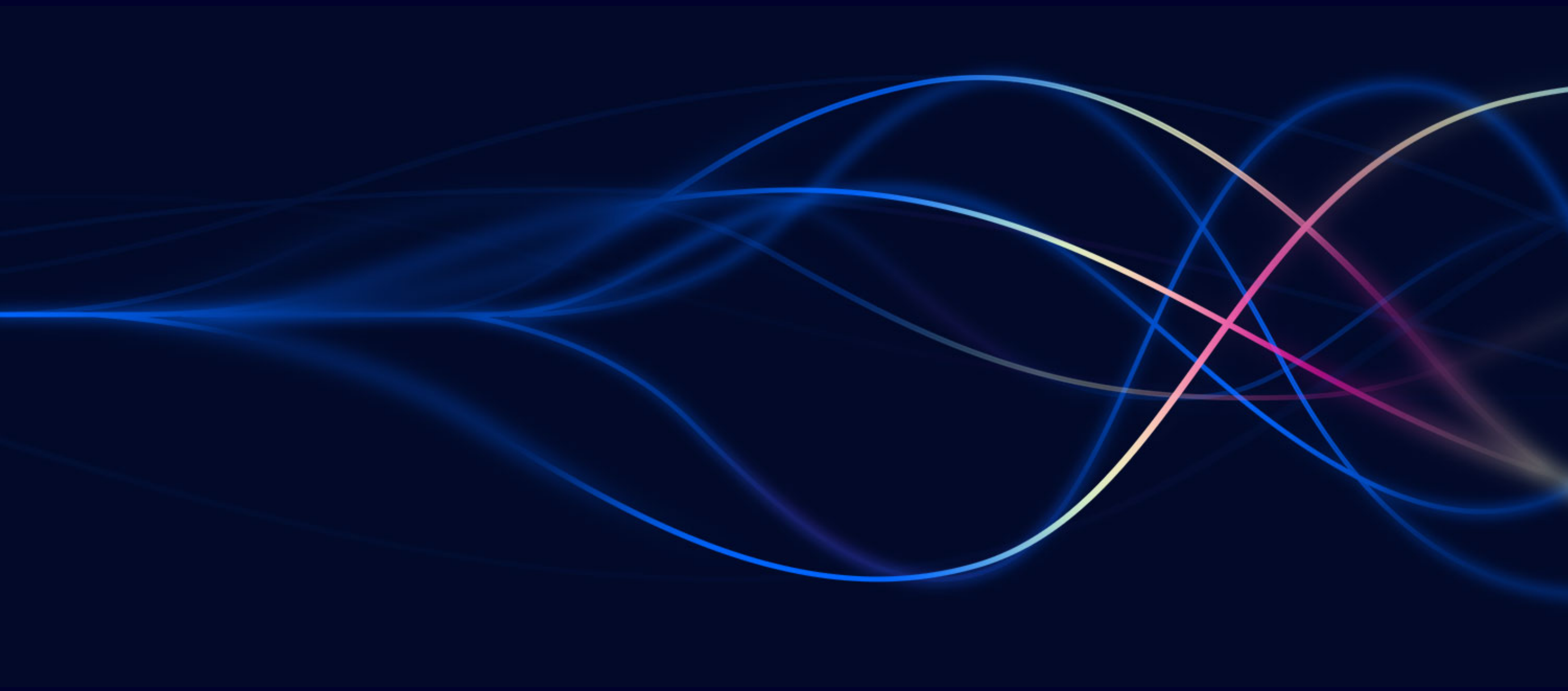
Q-FEEDS

Setup Guide
Exabeam SIEM API

Public



Version 1.0 - 16 December 2024

Introduction

In today's world, keeping your IT infrastructure secure is super important. Security Information and Event Management (SIEM) solutions are essential tools for detecting and responding to threats across your network. They can ingest external dynamic lists of threat indicators, known as Indicators of Compromise (IoCs), to enhance threat detection and investigation capabilities.

Q-Feeds provides dynamic, up-to-date lists of these IoCs, designed specifically for use with SIEM platforms like Exabeam. By integrating Q-Feeds into your Exabeam environment, you can improve your threat detection by enriching security events with the latest IoC data. This means Exabeam can identify malicious activity faster and provide better insights into emerging threats.

