

Cybersixgill API v2

Reference Guide

January 2025

Contents

Scope	5
Generating API Credentials	6
Authenticating Requests	8
The Cybersixgill API Suite	12
Actionable Alerts API	13
actionable-alert (get)	14
actionable-alert (delete)	17
actionable-alert (patch)	19
actionable_alert/stats (get)	21
actionable_alert/count (get)	23
actionable_alert/{actionable_alert_id} (get)	24
actionable_alert/{actionable_alert_id} (delete)	28
actionable_alert/{actionable_alert_id} (patch)	30
actionable_alert_content/{actionable_alert_id} (get)	33
alert_type_id/update_alert_frequency (patch)	38
Assets API	40
organization assets (get)	40
organization assets (put)	43
organization assets (post)	47
Credentials API	51
leaks (get)	52
DVE Enrichment API	55
enrich (post)	56
keyword_search (get)	61
{id} (get)	63
{remediation} (get)	66
cves_by_cpes (get)	68

DVE Feed API	70
ioc (DVE Feed)	71
ioc/ack (DVE Feed)	73
Dark Feed API	75
ioc (Dark Feed)	76
ioc/ack (Dark Feed)	78
Dark Feed Enrichment API	80
ioc/enrich (post)	81
Events Feed API	84
events_feed (get)	85
events_feed/ack (post)	90
Intel Items API	92
aggs (post)	93
intel_items (post)	97
intel_items (get)	103
intel_items/next	107
intel_items/{id}/thread	110
intel_items/thread/next	114
intel_items/{id}	116
histogram (post)	119
Multi-Tenancy API	123
organization (post)	124
organization (get)	126
organization (delete)	128
organization assets (post)	129
organization assets (get)	133
organization assets (put)	136
organization/{organization_id}/user (get)	140

organization/{organization_id}/user/{assigned_user_id} (post)	141
organization/{organization_id}/user/{assigned_user_id} (get)	143
organization/{organization_id}/user/{assigned_user_id} (put)	144
organization/{organization_id}/user/{assigned_user_id} (delete)	146
Appendix A - How to Query	148
Building Cybersixgill Search Queries	148

Scope

This document describes how to log in to the Cybersixgill Developer Portal and use Sixgill Ltd.'s APIs in your environment. It is a detailed reference with examples for the APIs endpoints.

The document contains the following sections:

- > [Generating API Credentials](#)
- > [Authenticating Requests](#)
- > [The Cybersixgill API Suite](#)
- > [Appendix A - How to Query](#)

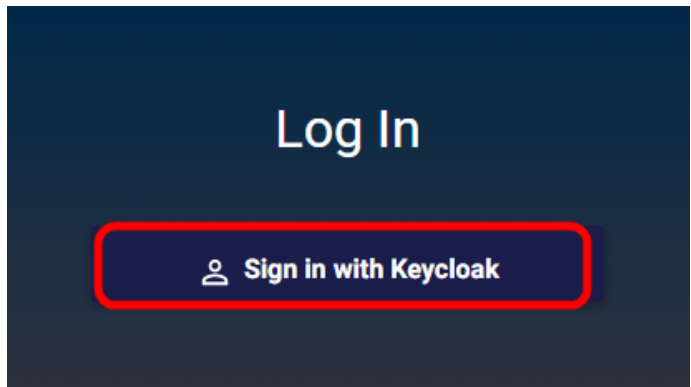
Generating API Credentials

Before you can use Cybersixgill's API, you must generate a client ID and secret by accessing the Developer Portal.

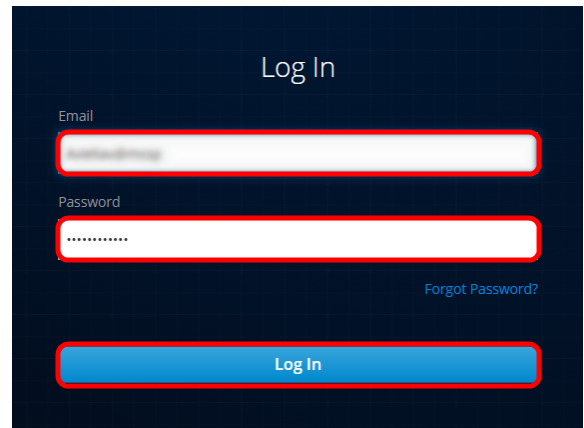
You will need your Cybersixgill credentials as defined when you registered with Cybersixgill.

To access Developer Portal:

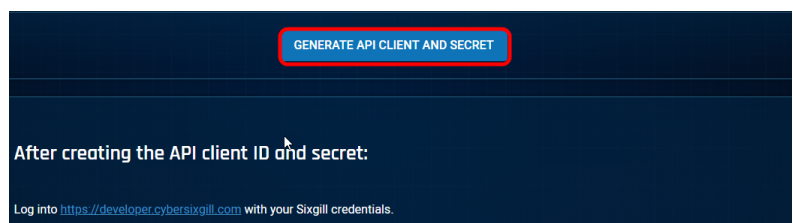
1. Open the following URL: <https://developer.cybersixgill.com> and click **Sign in with Keycloak**.



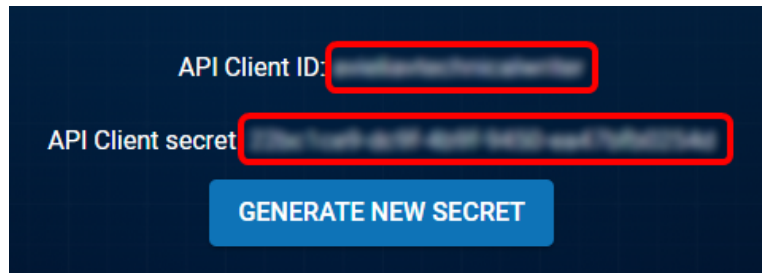
2. Enter your Cybersixgill credentials as defined when you registered with Cybersixgill and click **Log In**.



3. Click **GENERATE API CLIENT AND SECRET**.



4. Save the **API Client ID** and the **API Client secret** in a safe location. You will need it when using the API.



If you need to generate a new API client secret, click **GENERATE NEW SECRET**. You will need to apply the new secret to any application using the previous secret.

Authenticating Requests

API authentication is performed via HTTP Basic Auth using the API Client and Secret you generated (see [Generating API Credentials](#)). The authentication method uses the bearer scheme and returns a token that you must use in your request headers.

All API requests must be made over HTTPS. Requests without authentication will fail.

General

Item	Details
URL	https://api.cybersixgill.com/auth/token
Description	Returns an authentication token for use in your API requests headers.
Method	POST

A request body is required and you can define the following body parameters in the request.

Parameters

Parameter	Required	Type	Description
client_id	Yes	string	Your API Client ID that you generated in the Sixgill Ltd. Onboarding Portal (see Generating API Credentials)
client_secret	Yes	string	Your API Client secret that you generated in the Sixgill Ltd. Onboarding Portal (see Generating API Credentials)
grant_type	Yes	string	Set value to: client_credentials

Request example

```
curl -L -X POST 'https://api.cybersixgill.com/auth/token' \  
-H 'Content-Type: application/x-www-form-urlencoded' \  
-H 'Cache-Control: no-cache' \  
-H 'Content-Type: application/x-www-form-urlencoded' --data-urlencode 'grant_\  
type=client_credentials' --data-urlencode 'client_secret=<your client_secret>' --data-\  
urlencode 'client_id=<your client_id>'
```


Responses

Example: Response 200 - OK.



You will use access token value (between the " ") in the authorization header of your request.

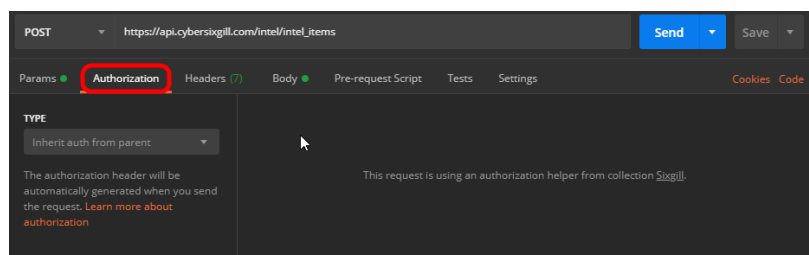
```
{
  "access_token":
  "eyJhbGciOiJIUzUxMiIsInR5cCI6IkpXZWQ0aXBvdC2ZDU4M
  y1lODI1LTRhNmEtYTZiMC1iNDhiNjA2MGM5YmlifQ.eyJleHAiOiJl
  bGwtZnJvbnRlbnQuc3ZjOjgwODAvYXV0aC9yZWZsbXMvTWZpbiImF1ZCI6Im
  FjY291bnQiLCJzdzWliOiJjY2QxZTRIMy1lZRxVokl_34Pg",
  "expires_in": 1800,
  "refresh_expires_in": 0,
  "token_type": "Bearer",
  "not-before-policy": 0,
  "scope": "email profile"
}
```

Example: Response 400 - Bad parameters.

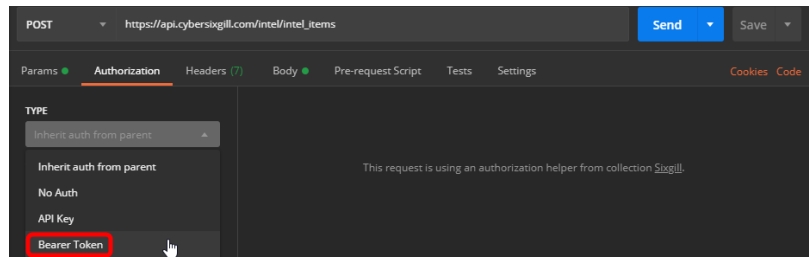
```
{
  "status_code": 400,
  "message": "Bad Parameters: query"
}
```

Example of Using Authentication in a Request in Postman

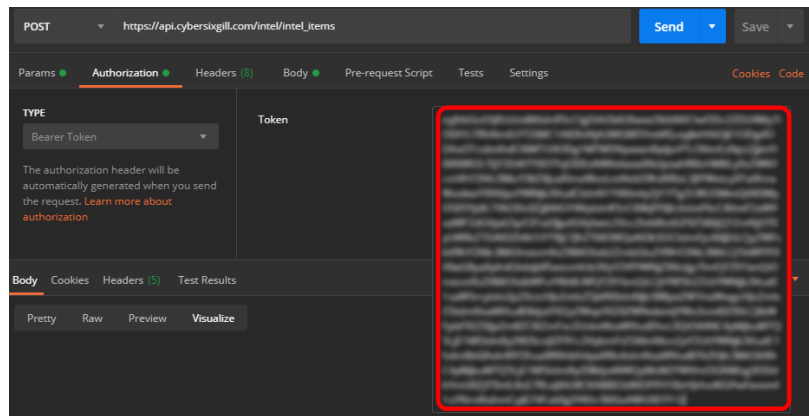
1. Click the **Authorization** tab.



2. In the **TYPE** list, click **Bearer Token**.

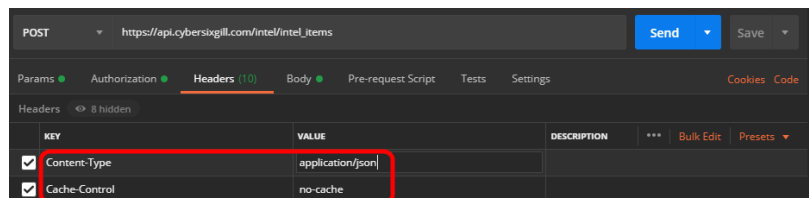


3. In the Token box, paste the **access_token** value returned by the auth/token request.

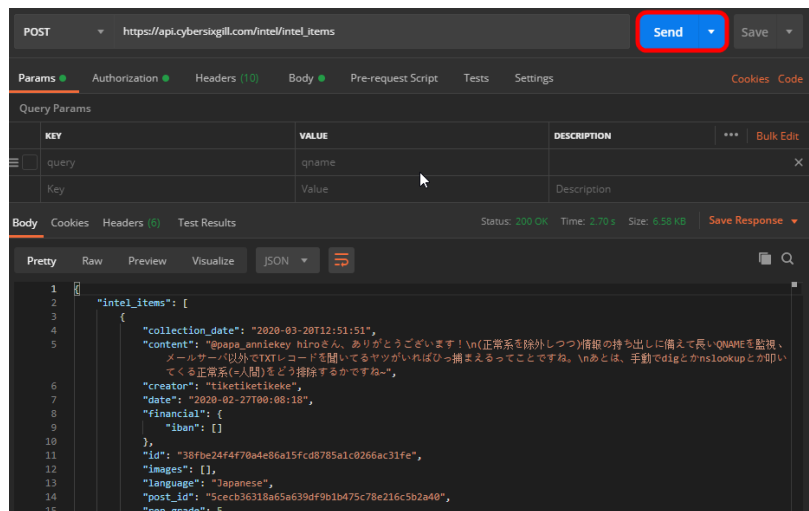


4. Click the **Headers** tab and add the following key values:

- > Content-Type = application/json
- > Cache-Control = no-cache



5. Set any parameters required for the request you are using and click **Send**. The response appears at the bottom of the window.



The Cybersixgill API Suite

Cybersixgill has created the following collection of APIs for use in your applications:



All data fetched by endpoints are returned as JSON files.

API	Description
Actionable Alerts API	Endpoints to manage actionable alerts.
Assets API	Endpoints to manage organization and user data.
Credentials API	Endpoints to get leaked credentials for a specified date range from the Sixgill system.
DVE Enrichment API	Endpoints to enrich your CVEs with Cybersixgill's dynamic vulnerability Exploit Score (DVE)
DVE Feed API	Endpoints to consume Cybersixgill's Dynamic Vulnerability Exploit DVE feed.
Dark Feed API	Endpoints for Dark Feed IOC data.
Dark Feed Enrichment API	Endpoints for Dark Feed IOC enrichment data.
Events Feed API	The Events Feed API provides endpoints to consume event items.
Intel Items API	Endpoints for obtaining detailed information on intel items, aggregations of intel items, and histograms based on a date range from the Cybersixgill system.
Multi-Tenancy API	Endpoints for use with the multi-tenant (MSSP) platform.

