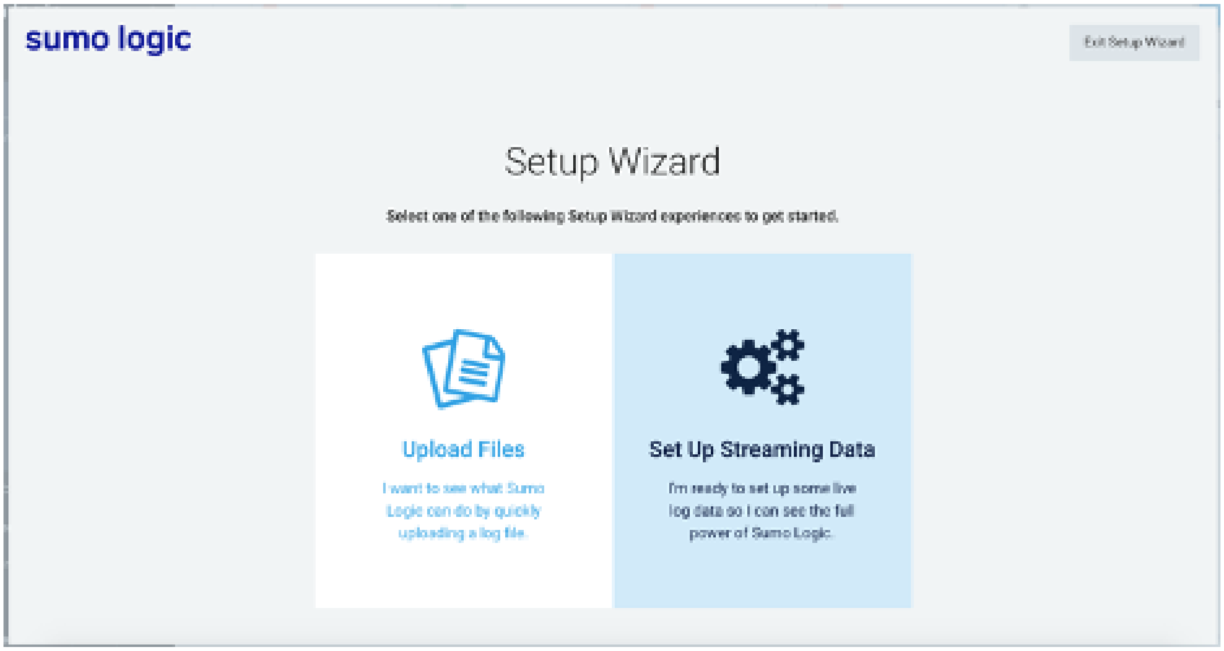
ZeroFOX Alerts are delivered to Sumo Logic via webhook from ZeroFOX to Sumo Logic. No custom installation is required; however, the Sumo Logic user must set up a HTTP Source and provide the ***Sumo Logic URL*** and their ***ZeroFOX API key*** to initiate content forwarding from

ZeroFOX to Sumo Logic. This can be done by sending an email request to product@zerofox.com.

For an in-depth explanation of ZeroFOX alert format, please visit our API documentation at https://api.zerofox.com/1.0/docs.

Collection Step 1: Set up an HTTP Source for ZeroFOX Cloud

From the *Manage Data* page in Sumo Logic, open the Setup Wizard and select *Set Up Streaming Data*.