This manual will show you how to set up and use Q-Feeds with your Exabeam SIEM, so you can maximize your threat detection capabilities. You'll learn how to configure data ingestion, import Q-Feeds IoCs, and validate the integration. With these steps, you'll be able to enhance your security posture, improve threat hunting, and keep your organization safe from cyber threats.

Using Q-Feeds for Enhanced Network Security

Q-Feeds provides dynamic lists of Indicators of Compromise (IoCs) to enhance your network security controls. These lists, based on Q-Feeds Threat Intelligence Data Feeds, are regularly updated with various types of IoCs such as IP addresses and domains. By using these lists, you can monitor and block user access to dangerous network resources effectively.

Available Lists of Indicators

Q-Feeds offers the following types of indicators:

Name	Type	Description	URI
Malware IPs	IP	List of dangerous IP addresses	https://api.qfeeds.com/api?feed_type=malware_ip&api_token=XXXXXX&limit= XXXXXX&type=csv
Malware Domains	URL	List of malicious domains	https://api.qfeeds.com/api?feed_type=malware_domains&api_token=XXXXXX&limit= XXXXXX&type=csv
Phishing URLs	URL	List of phishing URLs	https://api.qfeeds.com/api?feed_type=phishing_urls&limit= XXXXXX&type=csv

To optimize system performance and prevent unnecessary strain on our infrastructure, please schedule updates at the standard interval of 20 minutes. Setting the interval to less than 20 minutes is not beneficial and may overload the system.

Accessing the lists—including direct downloads into your network security solutions—requires an API token from Q-Feeds. You can request this token through your account manager or by visiting our website at https://qfeeds.com/start-trial-license/.

With the trial token, you will receive 14 days of free and full access to all our indicators of compromise. If you need assistance, please contact your account manager or email us at sales@qfeeds.com.

To test downloading the lists, you can use the cURL utility. Here is the syntax for Linux systems:

```
curl -v -u api_token:XXXXX https://api.qfeeds.com/api?feed_type=XXXX&limit=XXXXX
```

Parameters to use within the URL:

feed_type=	<feed type as described in the tables above f.e malware_ip, malware_domains etc.>
limit=	<optional limit on number of IOC's>
api_token=	<user token provided by Q-Feeds>
type=	<to define plain txt or CSV> *Exabeam only accepts CSV*

Setup Q-Feeds

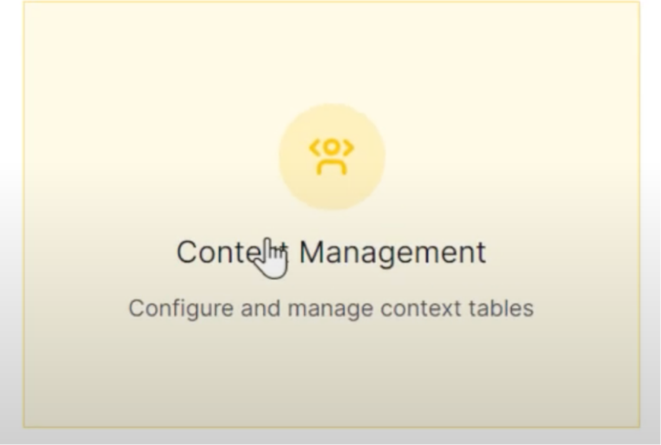
To create correlations based on our threat intelligence within you Exabeam SIEM we need to create a context table. Unfortunately, Exabeam does not support to add additional threat intelligence feeds other than their own. Therefore, we're going to use the API to enrich a context table with our IOC's.

Please follow the steps in this tutorial from Exabeam:

https://www.youtube.com/watch?v=o0bWclXMVpE

Written instructions below:

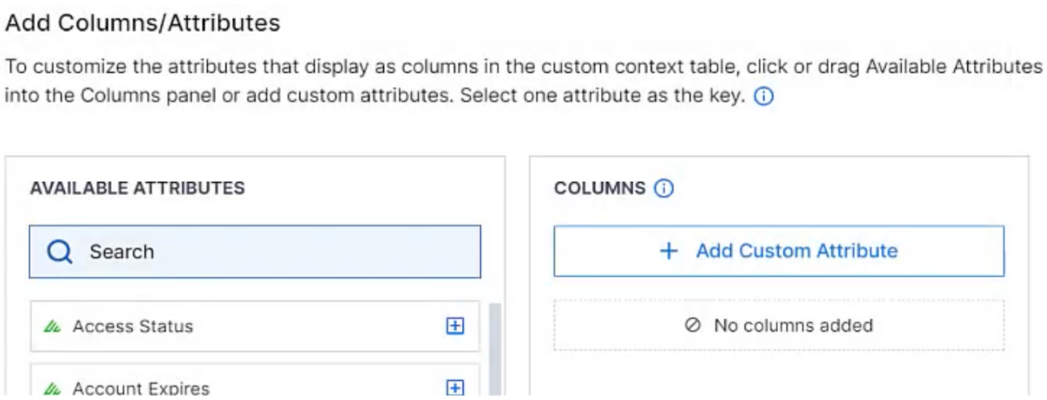
1. Therefore, go to **'Context Management'** and click on **'New table'**