Actionable Alerts API

The Actionable Alerts API provides endpoints for obtaining detailed information on actionable alerts.

The API contains the following endpoints.

Group	Description	Endpoint
Actionable Alerts	Get actionable alerts by ID list with optional filters.	/actionable-alert (get)
	Deletes a list of actionable alerts by ID with optional filters.	/actionable-alert (delete)
	Updates a list of actionable alerts by ID with optional filters.	/actionable-alert (patch)
	Gets actionable alerts statistics per user.	/actionable_alert/stats (get)
	Gets the total number of read and unread actionable alerts statistics by user.	/actionable_alert/count (get)
Actionable Alert	Gets an actionable alert by ID.	/actionable_alert/{actionable_alert_id} (get)
	Deletes an actionable alert by ID.	/actionable_alert/{actionable_alert_id} (delete)
	Updates an actionable alert by ID.	/actionable_alert/{actionable_alert_id} (patch)
Actionable Alert Content	Gets actionable alert content by alert ID.	/actionable_alert_content/{actionable_alert_id} (get)
Alert Type ID	Updates frequency of an alert type	/alert_type_id/update_alert_frequency (patch)

actionable-alert (get)

General

Item	Details
URL	https://api.cybersixgill.com/alerts/actionable-alert
Description	Get actionable alerts by ID list with optional filters.
Method	GET

Parameters

Parameter	Required	Type	Description
sort_by	No	string	Sort the results by the field specified, such as: <ul style="list-style-type: none">> date (default)> alert_name> threat_level
sort_order	No	string	Sets the sort order for the fetched results: <ul style="list-style-type: none">> asc> desc (default)
offset	No	string	Specifies the number of alerts to ignore before display the results. For example, offset: 200 displays the 201 st alert and forward. Default: 0 (displays from the first alert)
fetch_size	No	string	Number of alerts in the result. Default: 50
from_date	No	string	Fetch alerts from this date, format - YYYY-MM-DD HH:mm:ss

Parameter	Required	Type	Description
to_date	No	string	Fetch alerts up to this date, format - YYYY-MM-DD HH:mm:ss
status	No	array[string]	Filter by status: <ul style="list-style-type: none"> > treatment_required > in_treatment > resolved
alert_type_id	No	string	The unique identifier of an alert type.
organization_id	Yes (for multi-tenant)	string	organization_id (required for multi-tenant)
is_read	No	string	Filter by read: <ul style="list-style-type: none"> > unread
threat_level	No	string	Filter by threat level: <ul style="list-style-type: none"> > imminent > emerging
threat_type	No	string	Filter by threat type.

Request example

```
curl --location --request GET 'https://api.cybersixgill.com/alerts/actionable-alert?status=treatment_required' \
--header 'Authorization: Bearer <token>'
```

Responses

Example: Response 200 - OK.

```
{
  "alert_name": "RogueAppAlert",
  "category": "regular",
  "content": "Name: Emoji Smile Cute Theme\nApp Store: Google Play Store\nTriggered"
```

```
By: tech\nURL:  
https://play.google.com/store/apps/details?id=emoji.cute.smile.wallpaper\nDeveloper:  
Launcher Fantasy\nContact Details: utopiadesign01@gmail.com",  
  "date": "2020-05-13 18:15:05",  
  "id": "5ebc3929a4a7e300012365ae",  
  "read": false,  
  "site": "github",  
  "status": [  
    "name": "treatment_required"  
  ]  
  "threat_level": "imminent",  
  "threats": [  
    "Data Leak",  
    "Brand Protection",  
    "Phishing",  
    "Malware"  
  ],  
  "title": "An App Matching JJ Halen Assets was Found in an App Store",  
  "user_id": "5d2336aef8db38787dbe4f69"  
}
```

Example: Response 400 - Bad request.

```
{  
  "detail": "u'imminente' is not one of ['imminent', 'emerging']\n\nFailed validating 'enum'  
in schema:\n  {'description': 'Filter by alert threat level',\n   'enum': ['imminent',  
'emerging'],\n   'in': 'query',\n   'name': 'threat_level',\n   'type': 'string'}\n\nOn  
instance:\n  u'imminente",  
  "status": 400,  
  "title": "Bad Request",  
  "type": "about:blank"  
}
```


actionable-alert (delete)

General

Item	Details
URL	https://api.cybersixgill.com/alerts/actionable-alert
Description	Deletes a list of actionable alerts by ID with optional filters.
Method	DELETE

Parameters

Parameter	Required	Type	Description
organization_id	Yes (for multi-tenant)	string	organization_id (required for multi-tenant)
is_read	No	string	Filter by read: > unread
threat_level	No	string	Filter by threat level: > imminent > emerging
threat_type	No	string	Filter by threat type.
alert_id (body)	Yes	string	Actionable alerts ID, in format ["61bd2d749339dad426779da0", "61bcc13b9339dad426779d39"]

Request example

```
curl -X DELETE 'https://api.cybersixgill.com/alerts/actionable-alert?severity=high&threat_level=imminent' \
-H "Authorization: Bearer [access_token value]" \
-H 'Content-Type: application/json' \
--data-raw '[
  "5ebc3929a4a7e300012365ae"
]'
```

Responses

Example: Response 200 - Modified successfully.

```
{
  "items_modified_count": 1,
  "message": "Successfully deleted 1 Actionable Alerts",
  "status": 200
}
```

Example: Response 400 - Bad request.

```
{
  "detail": "u'imminente' is not one of ['imminent', 'emerging']\n\nFailed validating 'enum'
in schema:\n  {'description': 'Filter by alert threat level',\n   'enum': ['imminent',
'emerging'],\n   'in': 'query',\n   'name': 'threat_level',\n   'type': 'string'}\n\nOn
instance:\n  u'imminente'",
  "status": 400,
  "title": "Bad Request",
  "type": "about:blank"
}
```

actionable-alert (patch)

General

Item	Details
URL	https://api.cybersixgill.com/alerts/actionable-alert
Description	Updates a list of actionable alerts by ID with optional filters. It supports read/unread and a change in treatment status.
Method	PATCH

Parameters

Parameter	Required	Type	Description
organization_id	Yes (for multi-tenant)	string	organization_id (required for multi-tenant)
set_read	No	string	Filter by read: > unread
threat_level	No	string	Filter by threat level: > imminent > emerging
threat_type	No	string	Filter by threat type:

Request example

```
curl --location --request PATCH 'https://api.cybersixgill.com/alerts/actionable-alert' \
--header 'Authorization: Bearer <token>' \
--header 'Content-Type: application/json' \
--data-raw '{
  "id_list": [
    "5fb4c6a6d604c200010f0916"
  ],
  "set_read": "read"
}'
```

Responses

Example: Response 200 - OK.

```
{
  "items_modified_count": 1,
  "message": "Successfully updated 1 Actionable Alerts",
  "status": 200
}
```

Example: Response 400 - Bad request.

```
{
  "detail": "[u'111'] is not of type 'object'",
  "status": 400,
  "title": "Bad Request",
  "type": "about:blank"
}
```

actionable_alert/stats (get)

General

Item	Details
URL	https://api.cybersixgill.com/alerts/actionable_alert/stats
Description	Gets actionable alerts statistics per user.
Method	GET

Parameters

Parameter	Required	Type	Description
organization_id	Yes (for multi-tenant)	string	organization_id (required for multi-tenant)
threat_level	No	string	Filter by threat level: <ul style="list-style-type: none">> imminent> emerging

Request example

```
curl --location --request GET 'https://api.cybersixgill.com/alerts/actionable_alert/stats' \
--header 'Authorization: Bearer <token>'
```

Responses

Example: Response 200 - OK.

```
{
  "by_threat_level": {
    "emerging": 140,
    "imminent": 360
  },
  "by_threat_type": {
    "Brand Protection": 9,
```

```
"Compromised Accounts": 48,  
"DDoS Attack": 96,  
"Data Leak": 49,  
"Defacement": 97,  
"Fraud": 164,  
"Malware": 9,  
"Phishing": 82,  
"Vulnerability Exploit": 129,  
"Web Attack": 96  
},  
"total": 500  
}
```

Example: Response 400 - Bad request.

```
{  
  "detail": "u'imminente' is not one of ['imminent', 'emerging']\n\nFailed validating 'enum'  
in schema:\n  {'description': 'Filter by alert threat level',\n   'enum': ['imminent',  
'emerging'],\n   'in': 'query',\n   'name': 'threat_level',\n   'type': 'string'}\n\nOn  
instance:\n  u'imminente",  
  "status": 400,  
  "title": "Bad Request",  
  "type": "about:blank"  
}
```

actionable_alert/count (get)

General

Item	Details
URL	https://api.cybersixgill.com/alerts/actionable_alert/count
Description	Gets the total number of read and unread actionable alerts statistics by user.
Method	GET

Parameters

Parameter	Required	Type	Description
organization_id	Yes (for multi-tenant)	string	organization_id (required for multi-tenant)

Request example

```
curl --location --request GET 'https://api.cybersixgill.com/alerts/actionable_alert/count' \
--header 'Authorization: Bearer <token>'
```

Response

Example: Response 200 - OK.

```
{
  "total": 100,
  "read": 25,
  "unread": 75
}
```

actionable_alert/{actionable_alert_id} (get)

General

Item	Details
URL	https://api.cybersixgill.com/alerts/actionable_alert/{actionable_alert_id}
Description	Gets an actionable alert by ID.
Method	GET

Parameters

Parameter	Required	Type	Description
actionable_alert_id	Yes	string	actionable_alert_ID
organization_id	Yes (for multi-tenant)	string	organization_id (required for multi-tenant)

Request example

```
curl --location --request GET 'https://api.cybersixgill.com/alerts/actionable_alert/5fbcfeb23a5ce900013de081' \
--header 'Authorization: Bearer <token>'
```

Responses

Example: Response 200 - OK.

```
{
  "additional_info": {
    "asset_attributes": [
      "organization_name",
      "organization_aliases"
    ],
    "date": "2020-11-24T12:07:39",
    "matched_organization_aliases": [],
    "organization_aliases": [
      "first bank pr",

```


Example: Response 200 - OK.

```
"bearing point",
"sap ns2",
"carahsoft",
"santander",
"sap",
"cvs health",
"optiv",
"capgemini",
"accenture",
"boa",
"kpmg",
"sixgill"
],
"organization_name": "Sixgill",
"post_attributes": [
  "date",
  "site"
],
"query_attributes": [
  "organization_aliases"
],
"site": "telegram",
"template_id": "5dab44c04d91dd0c9da3bed1"
},
"alert_id": "5dab44c14d91dd0c9da3bef4",
"alert_name": "{organization_name}'s Compromised Login Details are Offered for Sale on {site}",
"assessment": "",
"category": "regular",
"content_type": "search_result_item",
"description": "Sixgill has recently identified a threat actor looking to sell access to an account of Sixgill or one of its brands and products. The sale offer was posted on 'telegram' on 2020-11-24T12:07:39.",
"es_id": "ac10de1aacd497249a0b86164af8fdf7d3460f98",
"es_item": {
  "category": "HOW MUCH BRO",
  "channel_message_id": 103727,
  "collection_date": "2020-11-24T12:07:40",
  "company_name": [
    "wells fargo"
  ],

```

Example: Response 200 - OK.

```
"content": "CASHAPP DROPS ( 5k and 10k) - $150-200\NEW SBA SAUCE WITH - $60 comes with free pro and walkthrough Video \20k Grant Approval link,sauce & walkthrough- $50 ( PRO ONLY NEEDED )\ Logins Boa, Chase, Wells Fargo - $55 ( shows how to login )",
  "creator": "CryptoKing23(1201313874)",
  "date": "2020-11-24T12:07:39",
  "enrichment_version": 23,
  "financial": {
    "iban": []
  },
  "id": "a3407afc01bd1f83d48a011fd96a2f9a",
  "images": [],
  "ips": [],
  "lang": "en",
  "lang_full": [
    {
      "lang": "en",
      "lang_percent": 0.99
    }
  ],
  "lang_percent": 0.99,
  "message_url": "https://t.me/YOUNGBAGGERSG4/103727",
  "post_id": "1b25dc035688ea6e2c83252f6b7967af",
  "rep_grade": 1.0,
  "site": "telegram",
  "site_grade": 5,
  "sources_author_id": 1201313874,
  "spont": 6.3381028175354,
  "tags": [
    "Company_name"
  ],
  "title": "Telegram Group HOW MUCH BRO",
  "type": "chat",
  "update_date": "2020-11-24T12:10:50.821439",
  "url": "https://t.me/YOUNGBAGGERSG4",
  "username": "Cryptolowkey23"
},
{id": "5fbcfeb23a5ce900013de081",
  "lang": "English",
  "langcode": "en",
  "read": true,
  "recommendations": [
```

Example: Response 200 - OK.

```
"Sixgill highly recommends Sixgill to further investigate the incident in order to
identify potentially compromised accounts.",
"Sixgill highly recommends Sixgill to notify users who are affected by this incident.",
"It is highly recommended to reset any compromised accounts' password."
],
"severity": 1,
"status": {
  "name": "in_treatment",
  "user": "5d2335fbf8db38787dbe2511"
},
"summary": "",
"threat_level": "imminent",
"threats": [
  "Fraud"
],
"title": "Sixgill's Compromised Login Details are Offered for Sale on 'telegram'",
"update_time": "2020-11-24 12:38:10",
"user_id": "5d233575f8db38787dbe24b6"
}
```

Example: Response 404 - Resource with specified ID was not found.

```
{
  "items_modified_count": 0,
  "message": "ActionableAlert with ID 5fbcfeb23a5ce900013de081a not found",
  "status": 404
}
```

actionable_alert/{actionable_alert_id} (delete)