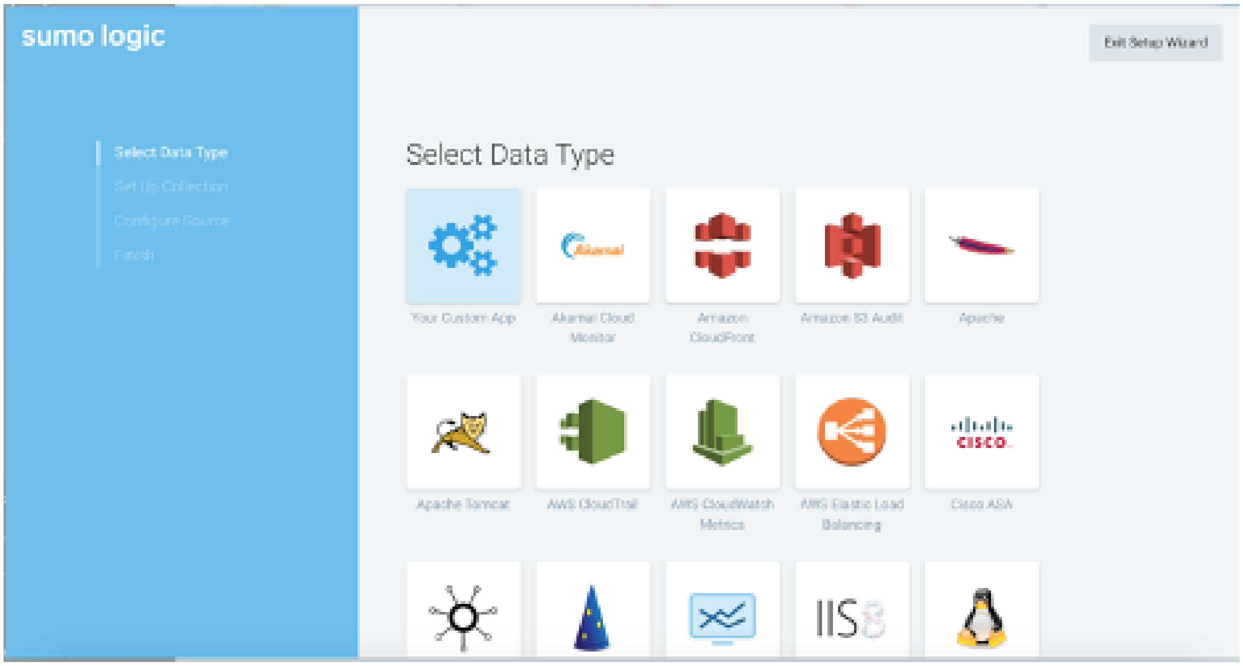
Setup Wizard

Select one of the following Setup Wizard experiences to get started.

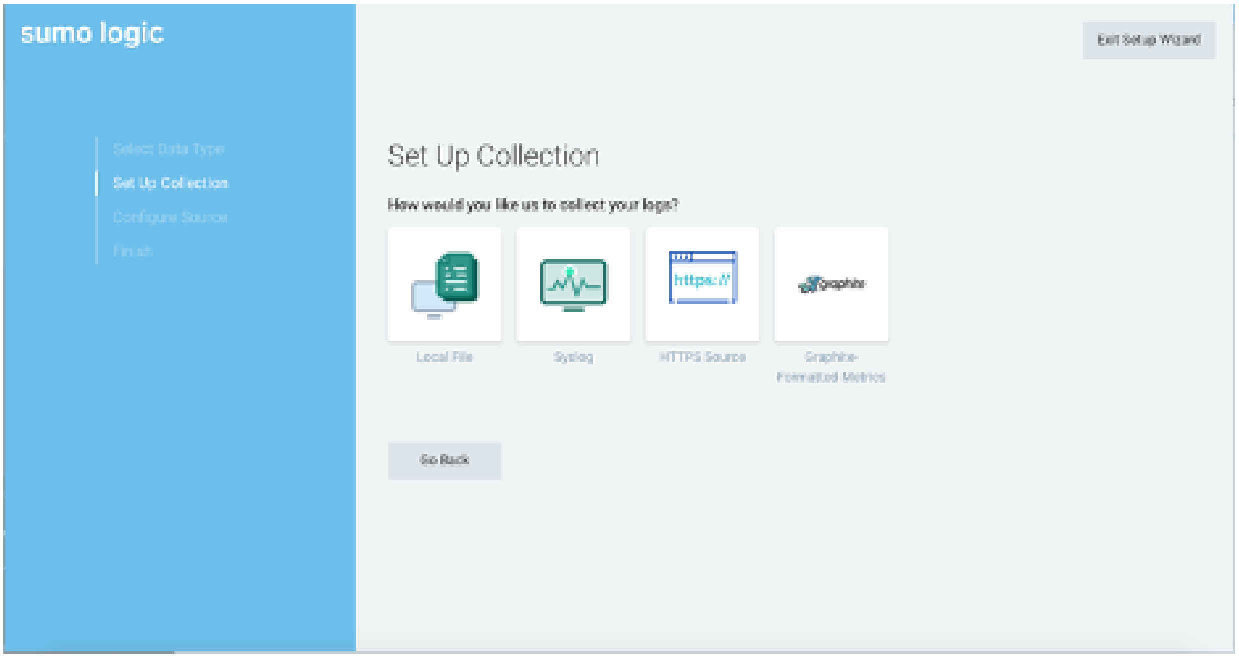
I want to see what Sumo Logic can do by quickly uploading a log file.