Context Management

Configure and manage context tables

2. Choose **'Add Custom'**, define a name and choose **other** for the table type.
3. Select **'Add attributes'** and click on **'Add Custom Attribute'** f.e. bad_ips or bad_domains or bad_urls based on the feed you want to ingest.
4. Assign the added attribute as **'key attribute'**



Add Columns/Attributes

To customize the attributes that display as columns in the custom context table, click or drag Available Attributes into the Columns panel or add custom attributes. Select one attribute as the key.

API Keys

In order to use the API to ingest the IOC's in the table you will need a API key from Exabeam.

1. Go to the admin settings → API keys en **create a new key**.
2. Set the permissions to **"manage context"**
3. Then after creation select the 3-dots menu behind the line you just created and select **'Generate and copy token'**. Paste the token for later use.

Get context table metadata

1. Go to https://developers.exabeam.com/exabeam/reference/getcontext-managementv1tables
2. **Paste the access token** you've acquired in the previous paragraph in the **token field.**
3. **Select the right base url for your region**
4. And click **'Try it!'**
5. Scroll down the results and find the context table(s) you've created earlier. **Copy the metadata.**
6. The ID for the attribute and the ID for the table itself are needed in a following step.

Add content to existing table

1. Go to https://developers.exabeam.com/exabeam/reference/postcontext-managementv1tablesidaddrecordsfromcsv
2. Fill in the field Specify the ID of an existing context table with the ID of your table you copied in step 6 of the last paragraph.
3. In the **sourceAttributes** fill in the type of attribute you would like to add **depending on the feed type**. It's either **IP, domain or url.**
4. The fild **targetAttributeIds** are in the metadata you've copied in step 6 of the previous paragraph.
5. Operation select **replace**

Now the API tool from Exabeam provides you with various script languages in order to automate this process. You can run scripts in various languages every 20 minutes to update and replace the context tables within Exabeam.

Example scripts

Here’s an example on how a shell script looks to enhance the context table with our Malware IP IOC’s:

```
curl --request POST \
    --url "https://api.eu.exabeam.cloud/context-management/v1/tables/<your-table-id>/addRecordsFromCsv" \
    --header 'accept: application/json' \
    --header 'authorization: Bearer <your-api-token-from-exabeam>' \
    --header 'content-type: multipart/form-data' \
    --form 'sourceAttributes=IP' \
    --form 'targetAttributeIds=<your-attribute-id>' \
    --form operation=replace \
    --form file=@<(curl "https://api.qfeeds.com/api.php?feed_type=malware_ip&api_token=<yourtoken>&type=csv")
```

A python script would look like this:

```
import requests
import io

# First, get the CSV from q-feeds
qfeed_url = "https://api.qfeeds.com/api.php?feed_type=malware_ip&api_token=<yourtoken>&type=csv"
qfeed_response = requests.get(qfeed_url)
qfeed_csv = qfeed_response.content  # this is the CSV data as bytes

# Now prepare the request to Exabeam
url = "https://api.eu.exabeam.cloud/context-management/v1/tables/<your-table-id>/addRecordsFromCsv"

payload = {
    "sourceAttributes": "<IP, domain or url depending on the feedtype>",
    "targetAttributeIds": "<your-attribute-id>",
    "operation": "replace"
}

# Instead of reading a local file, we just use the CSV data we got from q-feeds.
files = {
    "file": ("feed.csv", io.BytesIO(qfeed_csv), "text/csv")
}

headers = {
    "accept": "application/json",
    "authorization": "Bearer <your-api token from exabeam>"
}

response = requests.post(url, data=payload, files=files, headers=headers)
print(response.text)
```