General

Item	Details
URL	https://api.cybersixgill.com/alerts/actionable_alert/{actionable_alert_id}
Description	Deletes an actionable alert by ID.
Method	DELETE

Parameters

Parameter	Required	Type	Description
actionable_alert_id	Yes	string	actionable_alert_ID
organization_id	Yes (for multi-tenant)	string	organization_id (required for multi-tenant)

Request example

```
curl --location --request DELETE 'https://api.cybersixgill.com/alerts/actionable_alert/5fbcfeb23a5ce900013de081' \
--header 'Authorization: Bearer <token>'
```

Responses

Example: Response 200 - OK.

```
{
  "items_modified": [
    "5fbcfeb23a5ce900013de081"
  ],
  "items_modified_count": 1,
  "message": "Successfully deleted 5fbcfeb23a5ce900013de081",
  "status": 200
}
```

Example: Response 404 - Resource with specified ID was not found.

```
{  
  "items_modified_count": 0,  
  "message": "Actionable Alert with ID 5fbcfeb23a5ce900013de081a not found",  
  "status": 404  
}
```

actionable_alert/{actionable_alert_id} (patch)

General

Item	Details
URL	https://api.cybersixgill.com/alerts/actionable_alert/{actionable_alert_id}
Description	Updates an actionable alert by ID.
Method	PATCH

Parameters

Parameter	Required	Type	Description
actionable_alert_id	Yes	string	actionable_alert_ID
organization_id	Yes (for multi-tenant)	string	organization_id (required for multi-tenant)

A request body is required and you can define the following parameters in the request:

Parameter	Required	Type	Description
read	Yes	string	Values: > "read" > "unread"
threat_level	Yes	string	Values: > "imminent" > "emerging"
status	Yes	string	Values: > "treatment_required" > "in_treatment" > "resolved"

Request example

```
{
  "read": "read",
  "threat_level": "imminent",
  "status": {
    "status": "in_treatment",
  }
}
```

Responses

Example: Response 200 - OK.

```
{
  "items_modified": [
    "5fbcfeb23a5ce900013de081"
  ],
  "items_modified_count": 1,
  "message": "Successfully updated 5fbcfeb23a5ce900013de081",
  "status": 200
}
```

Example: Response 400 - Bad request.

```
{
  "detail": "'u'imminente' is not one of ['imminent', 'emerging']",
  "status": 400,
  "title": "Bad Request",
  "type": "about:blank"
}
```

Example: Response 400 - Bad request.

```
{
  "detail": "'resolve' is not one of ['treatment_required', 'in_treatment', 'resolved']",
  "status": 400,
  "title": "Bad Request",
  "type": "about:blank"
}
```

Example: Response 404 - Resource with specified ID was not found.

```
{
  "items_modified_count": 0,
  "message": "Actionable Alert with ID 5fbcfefb23a5ce900013de081a not found",
  "status": 404
}
```



actionable_alert_content/{actionable_alert_id} (get)

General

Item	Details
URL	https://api.cybersixgill.com/alerts/actionable_alert_content/{actionable_alert_id}
Description	Gets actionable alert content by alert ID.
Method	GET

Parameters

Parameter	Required	Type	Description
organization_id	Yes (for multi-tenant)	string	organization_id (required for multi-tenant)
actionable_alert_id	Yes	string	actionable_alert_ID
limit	No	integer	The number of replies.
fetch_content_urls	No	boolean	If true returns content_urls if it exists in alert content (max of 1000). Default: false
fetch_ips	No	boolean	If true returns content_ips if it exists in the alert content (max of 100).

Parameter	Required	Type	Description
highlight	No	boolean	highlight matched text Default: false
aggregate_alert_id	No	integer	aggregate_alert_ID Default: -1 <div style="border: 1px solid black; padding: 5px; background-color: #e1f5fe;">  <p>The aggregate_alert_id value is returned by the endpoint: actionable-alert (get)</p> <p>The value is an integer starting from 0 and incrementing (0,1,2,3,4...).</p> </div>

Request example

```
curl --location --request GET 'https://api.cybersixgill.com/alerts/actionable_alert_content/5fbcfeb23a5ce900013de081' \
--header 'Authorization: Bearer <token>'
```

Responses

Example: Response 200 - Fetch alert content by alert ID.

```
{
  "content": {
    "items": [
      {
        "_id": "1b25dc035688ea6e2c83252f6b7967af",
        "_source": {
          "category": "HOW MUCH BRO ™ ",
          "channel_message_id": 103471,
          "collection_date": "2020-11-24T00:02:03",
          "content": "Daily chat messages from Group: HOW MUCH BRO ™ ",
          "creator": "HOW MUCH BRO ™ ",
          "date": "2020-11-24T00:02:02",

```

Example: Response 200 - Fetch alert content by alert ID.

```
"enrichment_version": 23,
"financial": {
  "iban": []
},
"id": "1b25dc035688ea6e2c83252f6b7967af",
"ips": [],
"lang": "en",
"message_url": "https://t.me/YOUNGBAGGERSG4/103471",
"rep_grade": 1.0,
"site": "telegram",
"site_grade": 5,
"title": "Daily Telegram Group HOW MUCH BRO ™ ",
"type": "topic",
"update_date": "2020-11-24T00:06:00.808189"
}
},
{
  "_id": "7d2bbe565770148236041d5ce7f703d1bf2bf4e7",
  "_source": {
    "category": "HOW MUCH BRO ™ ",
    "channel_message_id": 103726,
    "collection_date": "2020-11-24T11:44:09",
    "content": "message me rather",
    "creator": "Chi~Bo¥™ °(891234274)",
    "date": "2020-11-24T11:44:08",
    "enrichment_version": 23,
    "financial": {
      "iban": []
    },
    "id": "abd52ef0dd4276c1c320a265ee9d235b",
    "images": [],
    "ips": [],
    "lang": "en",
    "message_url": "https://t.me/YOUNGBAGGERSG4/103726",
    "post_id": "1b25dc035688ea6e2c83252f6b7967af",
    "rep_grade": 1.0,
    "site": "telegram",
    "site_grade": 5,
    "sources_author_id": 891234274,
    "title": "Telegram Group HOW MUCH BRO ™ ",
    "type": "chat",
    "update_date": "2020-11-24T11:48:16.730743",
```

Example: Response 200 - Fetch alert content by alert ID.

```
    "username": "Nwokeobioma"
  }
},
{
  "_id": "ac10de1aacd497249a0b86164af8fdf7d3460f98",
  "_source": {
    "category": "HOW MUCH BRO ™ ",
    "channel_message_id": 103727,
    "collection_date": "2020-11-24T12:07:40",
    "company_name": [
      "wells fargo"
    ],
    "content": "CASHAPP DROPS ( 5k and 10k) - $150-200\nNEW SBA SAUCE WITH - $60 comes with free pro and walkthrough Video \n20k Grant Approval link,sauce & walkthrough- $50 ( PRO ONLY NEEDED) \n          Bank Logins Boa, Chase, Wells Fargo - $55 ( shows how to login )",
    "creator": "CryptoKing23(1201313874)",
    "date": "2020-11-24T12:07:39",
    "enrichment_version": 23,
    "financial": {
      "iban": []
    },
    "id": "a3407afc01bd1f83d48a011fd96a2f9a",
    "images": [],
    "ips": [],
    "lang": "en",
    "message_url": "https://t.me/YOUNGBAGGERSG4/103727",
    "post_id": "1b25dc035688ea6e2c83252f6b7967af",
    "rep_grade": 1.0,
    "site": "telegram",
    "site_grade": 5,
    "sources_author_id": 1201313874,
    "tags": [
      "Company_name"
    ],
    "title": "Telegram Group HOW MUCH BRO ™ ",
    "type": "chat",
    "update_date": "2020-11-24T12:10:50.441530",
    "username": "Cryptolowkey23"
  },
  "triggered_alert": true
},...
],
```

Example: Response 200 - Fetch alert content by alert ID.

```
"resultsFrom": 212,  
"total": 556  
},  
"content_type": "search_result_item"  
}
```

Example: Response 403 - Forbidden.

```
{  
  "items_modified_count": 0,  
  "message": "Authorization failure",  
  "status": 403  
}
```

Example: Response 404 - Resource with specified ID was not found.

```
{  
  "items_modified_count": 0,  
  "message": "ActionableAlertContent for alert with ID 5ff538e1fd20cbc15b1ba9b9 not  
found",  
  "status": 404  
}
```

Example: Response 404 - Aggregate alert ID does not exist.

```
{  
  "items_modified_count": 0,  
  "message": "aggregate_alert_id 11 not found",  
  "status": 404  
}
```

alert_type_id/update_alert_frequency (patch)

General

Item	Details
URL	https://api.cybersixgill.com/alerts/alert_type_id/update_alert_frequency
Description	Updates the frequency of an alert type
Method	PATCH

Parameters

Parameter	Required	Type	Description
organization_id	No	string	Organization IDs - required for multi-tenant
alert_type_id	Yes	string	The unique ID of the alert_type
frequency	Yes	string	Available values: ASAP, Daily, Weekly Default value : ASAP

Responses

Example: Response 200 - alert_type_id modified successfully.

```
{
  "items_modified_count": 1,
  "message": "alert_type_id modified successfully to a frequency of 'Weekly'",
  "status": 200
}
```

Example: Response 400 - Bad request.

```
{
  "detail": "'Weekli' is not one of ['ASAP', 'Daily', 'Weekly']\n\nFailed validating 'enum' in\nschema:\n  {'default': 'ASAP',\n   'enum': ['ASAP', 'Daily', 'Weekly'],\n   'in':\n'query',\n  'name': 'frequency',\n  'type': 'string'}\n\nOn instance:\n  'Weekli',\n  "status": 400,
}
```

Example: Response 404 - Not found.

```
{  
  "items_modified_count": 0,  
  "message": "The alert_type_id provided does not exist - 5e0dd67ceea4f445bb15ab5",  
  "status": 404  
}
```

Assets API

The Assets API provides endpoints to manage organization and user data.

The API contains the following endpoints.

Group	Description	Endpoint
Organization Assets	Gets organization assets by organization ID.	/organization assets (get)
	Updates organization assets by organization ID.	/organization assets (put)
	Creates assets for an organization.	/organization assets (post)

organization assets (get)

General

Item	Details
URL	https://api.cybersixgill.com/assets/organization
Description	Gets organization assets by organization ID.
Method	GET

Parameters

Parameter	Required	Type	Description
organization_id	Yes (for multi-tenant)	string	Organization ID (required for multi-tenant)

Responses

Example: Response 200 - Fetch organization assets.

```
{
  "organization_aliases": {
    "automatic": [
      "evil",
      "ev1l"
    ],
    "explicit": [
      "iVl"
    ]
  },
  "domain_names": {
    "automatic": [
      "google.com",
      "microsoft.com"
    ],
    "explicit": [
      "fb.com"
    ]
  },
  "ip_addresses": {
    "automatic": [
      "8.8.8.8",
      "6.6.6.6"
    ],
    "explicit": [
      "1.2.3.4"
    ]
  },
  "products": {
    "automatic": [
      "Vodka",
      "Skype"
    ],
    "explicit": [
      "Pineapples"
    ]
  },
  "executives": {
    "automatic": [
```

```
"John Doe",
"Vasya Pupkin"
],
"explicit": [
"Alice"
]
},
"third_parties": {
"automatic": [
"government",
"people"
],
"explicit": [
"kittens"
]
},
"cves": {
"automatic": [
"CVE-2000-0001"
],
"explicit": [
"CVE-2019-6666"
]
},
"bins": {
"automatic": [
"123456"
],
"explicit": [
"444444"
]
},
"read_only": true
}
```

Example: Response 400 - Bad request.

```
{
"message": "Authentication failure",
"status_code": 401
}
```

Example: Response 401 - User is not authenticated.

```
{  
  "message": "Authentication failure",  
  "status_code": 401  
}
```

Example: Response 403 - User does not have permissions.

```
{  
  "message": "Authentication failure",  
  "status_code": 401  
}
```

Example: Response 404 - Resource with specified ID was not found.

```
{  
  "message": "Authentication failure",  
  "status_code": 401  
}
```

organization assets (put)

General

Item	Details
URL	https://api.cybersixgill.com/assets/organization
Description	Updates organization assets by organization ID.
Method	PUT

Parameters

Parameter	Required	Type	Description
organization_id	Yes	string	Organization ID

Request example

A request body is required.