I'm ready to set up some live log data so I can see the full power of Sumo Logic.

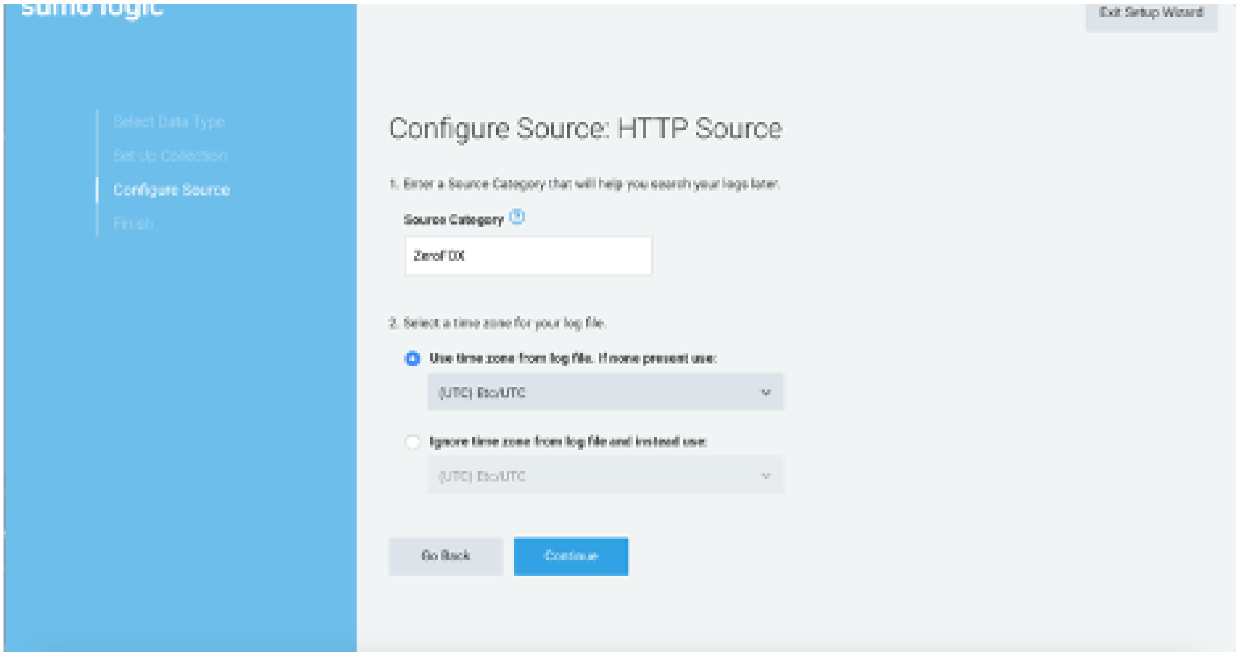
Select *Your Custom App* as the data type on the following screen.



Next, select *HTTP Source* as your collector.



Configure your HTTP Source to use ***ZeroFOX*** as the Source Category. You can either use the time zone from the log file or specify your own time zone. After doing so, click *Continue*.



Configure Source: HTTP Source

1. Enter a Source Category that will help you search your logs later.

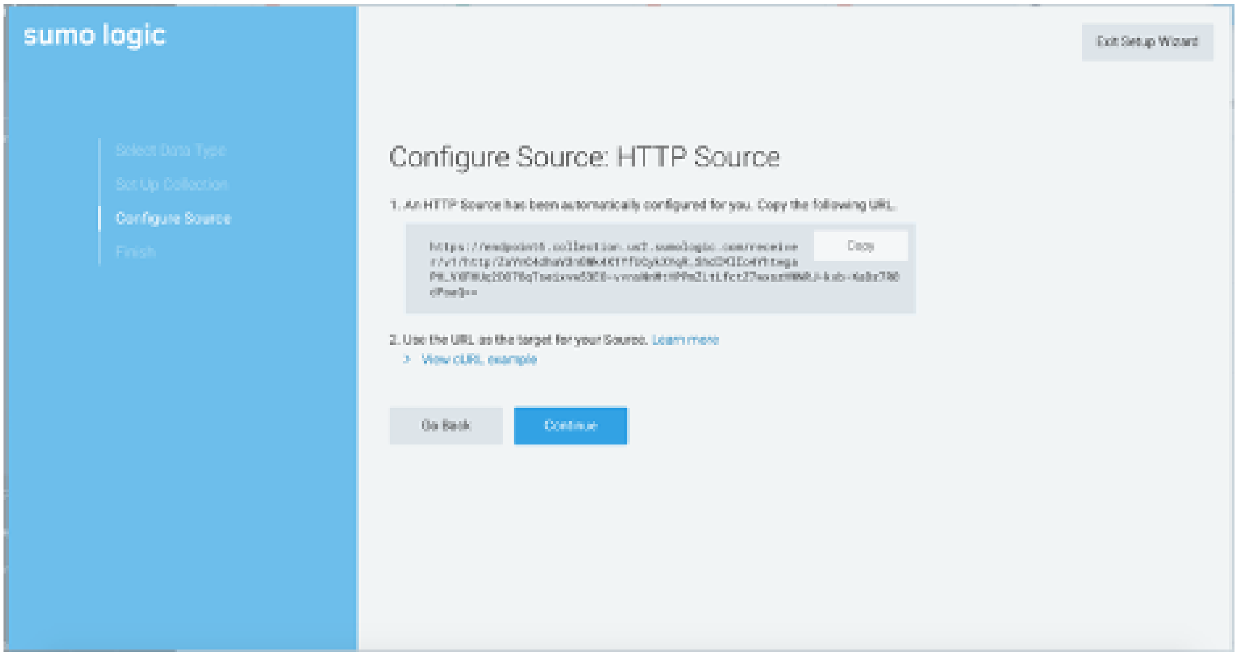
Source Category: ZeroFOX

2. Select a time zone for your log file.

● Use time zone from log file. If none present use: (UTC) Etc/UTC

○ Ignore time zone from log file and instead use: (UTC) Etc/UTC

Please copy and save the HTTP Source URL that appears on the following page. This will be necessary when configuring ZeroFOX Cloud webhooks. After copying the URL click *Continue*.



Configure Source: HTTP Source

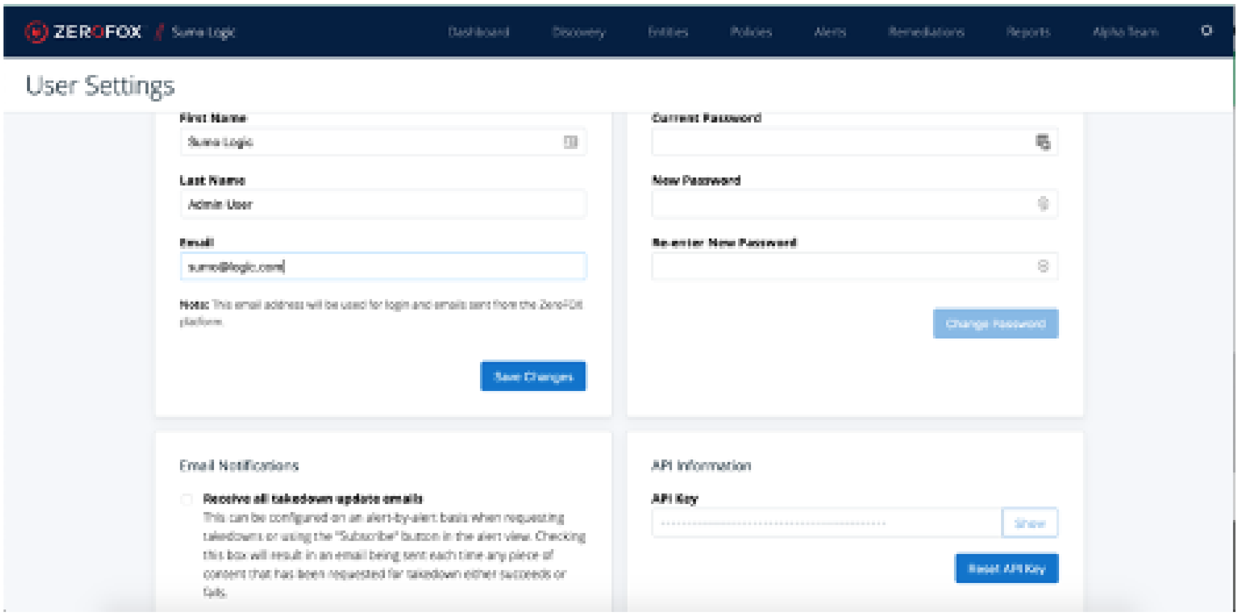
1. An HTTP Source has been automatically configured for you. Copy the following URL.

```
https://endpoint6.collection.us2.sumologic.com/receive
r/v1/http/[illegible]
[illegible]
[illegible]
```

2. Use the URL as the target for your Source. Learn more

Collection Step 2: Get Your ZeroFOX API Key

After setting up your HTTP Source, navigate to https://cloud.zerofox.com to obtain your API Key. Your API key can be found in the bottom-right section of the User Settings page (https://cloud.zerofox.com/settings/user-settings).