Example value for organization assets object with modified fields

```
{
  "organization_aliases": {
    "automatic": [
      "evil",
      "ev11"
    ],
    "explicit": [
      "ivl"
    ]
  },
  "domain_names": {
    "automatic": [
      "google.com",
      "microsoft.com"
    ],
    "explicit": [
      "fb.com"
    ]
  },
  "ip_addresses": {
    "automatic": [
      "8.8.8.8",
      "6.6.6.6"
    ],
    "explicit": [
      "1.2.3.4"
    ]
  },
  "products": {
    "automatic": [
      "Vodka",
      "Skype"
    ]
  }
}
```

```
],
  "explicit": [
    "Pineapples"
  ]
},
"executives": {
  "automatic": [
    "John Doe",
    "Vasya Pupkin"
  ],
  "explicit": [
    "Alice"
  ]
},
"third_parties": {
  "automatic": [
    "government",
    "people"
  ],
  "explicit": [
    "kittens"
  ]
},
"cves": {
  "automatic": [
    "CVE-2000-0001"
  ],
  "explicit": [
    "CVE-2019-6666"
  ]
},
"bins": {
  "automatic": [
    "123456"
  ],
  "explicit": [
    "444444"
  ]
},
"read_only": true
}
```

Responses

Example: Response 200 - Fetch organization assets.

```
{
  "items_modified": [
    "id1",
    "id2",
    "id3"
  ],
  "items_modified_count": 20,
  "message": "modified successfully",
  "status_code": 200
}
```

Example: Response 400 - Bad request.

```
{
  "message": "Authentication failure",
  "status_code": 401
}
```

Example: Response 401 - User is not authenticated.

```
{
  "message": "Authentication failure",
  "status_code": 401
}
```

Example: Response 403 - User does not have permissions.

```
{
  "message": "Authentication failure",
  "status_code": 401
}
```

Example: Response 404 - Resource with specified ID was not found.

```
{
  "message": "Authentication failure",
  "status_code": 401
}
```

organization assets (post)

General

Item	Details
URL	https://api.cybersixgill.com/assets/organization
Description	Creates assets for an organization.
Method	POST

Parameters

Parameter	Required	Type	Description
organization_id	Yes	string	Organization ID

Request example

Example value to create organization assets

```
{
  "organization_aliases": [
    "evil",
    "ev1l"
  ],
  "domain_names": [
    "google.com",
    "microsoft.com"
  ],
  "ip_addresses": [
    "8.8.8.8",
    "6.6.6.6"
  ]
}
```

```
],
"products": [
  "Vodka",
  "Skype"
],
"executives": [
  "John Doe",
  "Vasya Pupkin"
],
"third_parties": [
  "goverment",
  "people"
],
"cves": [
  "CVE-2000-0001"
],
"bins": [
  "123456"
],
"source": "explicit"
}
```

Responses

Example: Response 200 - Fetch organization assets after creation.

```
{
  "organization_aliases": {
    "automatic": [
      "evil",
      "ev1l"
    ],
    "explicit": [
      "iVl"
    ]
  },
  "domain_names": {
    "automatic": [
      "google.com",
      "microsoft.com"
    ],
    "explicit": [
```



```
"fb.com"
]
},
"ip_addresses": {
  "automatic": [
    "127.0.0.1",
    "6.6.6.6"
  ],
  "explicit": [
    "1.2.3.4"
  ]
},
"products": {
  "automatic": [
    "Vodka",
    "Skype"
  ],
  "explicit": [
    "Pineapples"
  ]
},
"executives": {
  "automatic": [
    "John Doe",
    "Vasya Pupkin"
  ],
  "explicit": [
    "Alice"
  ]
},
"third_parties": {
  "automatic": [
    "government",
    "people"
  ],
  "explicit": [
    "kittens"
  ]
},
"cves": {
  "automatic": [
    "CVE-2000-0001"
  ],
  "explicit": [
```

```
"CVE-2019-6666"  
  ]  
},  
"bins": {  
  "automatic": [  
    123456  
  ],  
  "explicit": [  
    444444  
  ]  
},  
"read_only": true  
}
```

Example: Response 400 - Bad request.

```
{  
  "message": "Authentication failure",  
  "status_code": 401  
}
```

Example: Response 401 - User is not authenticated.

```
{  
  "message": "Authentication failure",  
  "status_code": 401  
}
```

Example: Response 403 - User does not have permissions.

```
{  
  "message": "Authentication failure",  
  "status_code": 401  
}
```

Credentials API

The Credentials API gets leaked credentials for a specified date range from the Sixgill system.

The API contains the following endpoint:



Group	Description	Endpoint
Credentials	Get leaked credentials for a specified date range from the Sixgill system.	/leaks (get)

leaks (get)

General

Item	Details
URL	https://api.cybersixgill.com/credentials/leaks
Description	Get leaked credentials for a specified date range from the Sixgill system.
Method	GET

Parameters

Parameter	Required	Type	Description
domain	Yes	array [string]	Search for leaks matching this domain  Use only domain or email.
email	Yes	array [string]	Search for leaks matching this email  Use only domain or email.
from_date	No	string	Get credentials leaked after a given date. format is YYYY-MM-DD HH:mm:ss.
to_date	No	string	Get credentials leaked before a given date. format is YYYY-MM-DD HH:mm:ss.
max_results	No	integer	Maximum amount of results that can be returned Default = 100
skip	No	integer	Specifies how many leaked items to skip before displaying results. Default = 100

Example: Response 200 - Fetch result.

```
[
{
  "leaks": [
    {
      "breach_date": "2021-10-07",
      "breach_id": 24346,
      "breach_name": "",
      "description": "Published on paste_justpasteit on 2021-10-06T21:16:09 ....",
      "create_time": "2021-10-07 07:23:47",
      "domain": "test.com",
      "email": "guillaume.XXX@test.com",
      "hash_type": "plain",
      "name": "",
      "login_id": "",
      "password": "guillaume",
      "phone": ""
    },
    {
      "breach_date": "2021-09-19",
      "breach_id": 24097,
      "breach_name": "test.txt",
      "description": "Published on hosting_anonfiles on 2021-09-18T21:16:09, ...",
      "create_time": "2021-09-19 02:38:19",
      "domain": "test.com",
      "email": "missing1@test.com",
      "hash_type": "plain",
      "name": "",
      "login_id": "",
      "password": "tCzcRJ2WGh7Q",
      "phone": ""
    }
  ],
  "total_results": 79342
} ]
```

Response 400 - Bad request.

If a server error 400 with the description **Domains are forbidden** is received, it is possible that the user that sent the request is not authorized to access the API. Please contact the support team for further assistance.

DVE Enrichment API

The DVE enrichment API allows you to request information about specific CVEs, and receive the current snapshot status of those CVEs (what is their rating, are they currently trending/not trending, etc.). The enrichment mode comes in STIX 2.0.

The API contains the following endpoints:

Group	Description	Endpoint
DVE	Enrich CVEs with Cybersixgill intelligence.	/enrich (post)
Enrichment API Calls	Get CVEs that contain a keyword within a specified date range.	/keyword_search (get)
	Get data about a specific CVE.	/{id} (get)
	Get the remediation information for a specific CVE.	/{remediation} (get)
	Get CVEs which affect the CPEs that match specified filters.	/cves_by_cpes (get)

enrich (post)

General

Item	Details
URL	https://api.cybersixgill.com/dve_enrich/enrich
Description	Enrich CVEs with Cybersixgill intelligence.
Method	POST

Parameters

Parameter	Required	Type	Description
data	No	Object	See the request example below for the correct parameter format.

Request Examples

Example 1: CVEs first mentioned between specified dates

Body:

```
{
  "filters": {
    "first_mention_dates_range": {
      "from": "2020-02-18T00:00:00Z",
      "to": "2020-03-18T00:00:00Z"
    }
  },
  "results_size": 5,
  "from_index": 0
}
```

Example 2: Enriching a list of CVEs

Body:

```
{
```



```
"filters": {
  "ids": [
    "CVE-2020-0674"
  ]
},
"results_size": 5,
"from_index": 0
}
```

Example 3: Querying for all CVEs that have at least one PoC exploit

Body:

```
{
  "filters": {
    "attributes": [
      "Has_POC_exploit_attribute"
    ]
  },
  "results_size": 50,
  "from_index": 0
}
```

Example 4: Querying for all CVEs that have a DVE score between 8 and 10

Body:

```
{
  "filters": {
    "sixgill_rating_range": {
      "from": 8,
      "to": 10
    }
  },
  "results_size": 5,
  "from_index": 0
}
```

Example 5: Querying for all CVEs that are associated with ransomware groups

Body:

```
{
  "filters": {
    "attributes": [
      "Is_Related_Ransomware_attribute"
    ]
  },
  "results_size": 10,
  "from_index": 0
}
```

Responses

Example: Response 200 - The requested CVE's data.

```
{
  "id": "bundle--b56c1e2e-a40c-44ca-83dd-09e25936d273",
  "spec_version": "2.0",
  "x_bundle_size": 50,
  "x_total_matches": 100,
  "objects": [
    {
      "id": "vulnerability--c74d4bc9-d184-610a-7e81-66581422a535",
      "description": "A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767.\n",
      "rating": {
        "sixgill": {
          "current": 8.4,
          "highest": {
            "value": 9.2,
            "date": "2020-02-18T00:00:00Z"
          }
        }
      },
      "nvd": {
        "value": 7.6,
        "link": "https://nvd.nist.gov/vuln/detail/CVE-2020-0674",
      }
    }
  ]
}
```

```

    "severity": "HIGH",
    "publishDate": "2020-02-11T22:15:00Z",
    "modifyDate": "2020-02-12T17:53:00Z"
  }
},
"attributes": [
  {
    "name": "TrendingUnderground",
    "first_seen": "2023-02-18T00:00:00Z",
    "value": true,
    "description": "The CVE is trending on the underground"
  }
],
"mentions": {
  "mentions_total": 128,
  "first_mention": "2020-01-18T03:19:46Z",
  "last_mention": "2020-02-17T14:07:15Z"
},
"github": {
  "github_projects": 1,
  "watchersCount": 7,
  "forksCount": 2,
  "activity": {
    "first_date": "2020-01-23T12:30:51Z",
    "last_date": "2020-01-23T12:30:51Z"
  }
},
"topProjects": [
  {
    "link": "https://github.com/binaryfigments/CVE-2020-0674",
    "name": "binaryfigments/CVE-2020-0674"
  }
]
},
"nvd": {
  "baseMetricV2": {},
  "baseMetricV3": {},
  "link": "https://nvd.nist.gov/vuln/detail/CVE-2020-0674",
  "publishDate": "2020-02-11T22:15:00Z",
  "modifyDate": "2020-02-12T17:53:00Z"
},
"mitre": {
  "associated_ttp": [
    {
      "technique_name": "Proxy",

```

```
"technique_id": "T1090",
"sub_technique_name": "Proxy: External Proxy",
"sub_technique_id": "T1090.002",
"tactics": [
  {
    "tactic_name": "Command and Control",
    "tactic_id": "TA0011"
  }
]
}
]
```

Example: Default response 200 - Any response other than the data.

```
{
  "detail": "The server encountered an internal error and was unable to complete your request. Either the server is overloaded or there is an error in the application.",
  "status": 500,
  "title": "Internal Server Error",
  "type": "about:blank"
}
```

keyword_search (get)

General

Item	Details
URL	https://api.cybersixgill.com/dve_enrich/keyword_search
Description	Get CVEs that contain a keyword within a specified date range.
Method	GET

Parameters

Parameter	Required	Type	Description
keyword	Yes	String	The keyword search
lastModifiedStartDate	No	String	Start publish date, in format "%Y-%m-%dT%H:%MZ".
lastModifiedEndDate	No	String	End publish date, in format "%Y-%m-%dT%H:%MZ".

Responses

Example: Response 200 -

The following endpoint receives a search keyword, and returns all CVEs that match the keyword in their content (title, description, references), or CVEs whose CPE information matched the keyword. The resulting dictionary states whether the keyword appeared in the CVE, CPE, or both.

:

```
{
  "CVE-2019-1945": [
    "cve",
    "cpe"
  ],
  "CVE-2020-1122": [
    "cpe"
  ]
}
```

Example: Default response 200 - Any response other than the data.

```
{  
  "detail": "The server encountered an internal error and was unable to complete your  
  request. Either the server is overloaded or there is an error in the application.",  
  "status": 500,  
  "title": "Internal Server Error",  
  "type": "about:blank"  
}
```

{id} (get)

General

Item	Details
URL	https://api.cybersixgill.com/dve_enrich/{id}
Description	Get data about a specific CVE.
Method	GET

Parameters

Parameter	Required	Type	Description
id	Yes	String	CVE ID to use as a filter.

Request Example

```
curl -X GET 'https://api.cybersixgill.com/dve_enrich/CVE-2020-0796' \  
-H 'Content-Type: application/json' \  
-H 'X-Channel-Id: d5cd46c205c20c87006b55a18b106428' \  
-H 'Authorization: Bearer [access_token value]' \  
--data-raw '  
,
```

Responses

Example: Response 200 - The enriched CVE data with first_seen attribute.

```
{  
  "created": "2024-03-12T00:00:00.001000Z",  
  "description": "A improper neutralization of special elements used in an sql command ('sql injection') in Fortinet FortiClientEMS version 7.2.0 through 7.2.2, FortiClientEMS 7.0.1 through 7.0.10 allows attacker to execute unauthorized code or commands via specially crafted packets.",  
  "external_references": [  
    {  
      "external_id": "CVE-2023-48788",  
      "source_name": "cve"  
    }  
  ]  
}
```

```

    }
  ],
  "id": "vulnerability--f98a9252-aa70-ec86-2be2-41eb4ddd8a8d",
  "last_activity_date": "2024-09-02T13:58:21Z",
  "name": "CVE-2023-48788",
  "type": "vulnerability",
  "x_sixgill_info": {
    "affected_packages": [],
    "apts": [
      {
        "associated_country": "Unknown / Unmapped Actors",
        "common_name": "Akira"
      },
      {
        "associated_country": "Russia",
        "common_name": "APT29"
      },
      {
        "associated_country": "China",
        "common_name": "Aquatic Panda"
      },
      {
        "associated_country": "Unknown / Unmapped Actors",
        "common_name": "BianLian"
      },
      {
        "associated_country": "Iran",
        "common_name": "Nemesis Kitten"
      },
      {
        "associated_country": "Unknown / Unmapped Actors",
        "common_name": "Noescape"
      },
      {
        "associated_country": "Other Actors",
        "common_name": "QUILTED TIGER"
      }
    ],
    "apts_count": 30,
    "attributes": [
      {
        "description": "This CVE has at least one published Proof of Concept (POC) exploit.",
        "first_seen": "2024-03-15T04:42:40Z",

```



```
"name": "Has_POC_exploit_attribute",
"value": true
},
{
  "description": "The CVE is part of an at least one exploit kit",
  "name": "Has_Exploit_kit_attribute",
  "value": false
},
...
```

Example: Default response 200 - Any response other than the data.

```
{
  "detail": "The server encountered an internal error and was unable to complete your request. Either the server is overloaded or there is an error in the application.",
  "status": 500,
  "title": "Internal Server Error",
  "type": "about:blank"
}
```

{remediation} (get)

General

Item	Details
URL	https://api.cybersixgill.com/dve_enrich/{id}/remediation
Description	Get the remediation information for a specific CVE.
Method	GET

Parameters

Parameter	Required	Type	Description
id	Yes	String	CVE ID to use as a filter.
iq_remediation	No	Boolean	If true, retrieves detailed remediation steps for specific CVEs, ensuring you have the information needed to mitigate vulnerabilities effectively.

Request Example

```
curl -X GET 'https://api.cybersixgill.com/dve_enrich/CVE-2023-48788/remediation?iq_remediation=true' \
--data "ids": "CVE-2020-0674"
-H 'Content-Type: application/json' \
-H 'X-Channel-Id: d5cd46c205c20c87006b55a18b106428' \
-H 'Authorization: Bearer [access_token value]' \
--data-raw '
'
```

Responses

Example: Response 200 - The requested CVE's remedy.

```
[ { "advisory": "cybersixgill_iq", "description": "N/A", "solutions": "To remediate or fix CVE-2023-48788, you should follow these steps:\n\n1. Update Fortinet FortiClientEMS to the latest version available. Check the Fortinet website or contact their support for information on the latest patches or updates.\n\n2. Apply any available security patches or updates provided by Fortinet specifically addressing the SQL injection vulnerability associated with CVE-2023-48788.\n\n3. Regularly monitor for any new updates or patches released by Fortinet and promptly apply them to ensure the security of your FortiClientEMS installation.\n\n4. Implement secure coding practices and input validation techniques to prevent SQL injection attacks. This may involve reviewing and modifying the codebase of your application to properly sanitize and validate user input before executing SQL queries.\n\n5. Consider implementing a web application firewall (WAF) or intrusion detection/prevention system (IDS/IPS) to detect and block SQL injection attempts.\n\n6. Educate your users and administrators about the risks of SQL injection attacks and the importance of following secure coding practices.\n\nIt is always recommended to consult with Fortinet or a qualified security professional for specific guidance tailored to your environment and to ensure the proper remediation of CVE-2023-48788." } ]
```

cves_by_cpes (get)

General

Item	Details
URL	https://api.cybersixgill.com/dve_enrich/cves_by_cpes
Description	Get CVEs which affect the CPEs that match specified filters.
Method	GET

Parameters

Parameter	Required	Type	Description
enriched	No	Boolean	Whether to return just the IDs of the matching CVEs or to enrich them. Default value: true
results_size	No	Integer	The number of CVEs to return (maximum of 10). Default value: 10
from_index	No	Integer	The number of CVEs to skip on return (allows pagination). Default value: 0
vendor	Yes	String	The vendor of the CPEs to match.
product	Yes	String	The product of the CPEs to match.
part	No	String	The part of the CPEs to match.
version	No	String	The version of the CPEs to match.
update	No	String	The update of the CPEs to match.
edition	No	String	The edition of the CPEs to match.
language	No	String	The language of the CPEs to match.
sw_edition	No	String	The sw_edition of the CPEs to match.
target_software	No	String	The target_software of the CPEs to match.
target_hardware	No	String	The target_hardware of the CPEs to match.
other	No	String	The other of the CPEs to match.

Responses

Example: Response 200 - A list of enriched CVEs which are related to CPEs that match the filters.

```
[
  {
    "id": "CVE-2020-0674",
    "score": {
      "sixgill": {
        "highest": {
          "value": 8.4
        }
      }
    }
  }
]
```

Example: Default response 200 - Any response other than the data.

```
{
  "detail": "The server encountered an internal error and was unable to complete your request. Either the server is overloaded or there is an error in the application.",
  "status": 500,
  "title": "Internal Server Error",
  "type": "about:blank"
}
```

DVE Feed API

Cybersixgill's Dynamic Vulnerability Exploit (DVE) feed provides an ongoing stream of CVE intelligence events as they occur. The feed comes in STIX 2.0 format for easy ingestion.

The API contains the following endpoints:

Group	Description	Endpoint	Method
DVE	Consume DVE feed.	/ioc (DVE Feed)	GET
	Acknowledge consumed DVEs.	/ioc/ack (DVE Feed)	POST

ioc (DVE Feed)

General

Item	Details
URL	https://api.cybersixgill.com/dvefeed/ioc
Description	Get a bundle of DVE feed events in STIX2 format.
Method	GET

Parameters

Parameter	Required	Type	Description
limit	No	Integer	Amount of DVE feed events to consume. Default: 100
X-Channel-Id	Yes	String	Consumer channel of DVE feed. Use the following ID: d5cd46c205c20c87006b55a18b106428

Request example

```
change endpoint
curl --location --request GET 'https://api.cybersixgill.com/dvefeed/ioc' \
--header 'Content-Type: application/json' \
--header 'Cache-Control: no-cache' \
--header 'X-Channel-Id: d5cd46c205c20c87006b55a18b106428' \
--header 'Authorization: Bearer <access token>'
```

Responses

Example: Response 200 - Successfully fetched DVE bundle.

```
{
  "id": "bundle--b56c1e2e-a40c-44ca-83dd-09e25936d273",
  "objects": [
    {
      "created": "2019-05-01T06:13:14.000Z",
```

```
"description": "this is the description",
"id": "example--1",
"modified": "2019-05-08T03:43:44.000Z",
"name": "simple name",
"type": "example",
"additionalProp1": {}
}
],
"spec_version": "2.0",
"type": "bundle"
}
```

Example: Response 403 - Request not authorized.

```
{
  "status_code": 403,
  "message": "Not authorized"
}
```


ioc/ack (DVE Feed)

General

Item	Details
URL	https://api.cybersixgill.com/dvefeed/ioc/ack
Description	Acknowledge bulk of consumed DVEs.
Method	POST

Parameters

Parameter	Required	Type	Description
X-Channel-Id	Yes	String	Consumer channel of the DVE feed. Use the following ID: d5cd46c205c20c87006b55a18b106428

Request Example

```
curl --location --request POST 'https://api.cybersixgill.com/dvefeed/ioc/ack' \  
--header 'Content-Type: application/json' \  
--header 'Cache-Control: no-cache' \  
--header 'X-Channel-Id: d5cd46c205c20c87006b55a18b106428' \  
--header 'Authorization: Bearer <access token>'
```

Responses

Example: Response 200 - Number of successfully-acknowledged DVEs

```
2
```

Example: Response 403 - Request not authorized.

```
{
```

Example: Response 403 - Request not authorized.

```
"status_code": 403,  
"message": "Not authorized"  
}
```

Dark Feed API

Darkfeed is a feed of malicious indicators of compromise, including domains, URLs, hashes, and IP addresses.



Please make sure to include the X-Channel-id:
d5cd46c205c20c87006b55a18b106428 as mentioned below.

Group	Description	Endpoint	Method
IOC	Get a bundle of IOCs in STIX2 format.	/ioc (Dark Feed)	GET
	Acknowledge consumed IOCs.	/ioc/ack (Dark Feed)	POST

ioc (Dark Feed)

General

Item	Details
URL	https://api.cybersixgill.com/darkfeed/ioc
Description	Get a bundle of IOC items in STIX2 format.
Method	GET

Parameters

Parameter	Required	Type	Description
X-Channel-Id	Yes	string	IOC consumer channel. Use the following value: d5cd46c205c20c87006b55a18b106428
limit	No	integer	Amount of IOCs to consume. Default = 100



After each run of the **ioc** endpoint, run the **ioc/ack (Dark Feed)** endpoint to acknowledge you consumed a bundle (as set by the limit parameter) of IOC items. In this way, the next time you run the **ioc** endpoint, the next bundle of IOC items will be returned.

Request example

```
curl -X GET 'https://api.cybersixgill.com/darkfeed/ioc?limit=10' \  
-H "Authorization: Bearer [access_token value]" \  
-H "X-Channel-Id: d5cd46c205c20c87006b55a18b106428'
```

Responses

Example: Response 200 - Successfully fetched IOC bundle.


```
{
  "id": "bundle--b56c1e2e-a40c-44ca-83dd-09e25936d273",
  "objects": [
    {
      "created": "2019-05-01T06:13:14.000Z",
      "description": "this is the description",
      "id": "example--1",
      "modified": "2019-05-08T03:43:44.000Z",
      "name": "simple name",
      "type": "example",
      "additionalProp1": {}
    }
  ],
  "spec_version": "2.0",
  "type": "bundle"
}
```

Example: Response 403 - Request not authorized.

```
{
  "status_code": 403,
  "message": "Not authorized"
}
```

ioc/ack (Dark Feed)

General

Item	Details
URL	https://api.cybersixgill.com/darkfeed/ioc/ack
Description	<p>Acknowledges that you consumed a bundle of IOC items after running the ioc (Dark Feed) endpoint.</p> <div style="border: 1px solid black; background-color: #e1f5fe; padding: 10px;"> After each run of the ioc (Dark Feed) endpoint, run the ioc/ack endpoint to acknowledge you consumed a bundle (as set by the ioc endpoint limit parameter) of IOC items. In this way, the next time you run the ioc endpoint, the next bundle of IOC items will be returned.</div>
Method	POST

Parameters

Parameter	Required	Type	Description
X-Channel-Id	Yes	string	IOC consumer channel. Use the following value: d5cd46c205c20c87006b55a18b106428

Request example

```
curl -X POST 'https://api.cybersixgill.com/darkfeed/ioc/ack \  
-H "Authorization: Bearer [access_token value]" \  
-H "X-Channel-Id: d5cd46c205c20c87006b55a18b106428'
```

Responses

Example: Response 200 - Number of successfully acknowledged IOCs

```
2
```

Example: Response 403 - Request not authorized.

```
{  
  "status_code": 403,  
  "message": "Not authorized"  
}
```

Dark Feed Enrichment API

The Dark Feed Enrichment API provides endpoints for obtaining detailed information on IOCs (indicators of compromise).

The endpoint also allows you to enrich data based on two additional pivot points: actor name and post ID (i.e. getting all IOCs from a specific thread from an underground source).

The API contains the following endpoints:

Group	Description	Endpoint	Method
IOC Enrichment	Get items in STIX format related to the specified IOC.	/ioc/enrich (post)	POST

ioc/enrich (post)

General

Item	Details
URL	https://api.cybersixgill.com/ioc/enrich
Description	Get items in STIX format related to the specified IOC.
Method	POST

Parameters

Parameter	Required	Type	Description
X-Channel-Id	Yes	string	IOC consumer channel.

You can define the following optional parameters in the request:

Parameter	Type	Description
ioc_type	string	An array that can contain [ip, domain, url, hash]. Specify the value for these types in the sixgill_field_value parameter.
ioc_value	string	IOC items containing the value you specify here for the ioc_type parameter.
limit	integer	The number of IOC items to return. Default: 50 Minimum: 1
sixgill_field	string	Either of the following Cybersixgill fields: <ul style="list-style-type: none">> actor> post_id Specify the value for this field in the sixgill_field_value parameter.

Parameter	Type	Description
sixgill_field_value	string	IOC items containing the value you specify here for the sixgill_field parameter.
skip	integer	Specifies how many IOC items to skip before displaying results. For example, skip: 200 displays the 201th item and forward (till the limit is reached). Default: 0 (displays from the first item)

Request example using IOC enrichment

```
curl --location --request POST 'https://api.cybersixgill.com/ioc/enrich' \
--header 'Content-Type: application/json' \
--header 'Cache-Control: no-cache' \
--header 'X-Channel-Id: d5cd46c205c20c87006b55a18b106428' \
--header 'Authorization: <token>' \
--data-raw '{
  "ioc_type": "ip",
  "ioc_value": "190.2.31.172",
  "limit": 50,
  "skip": 0
}'
```

Request example using "sixgill_field"

```
curl --location --request POST 'https://api.cybersixgill.com/ioc/enrich' \
--header 'Content-Type: application/json' \
--header 'Cache-Control: no-cache' \
--header 'X-Channel-Id: d5cd46c205c20c87006b55a18b106428' \
--header 'Authorization: Bearer <token>' \
--data-raw '{
  "sixgill_field": "post_id",
  "sixgill_field_value": "459ef8c762fa6c34e19031141642e9097f43a405",
  "limit": 50,
  "skip": 0
}'
```

Responses

Example: Response 200 - Number of successfully acknowledged IOCs.

```
{
  "items": [
    {
      "created": "2019-05-01T06:13:14.000Z",
      "description": "this is the description",
      "id": "example--1",
      "modified": "2019-05-08T03:43:44.000Z",
      "name": "simple name",
      "type": "example",
      "additionalProp1": {}
    }
  ],
  "total": 1
}
```

Example: Response 403 - Request not authorized.

```
{
  "status_code": 403,
  "message": "Not authorized"
}
```

Example: Response 404 - Entered input is invalid.

```
{
  "message": "Invalid input",
  "status_code": 404
}
```

Events Feed API

The Events Feed API provides endpoints to consume event items.



Please make sure to include the X-Channel-id:
d5cd46c205c20c87006b55a18b106428 as mentioned below.

Group	Description	Endpoint	Method
Events Feed	Get a bundle of events items.	/_events_feed (get)	GET
	Acknowledges that you consumed a bundle of events items after running the Events feed (Cybersixgill Pulse) endpoint.	/events_feed/ack (post)	POST

events_feed (get)

General

Cybersixgill PulseTBD

Item	Details
URL	https://api.cybersixgill.com/events_feed
Description	Get a bundle of events items
Method	GET

Parameters

Parameter	Required	Type	Description
X-Channel-Id	Yes	string	Events feed consumer channel.
limit	No	Integer	Number of events to consume. Default = 100



After each run of **events_feed**, run [events_feed/ack \(post\)](#) to acknowledge you consumed a bundle of events items (as set by the limit parameter).
In this way, the next time you run **events_feed**, the next bundle of events items will be returned.