User Settings

First Name: Sumo Logic

Last Name: Admin User

Email: sumo@logic.com

Note: This email address will be used for login and emails sent from the ZeroFOX platform.

Current Password

New Password

Re-enter New Password

Email Notifications

□ Receive all takedown update emails
This can be configured on an alert-by-alert basis when requesting takedowns or using the "Subscribe" button in the alert view. Checking this box will result in an email being sent each time any piece of content that has been requested for takedown either succeeds or fails.

API Information

API Key: ••

Please note that your API key is only visible when generated. If you lose or need to reset your key, your previous API keys will be invalidated.

Collection Step 3: Enable Webhooks from ZeroFOX Cloud

Once you have set up your HTTP Source in Sumo Logic and have obtained your Sumo Logic Collection URL and ZeroFOX API key, please contact product@zerofox.com to enable webhooks for your account. Webhooks will be enabled within one business day.

Collection Step 4: Verify ZeroFOX Alert Log Collection

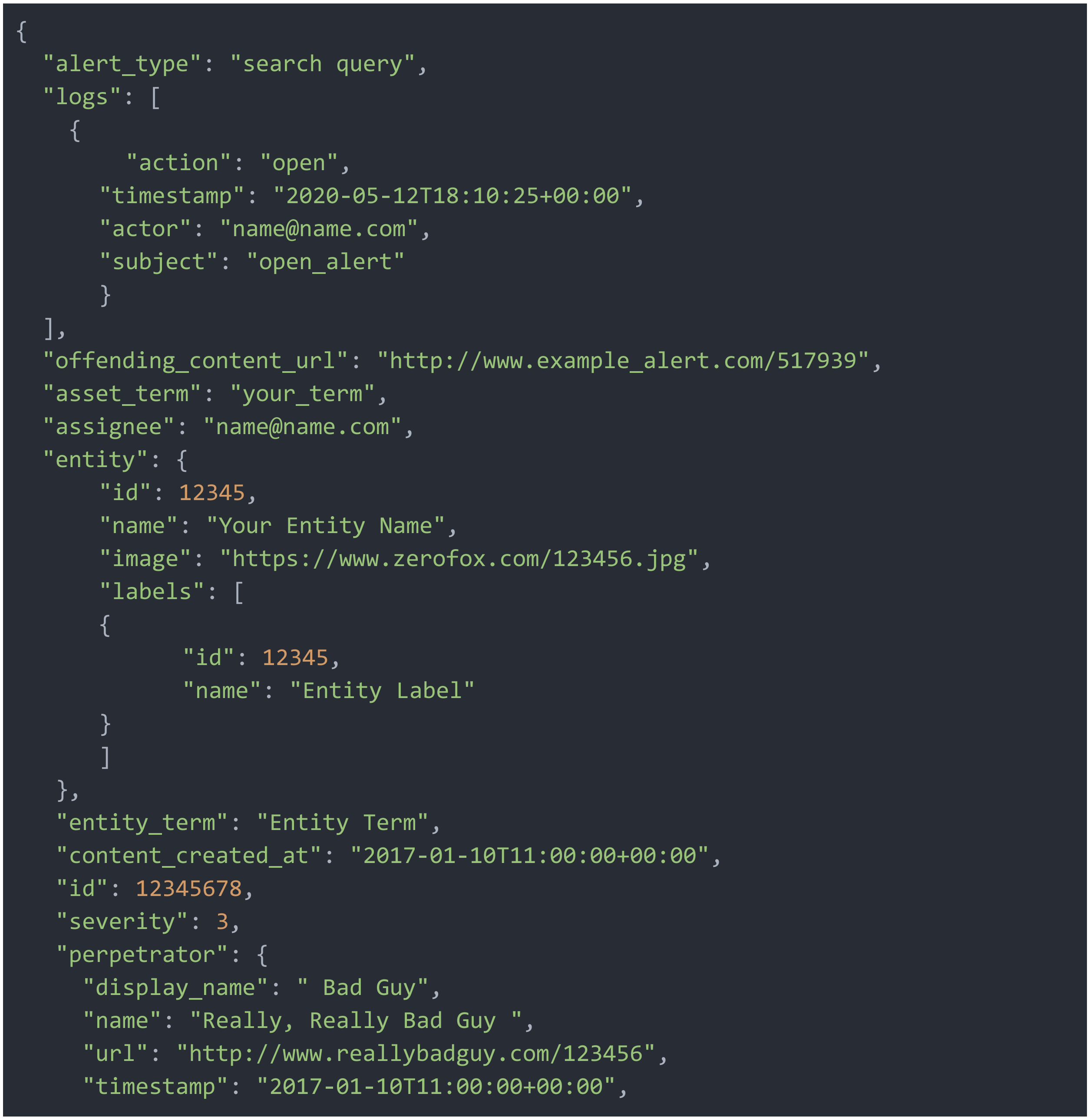
In Sumo Logic, open a Live Tail tab and run a search to verify Sumo Logic is receiving findings for the ZeroFOX source. Search by the source category you assigned to the HTTP Source that receives the log data ("ZeroFOX"), for example:

```
_sourceCategory="ZeroFOX"
```

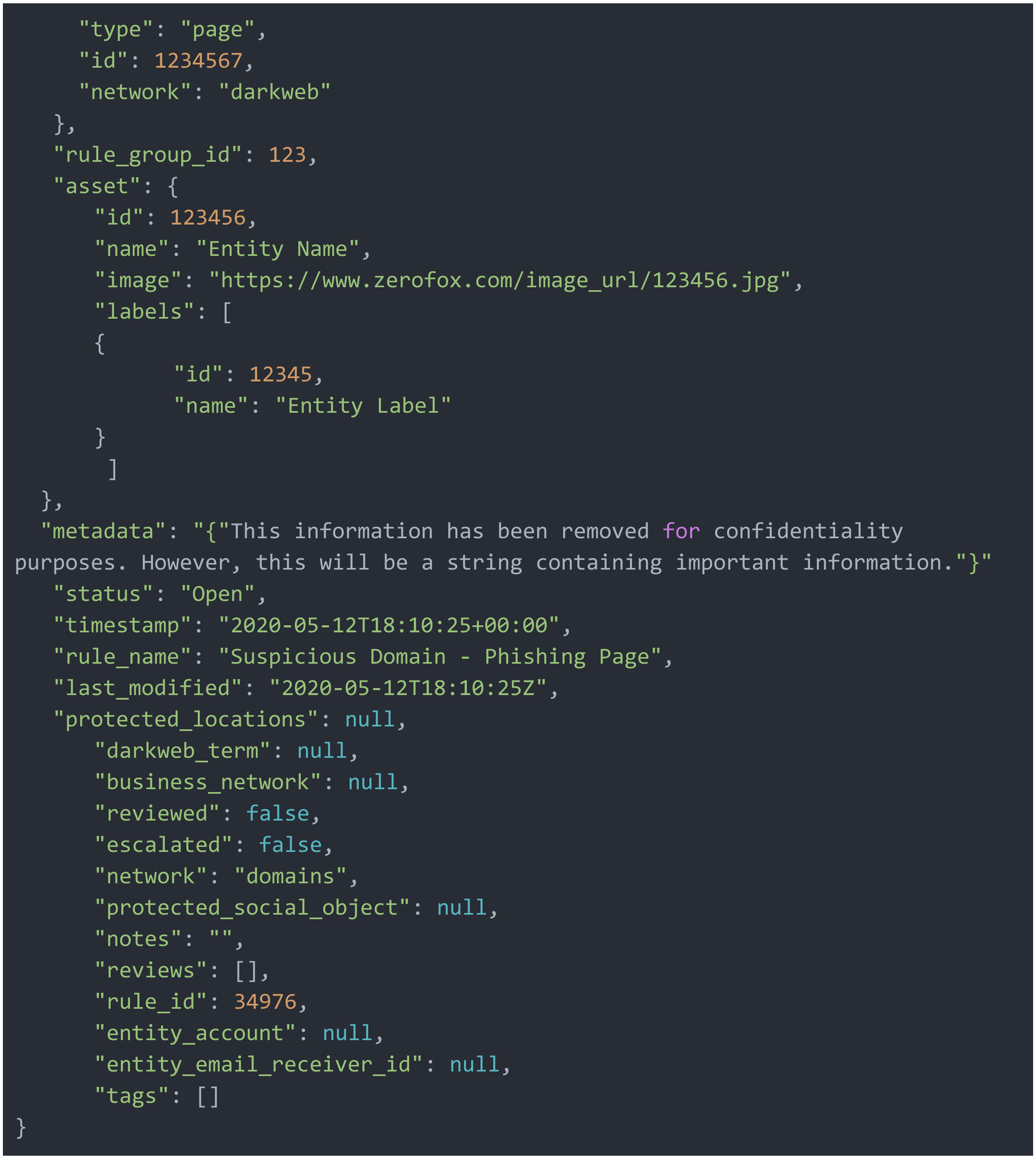
For more information on Sumo Logic's Live Tail, see Sumo Logic Live Tail documentation.