Request example

```
curl -X POST 'https://api.cybersixgill.com/events_feed?limit=100 \
-H "Authorization: Bearer [access_token value]" \
-H "X-Channel-Id: d5cd46c205c20c87006b55a18b106428'
```

Example: Response 200 – Successfully fetched events bundle.

```
{
```

Example: Response 200 – Successfully fetched events bundle.

```
"total_items": 100,
"objects": [
  {
    "id": "N2HIko8BrIIDbz7Kkcw6",
    "event_domain": "Cyber News",
    "entities": {
      "domains": [
        "theregister.com"
      ]
    },
    "intel_item_id": "7b7340c96714be5408866f0be472b2842bbce441",
    "summary": "Joe Biden spends more on Facebook and Instagram ads than Donald Trump, but ads attacking the US president outnumber those attacking his likely rival in this year's presidential election, according to data analysis. The research project is led by Professor Jennifer Stromer-Galley, senior associate dean at Syracuse University's School of Information Studies, who has researched presidential campaigning in the internet age from 1996 to 2016.",
    "actor": "Lindsay Clark",
    "site": "cybernews_theregister",
    "event_creation_date": "2024-05-19T21:36:09.014899",
    "collection_date": "2024-05-19T17:43:43",
    "intel_item_date": "2024-05-17T19:29:00",
    "event": "Biden outspends Trump in social media ad war",
    "topic_category": "Industry news",
    "substance": "news",
    "organizations": [
      "Neo4j",
      "Syracuse University's Institute for Democracy, Journalism and Citizenship (IDJC)"
    ],
    "products": [
      "Facebook",
      "Instagram",
      "Neo4j"
    ],
    "sector": [
      "Education"
    ],
    "individuals": [
      "Joe Biden",
      "Donald Trump",
      "Professor Jennifer Stromer-Galley"
    ],
  },
]
```

Example: Response 200 – Successfully fetched events bundle.

```
"tags": [
  "Biden",
  "Trump",
  "Social Media",
  "Neo4j",
  "Syracuse University"
]
},
{
  "id": "8kM-k48BmCDGGZFP5e1k",
  "event_domain": "Cyber News",
  "entities": {
    "malware": [
      "onion",
      "medusalocker",
      "medusa",
      "wildfire",
      "defender"
    ],
    "ransomware": [],
    "apt": [
      "medusa ransomware gang",
      "medusa"
    ],
    "cves": [],
    "domains": [
      "paloaltonetworks.com",
      "winitor.com",
      "thedfirreport.com",
      "github.com",
      "malwarebytes.com",
      "bleepingcomputer.com",
      "crn.com",
      "microsoft.com",
      "securityscorecard.com",
      "paloaltonetworks.jp",
      "safengine.com",
      "filemail.com",
      "cyberthreatalliance.org",
      "virusotal.com",
      "cisa.gov"
    ]
  },
}
```

Example: Response 200 – Successfully fetched events bundle.

```
"hash": {
  "md5": [],
  "sha1": [],
  "sha256": [
    "7d68da8aa78929bb467682ddb080e750ed07cd21b1ee7a9f38cf2810eeb
9cb95",
    "9144a60ac86d4c91f7553768d9bef848acd3bd9fe3e599b7ea2024a8a31
15669",
    "4d4df87cf8d8551d836f67fbde4337863bac3ff6b5cb324675054ea023b1
2ab6",
    "736de79e0a2d08156bae608b2a3e63336829d59d38d61907642149a566
ebd270",
    "657c0cce98d6e73e53b4001eeee51ed91fdcf3d47a18712b6ba9c66d596
77980"
  ]
},
"ips": []
},
"intel_item_id": "68406f581e8777fb61dcd780738ce3055d00b571",
"summary": "Unit 42 Threat Intelligence analysts have noticed an escalation in
Medusa ransomware activities and a shift in tactics toward extortion, characterized by
the introduction in early 2023 of their dedicated leak site called the Medusa Blog.
Medusa threat actors use this site to disclose sensitive data from victims unwilling to
comply with their ransom demands. The article provides a detailed technical analysis of
the Medusa ransomware group's tactics, tools, and procedures, as well as
recommendations for protections and mitigations.",
"actor": "Anthony Galiette,Doel Santos",
"site": "blog_paloaltounit42",
"event_creation_date": "2024-05-19T23:45:23.808478",
"collection_date": "2024-05-19T18:10:47",
"intel_item_date": "2024-01-11T14:00:00",
"event": "Medusa Ransomware Turning Your Files into Stone",
"topic_category": "Ransomware",
"substance": "analysis/commentary",
"organizations": [
  "Palo Alto Networks"
],
"products": [
  "Cortex XDR",
  "WildFire",
  "Cloud-Delivered Security Services",
  "Next-Generation Firewall",
  "Prisma Cloud",
  "Cortex Xpanse"
```


Example: Response 200 – Successfully fetched events bundle.

```
],  
  "tags": [  
    "Medusa ransomware",  
    "ransomware group",  
    "cybersecurity",  
    "data breach",  
    "extortion"  
  ]  
},
```

Example: Response 403 - Request not authorized.

```
{  
  "status_code": 403,  
  "message": "Not authorized"  
}
```

events_feed/ack (post)

General

Cybersixgill PulseTBD

Item	Details
URL	https://api.cybersixgill.com/events_feed/ack
Description	Acknowledges that you consumed a bundle of events items after running the Events feed (Cybersixgill Pulse) endpoint.
Method	POST

Parameters

Parameter	Required	Type	Description
X-Channel-Id	Yes	string	Events feed consumer channel.



After each run of [events_feed \(get\)](#), run **events_feed/ack** to acknowledge you consumed a bundle of events items (as set by the [events_feed \(get\)](#) limit parameter).

In this way, the next time you run [events_feed \(get\)](#), the next bundle of events items will be returned.

Request example

```
curl -X POST 'https://api.cybersixgill.com/events_feed/ack \  
-H "Authorization: Bearer [access_token value]" \  
-H "X-Channel-Id: d5cd46c205c20c87006b55a18b106428'
```

Example: Response 200 - Number of successfully acknowledged events.

```
2
```

Example: Response 403 - Request not authorized.

```
{  
  "status_code": 403,  
  "message": "Not authorized"  
}
```

Intel Items API

The Intel Items API provides endpoints for obtaining detailed information on intel items, aggregations of intel items, and histograms based on a date range from the Cybersixgill system.

The API contains the following endpoints:

Group	Description	Endpoint	Method
Aggregations	Get aggregation of intel items	/aggs (post)	POST
Intel Items	Get intel items - advanced variation	/intel_items (post)	POST
	Get a list of intel items based on a search query.	/intel_items (get)	GET
	Gets the next batch of intel items	/intel_items/next	POST
	Get a thread page content	/intel_items/{id}/thread	GET
	Get the next batch of intel items related to a thread.	/intel_items/thread/next	POST
	Get an intel item	/intel_items/{id}	GET
Histogram	Get date histogram of intel items	/histogram (post)	POST

aggs (post)


General

Item	Details
URL	https://api.cybersixgill.com/intel/aggs
Description	Get an aggregation of intel items based on a given query and field. The aggregation of intel items are returned as a list of intel items in the given field, sorted from high to low. The number of results can be set as a parameter (default is 10 results).
Method	POST

Parameters

No parameters

A request body is required and you can define the following parameters in the request.

Parameter	Required	Type	Description
field	Yes	string	The field for the aggregation. Available values include tags, actor, site, category, type, and language
query	Yes	string	<p>A search query for requesting data.</p> <div style="border: 1px solid black; padding: 10px; background-color: #e1f5fe;"> <p> The query string is case-INsensitive. In the following examples, the result will be the same.</p> <p><u>Example 1</u></p> <pre style="background-color: #f5f5f5; padding: 5px;">{"query": "actor:Moot", "results_size": 400, }</pre> <p><u>Example 2</u></p> <pre style="background-color: #f5f5f5; padding: 5px;">{"query": "actor:mOOt", "results_size": 400, }</pre> <p><u>Example 3</u></p> <pre style="background-color: #f5f5f5; padding: 5px;">{"query": "actor:moot", "results_size": 400, }</pre> </div>
date_range	No	string	<p>items that were collected between two dates (UTC). The date_range format can be either:</p> <ul style="list-style-type: none"> > YYYY-MM-DD HH:mm:ss TO YYYY-MM-DD HH:mm:ss > YYYY-MM-DD HH TO now (default)

Parameter	Required	Type	Description
filters	No	JSON dictionary	Options for filtering a query. Filter parameter contains one or more keys (name of parameter such as tags, actor, site, category, type, and language) and their value.
results_size	No	integer	The amount of items in the aggregation field. Each field item in the aggregation includes an occurrence count. Default = 10



A filter used in the body of a POST is case sensitive. For example, using an actor filter "JOHN" and an actor filter "john" will give different results.

Request example

```
curl -X POST "https://api.cybersixgill.com/intel/aggs" \
-H "Authorization: Bearer [access_token value]" \
-H "accept: application/json" \
-H "Content-Type: application/json" -d \
{"query":"cyber","date_range":"2019-01-01 TO 2020-10-20","filters":{"site":["sixgill","twitter"],"actor":["John Doe"]},"field":"tags","results_size":10}
```

Responses

Example: Response 200 - Data fetched successfully

```
{
  "field": "tags",
  "intel_items_count": 100,
  "aggregations": [
    {
      "key": "drugs",
      "intel_items_count": 60
    },
    {
      "key": "malware",
```

```
"intel_items_count": 40
}
]
}
```

Example: Response 400 - Bad parameters.

```
{
  "status_code": 400,
  "message": "Bad Parameters: query"
}
```


intel_items (post)


General


Item	Details
URL	https://api.cybersixgill.com/intel/intel_items
Description	Get a list of intel_items
Method	POST

Parameters

No parameters

A request body is required and you can define the following parameters in the request.

Parameter	Required	Type	Description
query	Yes	string	<p>A search query for requesting data.</p> <div style="border: 1px solid black; padding: 10px; background-color: #e1f5fe;">  <p>The query string is case-INsensitive. In the following examples, the result will be the same.</p> <p><u>Example 1</u></p> <pre> {"query": "actor:Moot", "results_size": 400, } </pre> <p><u>Example 2</u></p> <pre> {"query": "actor:m00t", "results_size": 400, } </pre> <p><u>Example 3</u></p> <pre> {"query": "actor:moot", "results_size": 400, } </pre> </div>
date_range	No	string	<p>Items that were collected between two dates (UTC). The date_range format can be either:</p> <ul style="list-style-type: none"> > YYYY-MM-DD HH:mm:ss TO YYYY-MM-DD HH:mm:ss > YYYY-MM-DD HH:mm:ss TO now (default)
filters	No	JSON dictionary	<p>Options for filtering a query. The filters parameter contains one or more keys (name of parameter such as tags, actor, site, category, type, and language) and their value.</p>

Parameter	Required	Type	Description
highlight	No	boolean	<ul style="list-style-type: none"> > true - highlight the query string in the results. > false (default) - do not highlight the query string in the results.
module	No	string	<p>Sets the scope for the search. Available values:</p> <ul style="list-style-type: none"> > cti > osint <p>Default value: cti</p> <div style="border: 1px solid black; background-color: #e1f5fe; padding: 5px; margin-top: 10px;">  The values are non-exclusive and are lowercase letters. </div>
partial_content	No	boolean	<ul style="list-style-type: none"> > true (default)- response will contain only 400 characters relating to the content. > false - complete content is fetched.
results_size	No	integer	<p>The amount of items in the aggregation field. Each field item in the aggregation includes an occurrence count.</p> <p>Default = 50</p>
scroll	No	boolean	<ul style="list-style-type: none"> > true - return a scroll_id so that you can further filter the data fetched by this endpoint. The scroll_id is used as a value in the intel_items/next > false (default) - no scroll_id is returned.

Parameter	Required	Type	Description
sort	No	string	Sort the results by the field specified, such as: <ul style="list-style-type: none"> > date (default) > title > actor > site > type > sixgill_rank > reputation > replies
sort_type	No	string	Sets the sort order for the fetched results: <ul style="list-style-type: none"> > desc (default) - descending > asc - ascending



A filter used in the body of a POST is case sensitive. For example, using an actor filter "JOHN" and an actor filter "john" will give different results.

Request example

```
curl -X POST "https://api.cybersixgill.com/intel/intel_items" \
-H "Authorization: Bearer [access_token value]" \
-H "accept: application/json" \
-H "Content-Type: application/json" \
-d "{\"query\": \"cyber\", \"date_range\": \"2019-01-01 TO 2020-10-20\", \"partial_content\": true, \"results_size\": 100, \"scroll\": false, \"sort\": \"date\", \"sort_type\": \"desc\", \"highlight\": false, \"filters\": { \"site\": [ \"sixgill\", \"twitter\" ], \"actor\": [ \"John Doe\" ] } }"
```

Responses

Example: Response 200 - Data fetched successfully.