Sample Log Message

This section provides an example of a JSON alert log sent by ZeroFOX and logged in Sumo Logic.



```
{
  "alert_type": "search query",
  "logs": [
    {
        "action": "open",
      "timestamp": "2020-05-12T18:10:25+00:00",
      "actor": "name@name.com",
      "subject": "open_alert"
      }
  ],
  "offending_content_url": "http://www.example_alert.com/517939",
  "asset_term": "your_term",
  "assignee": "name@name.com",
  "entity": {
      "id": 12345,
      "name": "Your Entity Name",
      "image": "https://www.zerofox.com/123456.jpg",
      "labels": [
      {
            "id": 12345,
            "name": "Entity Label"
      }
      ]
   },
   "entity_term": "Entity Term",
   "content_created_at": "2017-01-10T11:00:00+00:00",
   "id": 12345678,
   "severity": 3,
   "perpetrator": {
     "display_name": " Bad Guy",
     "name": "Really, Really Bad Guy ",
     "url": "http://www.reallybadguy.com/123456",
     "timestamp": "2017-01-10T11:00:00+00:00",
```



```
     "type": "page",
     "id": 1234567,
     "network": "darkweb"
   },
   "rule_group_id": 123,
   "asset": {
      "id": 123456,
      "name": "Entity Name",
      "image": "https://www.zerofox.com/image_url/123456.jpg",
      "labels": [
      {
            "id": 12345,
            "name": "Entity Label"
      }
       ]
  },
  "metadata": "{"This information has been removed for confidentiality
purposes. However, this will be a string containing important information."}"
   "status": "Open",
   "timestamp": "2020-05-12T18:10:25+00:00",
   "rule_name": "Suspicious Domain - Phishing Page",
   "last_modified": "2020-05-12T18:10:25Z",
   "protected_locations": null,
      "darkweb_term": null,
      "business_network": null,
      "reviewed": false,
      "escalated": false,
      "network": "domains",
      "protected_social_object": null,
      "notes": "",
      "reviews": [],
      "rule_id": 34976,
      "entity_account": null,
      "entity_email_receiver_id": null,
      "tags": []
}
```

Sumo Logic Query Sample

The following is an example query that shows how to query alert information by network by hour.

```
_sourceCategory="ZeroFOX"
| json field=_raw "status"
| json field=_raw "network"
| timeslice 1h
| count by _timeslice, network
| sort by _timeslice asc
| transpose row _timeslice column network as *
```

Install the ZeroFOX App in Sumo Logic and View Dashboards

This section provides instructions on how to install the ZeroFOX Cloud Application for Sumo Logic, as well as examples of each of the dashboard. The pre-configured queries and dashboard provide easy-to-access visual insights into your data.

Install the ZeroFOX Cloud Application

Locate and install the ZeroFOX Cloud app from Sumo Logic's **App Catalog**. If you want to see a preview of the dashboards included with the app before installing, click **Preview Dashboards**.

1. From the **App Catalog**, search for and select the **ZeroFOX Cloud** app.
2. To install the app, click **Add to Library** and complete the following fields.
    a. **App Name**: You can retain the existing name, or enter a name of your choice for the app.
    b. **Data Source**: Select either of these options for the data source.
        i. Choose **Source Category** and select the ZeroFOX source category from the list (or whatever you named your HTTP Source when setting up for ZeroFOX).
        ii. Choose **Enter a Custom Data Filter**, and enter a custom source category beginning with an underscore. For example: (_sourceCategory=MyCategory).
    c. **Advanced**: Select the Location in Library (the default is the Personal folder in the library), or click New Folder to add a new folder.
3. Click **Add to Library**.