Some items (such as CC) return additional information specifically related to the item, as shown in the example below.

```
{
  "scroll_id":
  "DXF1ZXJ5QW5kRmV0Y2gBAAAAAAWGXMWLWNBZXN5M2ISTEsxbm1FMGxvVIJL
  QQ==",
  "intel_items": [
    {
      "category": "Leaks",
      "cc": {
        "bin": "557111",
        "city": "Kielce",
        "zip": "25-135",
        "bank_name": "Akbank T.a.s.",
        "dob": "string",
        "country": "TUR",
        "price": "$35.00",
        "address": "5-48",
        "card_type": "Akbank T.a.s. credit",
        "phone": "4455...",
        "state": "Akbank T.a.s.null",
        "card_subtype": "Standard",
        "category": "cvv2",
        "country_original": "Turkey",
        "email": "yes",
        "cardholder_name": "John"
      },
      "sub_category": "Cracked Programs, Malicious Software",
      "collection_date": "2019-12-18T15:51:21",
      "content": "content...@sixgill-start-highlight@<highlited_text>@sixgill-end-
      highlight@content continue...",
      "comments_count": 7,
      "actor": "mryang",
      "date": "2019-12-18T15:51:21",
      "id": "339ff5af35b8aaeeda40c5f09f6fe1bd",
      "images": [
```

```

{
  "key": "forum_community/59b2ccded71fcfdb473233a1319098f3.jpg",
  "metadata": {},
  "pos": 140,
  "safe_search": {
    "adult": 1,
    "medical": "1s",
    "spoon": 1,
    "violence": 1
  },
  "size": {
    "height": 85,
    "width": 320
  },
  "text": "OCR text..."
}
"intel_id":
"dGVsZWdyYW1fMzM5ZmY1YWYzNWl4YWFIZWRhNDBjNWYwOWY2ZmUxYmQ="
],
"language": "English",
"post_id": "4129addef3160b4021bbff662d7a2a1a",
"site": "forum_community",
"title": "title...",
"type": "post",
"tags": [
  "Hacking",
  "Malware"
],
"url": "https://site_url/..."
}
],
"total_intel_items": 100
}

```

Example: Response 400 - Bad parameters.

```

{
  "status_code": 400,
  "message": "Bad Parameters: query"
}

```

intel_items (get)

General

Item	Details
URL	https://api.cybersixgill.com/intel/intel_items?query=[query details]
Description	Get a list of intel_items based on a search query.
Method	GET

Parameters

Parameter	Required	Type	Description
query	Yes	string	A search query for requesting data.
results_size	No	integer	The amount of items in the aggregation field. Each field item in the aggregation includes an occurrence count. Default = 50
highlight	No	boolean	> true - highlight the query string in the results. > false (default) - do not highlight the query string in the results.
custom_highlight_start_tag	No	string	Choose which text will mark the start of a highlighted. default - @sixgill-start-highlight@
custom_highlight_end_tag	No	string	Choose which text will mark the end of a highlighted text. default - @sixgill-end-highlight@
recent_items	No	boolean	If set to true retrieve data from last 2 days. Default: false

Request example

```
curl -X GET "https://api.cybersixgill.com/intel/intel_
items?query=actor%3Djohn&results_size=50&highlight=true" \
-H "Authorization: Bearer [access_token value]" \
-H "accept: application/json"
```

Responses

Example: Response 200 - Data fetched successfully.



Some items (such as CC) return additional information specifically related to the item, as shown in the example below.

```
{
  "total_intel_items": 100,
  "intel_items": [
    {
      "category": "Leaks",
      "cc": {
        "bin": 557111,
        "city": "Kielce",
        "zip": "25-135",
        "bank_name": "Akbank T.a.s.",
        "dob": "string",
        "country": "TUR",
        "price": "$35.00",
        "address": "5-48",
        "card_type": "Akbank T.a.s. credit",
        "phone": "4455...",
        "state": "Akbank T.a.s.null",
        "card_subtype": "Standard",
        "category": "cvv2",
        "country_original": "Turkey",
        "email": "yes",
        "cardholder_name": "John"
      },
      "sub_category": "Cracked Programs, Malicious Software",
      "collection_date": "2019-12-18T15:51:21",
    }
  ]
}
```



```

"content": "content...@sixgill-start-highlight@<highlited_text>@sixgill-end-
highlight@content continue...",
"comments_count": 7,
"actor": "mryang",
"date": "2019-12-18T15:51:21",
"id": "339ff5af35b8aaeeda40c5f09f6fe1bd",
"images": [
  {
    "key": "forum_community/59b2ccded71fcfdb473233a1319098f3.jpg",
    "metadata": {},
    "pos": 140,
    "safe_search": {
      "adult": 1,
      "medical": "1s",
      "spooof": 1,
      "violence": 1
    },
    "size": {
      "height": 85,
      "width": 320
    },
    "text": "OCR text..."
  }
]
"intel_id":
"dGVsZWdyYW1fMzM5ZmY1YWYzNWl4YWFIZWRhNDBjNWYwOWY2ZmUxYmQ=",
],
"language": "English",
"post_id": "4129addef3160b4021bbff662d7a2a1a",
"site": "forum_community",
"title": "title...",
"type": "post",
"tags": [
  "Hacking",
  "Malware"
],
"url": "https://site_url/..."
}
]
}

```

Example: Response 400 - Bad parameters.

```
{  
  "status_code": 400,  
  "message": "Bad Parameters: query"  
}
```

intel_items/next

General

Item	Details
URL	https://api.cybersixgill.com/intel/intel_items/next
Description	Get the next batch of intel items based on a scroll_id. See intel_items (post)
Method	POST

Parameters

No parameters

A request body is required and you can define the following parameters in the request.

Parameter	Required	Type	Description
scroll_id	Yes	string	The scroll_id returned from intel_items (post)

Request example

```
curl -X POST "https://api.cybersixgill.com/intel/intel_items/next" \  
-H "Authorization: Bearer [access_token value]" \  
-H "accept: application/json" \  
-H "Content-Type: application/json" \  
-d "{\"scroll_\  
id\": \"DXF1ZXJ5QW5kRmV0Y2gBAAAAAAWGXMWLWNBZXN5M2lSTEsbm1FMGxv\  
VJLQQ==\"}"
```

Responses

Example: Response 200 - Data fetched successfully.



Some items (such as CC) return additional information specifically related to the item, as shown in the example below.

```
{
  "scroll_id": "DXF1ZXJ5QW5kRmV0Y2gBAAAAAAWGXMWLWNBZXN5M2ISTE
  sxbm1FMGxvVIJLQQ==",
  "total_intel_items": 100,
  "intel_items": [
    {
      "category": "Leaks",
      "cc": {
        "bin": 557111,
        "city": "Kielce",
        "zip": "25-135",
        "bank_name": "Akbank T.a.s.",
        "dob": "string",
        "country": "TUR",
        "price": "$35.00",
        "address": "5-48",
        "card_type": "Akbank T.a.s. credit",
        "phone": "4455...",
        "state": "Akbank T.a.s.null",
        "card_subtype": "Standard",
        "category": "cvv2",
        "country_original": "Turkey",
        "email": "yes",
        "cardholder_name": "John"
      },
      "sub_category": "Cracked Programs, Malicious Software",
      "collection_date": "2019-12-18T15:51:21",
      "comments_count": 7,
      "content": "content...@sixgill-start-highlight@<highlited_text>@sixgill-end-
      highlight@content continue...",
      "actor": "mryang",
      "date": "2019-12-18T15:51:21",
      "id": "339ff5af35b8aaeeda40c5f09f6fe1bd",
      "images": [
```

```
{
  "key": "forum_community/59b2ccded71fcfdb473233a1319098f3.jpg",
  "metadata": {},
  "pos": 140,
  "safe_search": {
    "adult": 1,
    "medical": 1,
    "spoon": 1,
    "violence": 1
  },
  "size": {
    "height": 85,
    "width": 320
  },
  "text": "OCR text..."
}
],
"language": "English",
"post_id": "4129addef3160b4021bbff662d7a2a1a",
"site": "forum_community",
"title": "title...",
"type": "post",
"tags": [
  "Hacking",
  "Malware"
],
"url": "https://site_url/..."
}
]
```

Example: Response 400 - Bad parameters.

```
{
  "status_code": 400,
  "message": "Bad Parameters: query"
}
```

intel_items/{id}/thread

General

Item	Details
URL	https://api.cybersixgill.com/intel/intel_items/{intel item ID}/thread
Description	Get the thread page content of a specific intel item for an item id. A thread can include posts, products, and replies.
Method	GET

Parameters

Parameter	Required	Type	Description
id	Yes	string	Required intel item ID.
thread_site	Yes	string	Name of the thread site.
results_size	No	integer	Maximum number of intel_items in the result (main_ post + replies). Default = 300
highlight_query	No	string	A query for highlighting terms in the intel_items results
custom_highlight_start_tag	No	string	Choose which text will mark the start of a highlighted text. default - @sixgill-start-highlight@
custom_highlight_end_tag	No	string	Choose which text will mark the end of a highlighted text. default - @sixgill-end-highlight@
scroll	No	boolean	> true - return a scroll_id so that you can further filter the data fetched by this endpoint. The scroll_id is used as a value in the intel_items/thread/next > false (default) - no scroll_id is returned.

Parameter	Required	Type	Description
split_to_parts	No	boolean	When set to true, the content will be split to chunks.
recent_items	No	boolean	If set to true retrieve data from last 2 days. Default: false

Request example

```
curl -X GET "https://api.cybersixgill.com/intel/intel_
items//4129addef3160b4021bbff662d7a2a1a/thread?thread_site=forum_
cyber&results_size=100&scroll=true" \
-H "Authorization: Bearer [access_token value]" \
-H "accept: application/json"
```

Responses

Example: Response 200 - Data fetched successfully.



Some items (such as CC) return additional information specifically related to the item, as shown in the example below.

```
{
  "main_post": {
    "id": "0635f980c64bc23970ff20613e3a4caf5f77519e",
    "category": "Cyber attacks",
    "sub_category": "Phishing",
    "content": "Content_here",
    "actor": "Anonymous",
    "date": "2018-07-20T18:36:00",
    "language": "English",
    "site": "forum_sixgill",
    "site_grade": 5,
    "subject": "How to make money",
    "type": "post",
    "url": "https://....",
    "images": [
      {
        "key": "forum_community/59b2ccded71fcfdb473233a1319098f3.jpg",
```

```

"metadata": {},
"pos": 140,
"safe_search": {
  "adult": 1,
  "medical": 1,
  "spoof": 1,
  "violence": 1
},
"size": {
  "height": 85,
  "width": 320
},
"text": "OCR text..."
}
]
},
"replies": [
{
  "_id": "11233169",
  "content": "reply content here",
  "actor": "user1",
  "date": "2018-07-20T18:38:00",
  "depth": null,
  "language": "English",
  "site": "forum_sixgill",
  "type": "reply"
},
{
  "_id": "11233171",
  "content": "reply content here",
  "actor": "user2",
  "date": "2018-07-20T18:39:00",
  "depth": null,
  "language": "English",
  "site": "forum_sixgill",
  "type": "reply"
}
],
"total": 8
}

```


Example: Response 400 - Bad parameters.

```
{  
  "status_code": 400,  
  "message": "Bad Parameters: query"  
}
```

intel_items/thread/next

General

Item	Details
URL	https://api.cybersixgill.com/intel/intel_items/thread/next
Description	Get the next batch of intel items related to the thread based on a scroll_id. See intel_items/next
Method	POST

Parameters

A request body is required and you can define the following parameters in the request.

Parameter	Required	Type	Description
scroll_id	Yes	string	The scroll_id returned from intel_items/{id}/thread
split_to_parts	No	boolean	When set to true, the content will be split to chunks
custom_highlight_start_tag	No	string	Choose which text will mark the start of an highlighted text. default - @sixgill-start-highlight@
custom_highlight_end_tag	No	string	Choose which text will mark the end of an highlighted text. default - @sixgill-end-highlight@
recent_items	No	boolean	If set to true retrieve data from last 2 days. Default: false

Request example

```
curl -X POST "https://api.cybersixgill.com/intel/intel_items/thread/next" /
-H "Authorization: Bearer [access_token value]" /
-H "accept: application/json" /
-H "Content-Type: application/json" -d "{\"scroll_
id\": \"DXF1ZXJ5QW5kRmV0Y2gBAAAAAAWGXMWLWNBZXN5M2lSTEsbm1FMGxv
VJLQQ==\"}"
```

Responses

Example: Response 200 - Data fetched successfully.



Some items (such as CC) return additional information specifically related to the item, as shown in the example below.

```
{
  "replies": [
    {
      "_id": "11233169",
      "content": "reply content here",
      "actor": "user1",
      "date": "2018-07-20T18:38:00",
      "depth": null,
      "language": "English",
      "site": "forum_sixgill",
      "type": "reply"
    },
    {
      "_id": "11233171",
      "content": "reply content here",
      "actor": "user2",
      "date": "2018-07-20T18:39:00",
      "depth": null,
      "language": "English",
      "site": "forum_sixgill",
      "type": "reply"
    }
  ],
  "scroll_id": "DXF1ZXJ5QW5kRmV0Y2gBAAAAAAWGXMWLWNBZXN5M2ISTE
  sxbm1FMGxvVIJLQQ=="
}
```

Example: Response 400 - Bad parameters.

```
{
  "status_code": 400,
  "message": "Bad Parameters: query"
}
```


intel_items/{id}

General

Item	Details
URL	https://api.cybersixgill.com/intel/intel_items/intel_id
Description	Get detailed information for a specific intel_item based on the intel item's ID
Method	GET

Parameters

Parameter	Required	Type	Description
id	Yes	string	The ID of the intel item

 To get faster search results, use the intel_id value.

Request example

```
curl -X GET "https://api.cybersixgill.com/intel/intel_items/12345" \  
-H "Authorization: Bearer [access_token value]" \  
-H "accept: application/json"
```

Responses

Example: Response 200 - OK.

```
{  
  "category": "Leaks",  
  "cc": {  
    "bin": 557111,  
    "city": "Kielce",  
    "zip": "25-135",
```

```
"bank_name": "Akbank T.a.s.",
"dob": "string",
"country": "TUR",
"price": "$35.00",
"address": "5-48",
"card_type": "Akbank T.a.s. credit",
"phone": "4455...",
"state": "Akbank T.a.s.null",
"card_subtype": "Standard",
"category": "cvv2",
"country_original": "Turkey",
"email": "yes",
"cardholder_name": "John"
},
"sub_category": "Cracked Programs, Malicious Software",
"collection_date": "2019-12-18T15:51:21",
"comments_count": 7,
"content": "content...@sixgill-start-highlight@<highlited_text>@sixgill-end-
highlight@content
continue...",
"actor": "mryang",
"date": "2019-12-18T15:51:21",
"id": "339ff5af35b8aaeeda40c5f09f6fe1bd",
"images": [
{
"key": "forum_community/59b2ccded71fcfdb473233a1319098f3.jpg",
"metadata": {},
"pos": 140,
"safe_search": {
"adult": 1,
"medical": 1,
"spooof": 1,
"violence": 1
},
"size": {
"height": 85,
"width": 320
},
"text": "OCR text..."
}
]
"intel_id":
"dGVsZWdyYW1fMzM5ZmY1YWYzNWl4YWFIZWRhNDBjNWYwOWY2ZmUxYmQ=",
],
"language": "English",
```

```
"post_id": "4129addef3160b4021bbff662d7a2a1a",
"site": "forum_community",
"title": "title...",
"type": "post",
"tags": [
  "Hacking",
  "Malware"
],
"url": "https://site_url/..."
}
```

Example: Response 400 - Bad parameters.

```
{
  "status_code": 400,
  "message": "Bad Parameters: query"
}
```

histogram (post)


General

Item	Details
URL	https://api.cybersixgill.com/intel/histogram
Description	Get a date histogram of intel item query results. The histogram is a graph depicting the amount of intel items for a given interval.
Method	POST

Parameters

Parameter	Required	Type	Description
interval	Yes	string	The time interval for the histogram.