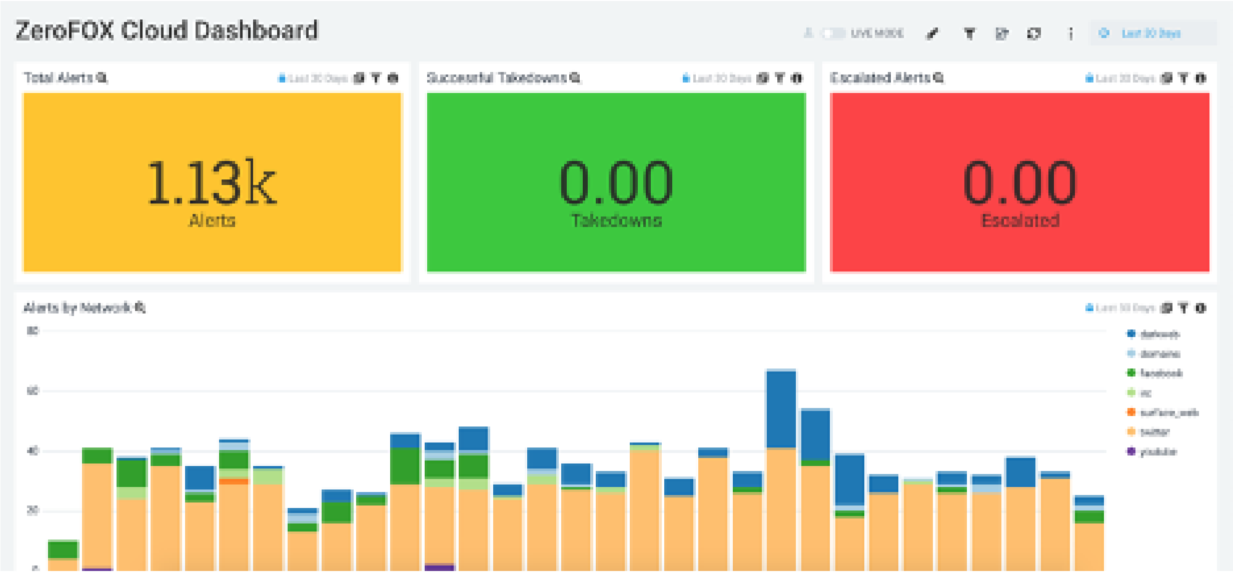
Once the ZeroFOX Cloud app is installed, it will appear in your Personal folder (or other folder that you specified). From here, you can share it with your organization.

Panels will start to populate automatically. It's important to note that each panel slowly fills with data matching the time range query and received since the panel was created. Some results won't immediately be available, but as content collection and forwarding occurs, you'll see a full dashboard filled with actionable information.

ZeroFOX Cloud Dashboard in Sumo Logic

This dashboard shows ZeroFOX alerting activity by date, network, entity, and rule, as well as total alerting, escalation and takedown activity. You can use this default dashboard to:

- See total alerts generated during the period
- View alert breakdown by network by day
- View alert breakdown by protected entity by day
- Review escalated alert metrics
- View alert breakdown by status by day
- View alerts generated by ZeroFOX rule by day
- Review takedown activity to see how much content is successfully taken down and what is still in progress
- Review accumulated alert activity by network for the period
- You can apply dashboard-level filters to view activity for the time period of your choice (prior 7 days by default)



The Sumo Logic dashboard shows summarized alert activity collected from ZeroFOX artificial intelligence technology.

About ZeroFOX

ZeroFOX, the global category leader in public attack surface protection, safeguards modern organizations from dynamic security risks across social, mobile, surface, deep and dark web, email and collaboration platforms. Using diverse data sources and artificial intelligence-based analysis, the ZeroFOX Platform identifies and remediates targeted phishing attacks, credential compromise, data exfiltration, brand hijacking, executive and location threats and more. The patented ZeroFOX SaaS technology processes and protects millions of posts, messages and accounts daily across the social and digital landscape, spanning LinkedIn, Facebook, Slack, Instagram, Pastebin, YouTube, mobile app stores, the deep & dark web, domains, email and more.