A request body is required and you can define the following parameters in the request.

Parameter	Required	Type	Description
query	Yes	string	<p>A search query for requesting data.</p> <div style="border: 1px solid black; padding: 10px; background-color: #e6f2ff;"> <p> The query string is case-INsensitive. In the following examples, the result will be the same.</p> <p><u>Example 1</u></p> <pre style="background-color: #f0f0f0; padding: 5px;">{"query": "actor:Moot", "results_size": 400, }</pre> <p><u>Example 2</u></p> <pre style="background-color: #f0f0f0; padding: 5px;">{"query": "actor:m00t", "results_size": 400, }</pre> <p><u>Example 3</u></p> <pre style="background-color: #f0f0f0; padding: 5px;">{"query": "actor:moot", "results_size": 400, }</pre> </div>
date_range	No	string	<p>Items that were collected between two dates (UTC). The date_range format can be either:</p> <ul style="list-style-type: none"> > YYYY-MM-DD HH:mm:ss TO YYYY-MM-DD HH:mm:ss > YYYY-MM-DD HH:mm:ss TO now.

Parameter	Required	Type	Description
filters	No	JSON dictionary	Options for filtering a query. The filters parameter contains one or more keys (name of parameter such as tags, actor, site, category, type, and language) and their value.
results_size	No	integer	The amount of items in the aggregation field. Each field item in the aggregation includes an occurrence count.



A filter used in the body of a POST is case sensitive. For example, using an actor filter "JOHN" and an actor filter "john" will give different results.

Request example

```
curl -X POST "https://api.cybersixgill.com/intel/histogram" \
-H "Authorization: Bearer [access_token value]" \
-H "accept: application/json" \
-H "Content-Type: application/json" \
-d "{\"query\": \"cyber\", \"date_range\": \"2019-01-01 TO 2020-10-20\", \"filters\": {\"site\": [\"sixgill\", \"twitter\"], \"actor\": [\"John Doe\"]}, \"interval\": \"month\"}"
```

Responses

Example: Response 200 - OK.

```
{
  "field": "tags",
  "intel_items_count": 100,
  "aggregations": [
    {
      "key": "drugs",
      "intel_items_count": 60
    },
    {
      "key": "malware",
```

```
"intel_items_count": 40
}
]
```

Example: Response 400 - Bad parameters.

```
{
  "status_code": 400,
  "message": "Bad Parameters: query"
}
```

Multi-Tenancy API

The Multi-Tenancy API provides endpoints for use with the multi-tenant (MSSP) platform.



The Multi-Tenancy API endpoints are located in the "Organizations and Users API" section of the API Gallery.

The API contains the following endpoints.

Group	Description	Endpoint
Organization	Creates an organization.	/organization (post)
	Gets a list of organizations.	/organization (get)
	Deletes an organization by ID.	/organization (delete)
Organization Assets	Creates assets for an organization.	/organization assets (post)
	Gets organization assets by organization ID.	/organization assets (get)
	Updates organization assets by organization ID.	/organization assets (put)
User Role in Organization	Gets a list of users with roles by organization ID.	/organization/{organization_id}/user (get)
	Assigns the user to the organization with a given role.	/organization/{organization_id}/user/{assigned_user_id} (post)
	Gets user roles by organization ID.	/organization/{organization_id}/user/{assigned_user_id} (get)
	Assigns the user a new role in the organization.	/organization/{organization_id}/user/{assigned_user_id} (put)
	Deletes the user's assignment to the organization.	/organization/{organization_id}/user/{assigned_user_id} (delete)

organization (post)

General

Item	Details
URL	https://api.cybersixgill.com/multi-tenant/organization
Description	Creates an organization.
Method	POST

Parameters

Parameter	Required	Type	Description
organization	No	object	Organization object to create.

Example value

```
{
  "name": "Bank of Atlantis",
  "organization_commercial_category": "customer",
  "countries": [
    "Canada"
  ],
  "industries": [
    "Healthcare",
    "Logistics"
  ]
}
```

Responses

Example: Response 200 - Fetch organization after creation.

```
{
  "id": "5bf6c3900310e92553ca60cb",
  "name": "Bank of Atlantis",
  "organization_commercial_category": "customer",
  "organization_type": "managed",
}
```

```
"countries": [  
  "Canada"  
],  
"industries": [  
  "Healthcare",  
  "Logistics"  
]  
}
```

Example: Response 401 - User is not authenticated.

```
{  
  "message": "Authentication failure",  
  "status_code": 401  
}
```

organization (get)

General

Item	Details
URL	https://api.cybersixgill.com/multi-tenant/organization
Description	Gets a list of organizations.
Method	GET

Parameters

Parameter	Required	Type	Description
organization_name	No	string	Optional filters <ul style="list-style-type: none">> name of organization> part of a name

Responses

Example: Response 200 - Fetch organizations.

```
[
  {
    "id": "5bf6c3900310e92553ca60cb",
    "name": "Bank of Atlantis",
    "organization_commercial_category": "customer",
    "organization_type": "managed",
    "countries": [
      "Canada"
    ],
    "industries": [
      "Healthcare",
      "Logistics"
    ]
  }
]
```

Example: Response 401 - User is not authenticated.

```
{  
  "message": "Authentication failure",  
  "status_code": 401  
}
```

organization (delete)

General

Item	Details
URL	https://api.cybersixgill.com/multi-tenant/organization/{organization_id}
Description	Deletes an organization by ID.
Method	DELETE

Parameters

Parameter	Required	Type	Description
organization_id	Yes	string	Organization ID

Responses

Example: Response 200 - Fetch result of organization removal.

```
{
  "items_modified": [
    "id1",
    "id2",
    "id3"
  ],
  "items_modified_count": 20,
  "message": "modified successfully",
  "status_code": 200
}
```


organization assets (post)

General

Item	Details
URL	https://api.cybersixgill.com/multi-tenant/organization/{organization_id}/assets
Description	Creates assets for an organization.
Method	POST



Use this POST API endpoint to create the assets for an organization for the first time.
To update organization assets use a PUT API endpoint, [organization assets \(put\)](#).

Parameters

Parameter	Required	Type	Description
organization_id	Yes	string	Organization ID
assets	No	object	Organization assets object to create.

Example value for assets

```
{
  "organization_aliases": [
    "evil",
    "ev11"
  ],
  "domain_names": [
    "google.com",
    "microsoft.com"
  ],
  "ip_addresses": [
    "127.0.0.1",
    "6.6.6.6"
  ],
}
```

```
"products": [
  "Vodka",
  "Skype"
],
"executives": [
  "John Doe",
  "Vasya Pupkin"
],
"third_parties": [
  "government",
  "people"
],
"cves": [
  "CVE-2000-0001"
],
"bins": [
  123456
],
"source": "explicit"
}
```

Responses

Example: Response 200 - Fetch organization assets after creation.

```
{
  "organization_aliases": {
    "automatic": [
      "evil",
      "ev11"
    ],
    "explicit": [
      "ivl"
    ]
  },
  "domain_names": {
    "automatic": [
      "google.com",
      "microsoft.com"
    ],
    "explicit": [
      "fb.com"
    ]
  }
}
```

```
]
},
"ip_addresses": {
  "automatic": [
    "127.0.0.1",
    "6.6.6.6"
  ],
  "explicit": [
    "1.2.3.4"
  ]
},
"products": {
  "automatic": [
    "Vodka",
    "Skype"
  ],
  "explicit": [
    "Pineapples"
  ]
},
"executives": {
  "automatic": [
    "John Doe",
    "Vasya Pupkin"
  ],
  "explicit": [
    "Alice"
  ]
},
"third_parties": {
  "automatic": [
    "government",
    "people"
  ],
  "explicit": [
    "kittens"
  ]
},
"cvcs": {
  "automatic": [
    "CVE-2000-0001"
  ],
  "explicit": [
    "CVE-2019-6666"
  ]
}
```

```
]
},
"bins": {
  "automatic": [
    123456
  ],
  "explicit": [
    444444
  ]
},
"read_only": true
}
```

Example: Response 401 - User is not authenticated.

```
{
  "message": "Authentication failure",
  "status_code": 401
}
```

organization assets (get)

General

Item	Details
URL	https://api.cybersixgill.com/multi-tenant/organization/{organization_id}/assets
Description	Gets organization assets by organization ID.
Method	GET

Parameters

Parameter	Required	Type	Description
organization_id	Yes	string	Organization ID

Responses

Example: Response 200 - Fetch organization assets.

```
{
  "organization_aliases": {
    "automatic": [
      "evil",
      "ev1l"
    ],
    "explicit": [
      "ivl"
    ]
  },
  "domain_names": {
    "automatic": [
      "google.com",
      "microsoft.com"
    ],
    "explicit": [
      "fb.com"
    ]
  }
}
```

```
"ip_addresses": {
  "automatic": [
    "127.0.0.1",
    "6.6.6.6"
  ],
  "explicit": [
    "1.2.3.4"
  ]
},
"products": {
  "automatic": [
    "Vodka",
    "Skype"
  ],
  "explicit": [
    "Pineapples"
  ]
},
"executives": {
  "automatic": [
    "John Doe",
    "Vasya Pupkin"
  ],
  "explicit": [
    "Alice"
  ]
},
"third_parties": {
  "automatic": [
    "government",
    "people"
  ],
  "explicit": [
    "kittens"
  ]
},
"cves": {
  "automatic": [
    "CVE-2000-0001"
  ],
  "explicit": [
    "CVE-2019-6666"
  ]
},
}
```

```
"bins": {
  "automatic": [
    123456
  ],
  "explicit": [
    444444
  ]
},
"read_only": true
}
```

Example: Response 401 - User is not authenticated.

```
{
  "message": "Authentication failure",
  "status_code": 401
}
```

organization assets (put)

General

Item	Details
URL	https://api.cybersixgill.com/multi-tenant/organization /{organization_id}/assets
Description	<p>Updates organization assets by organization ID.</p> <p>This call replaces the content of the existing assets. Note that the "automatic" section refers to assets discovered by Cybersixgill's automatic attack surface scan mechanism (optional service), and if updated, replaces the existing list, with items not included entering an "excluded" state. Explicit refers to assets that you have explicitly defined as relevant to the organization on your own.</p> <p>Sending assets in the "automatic" section that are not there to begin with will result in an error response.</p>
Method	PUT



Use this PUT API endpoint to update the assets for an organization. Use the POST API endpoint to create the assets for an organization for the first time, [organization assets \(post\)](#).

Parameters

Parameter	Required	Type	Description
assets	Yes	object	Organization assets object with modified fields.
organization_id	Yes	string	Organization ID

Example value for assets

```
{  
  "organization_aliases": {
```



```
"automatic": [
  "evil",
  "ev1l"
],
"explicit": [
  "ivl"
]
},
"domain_names": {
  "automatic": [
    "google.com",
    "microsoft.com"
  ],
  "explicit": [
    "fb.com"
  ]
},
"ip_addresses": {
  "automatic": [
    "127.0.0.1",
    "6.6.6.6"
  ],
  "explicit": [
    "1.2.3.4"
  ]
},
"products": {
  "automatic": [
    "Vodka",
    "Skype"
  ],
  "explicit": [
    "Pineapples"
  ]
},
"executives": {
  "automatic": [
    "John Doe",
    "Vasya Pupkin"
  ],
  "explicit": [
    "Alice"
  ]
},
}
```

```
"third_parties": {
  "automatic": [
    "government",
    "people"
  ],
  "explicit": [
    "kittens"
  ]
},
"cves": {
  "automatic": [
    "CVE-2000-0001"
  ],
  "explicit": [
    "CVE-2019-6666"
  ]
},
"bins": {
  "automatic": [
    123456
  ],
  "explicit": [
    444444
  ]
},
"read_only": true
}
```

Responses

Example: Response 200 - Fetch organization assets.

```
{
  "items_modified": [
    "id1",
    "id2",
    "id3"
  ],
  "items_modified_count": 20,
  "message": "modified successfully",
  "status_code": 200
}
```

Example: Response 401 - User is not authenticated.

```
{  
  "message": "Authentication failure",  
  "status_code": 401  
}
```

organization/{organization_id}/user (get)

General

Item	Details
URL	https://api.cybersixgill.com/multi-tenant/organization/{organization_id}/user
Description	Gets a list of users with roles by organization ID. Use this with your managing organization's ID to get a list of your users and their IDs.
Method	GET

Parameters

Parameter	Required	Type	Description
organization_id	Yes	string	Organization ID

Responses

Example: Response 200 - Fetch list of assigned users.

```
[
  {
    "user_id": "aaa111bbb222ccc333ddd444",
    "user_name": "John Doe",
    "user_email": "john@doe.com",
    "role_id": "5d23342df5feaf006a8a8929",
    "role_name": "viewer"
  }
]
```

Example: Response 401 - User is not authenticated.

```
{
  "message": "Authentication failure",
  "status_code": 401
}
```


organization/{organization_id}/user/{assigned_user_id} (post)

General

Item	Details
URL	https://api.cybersixgill.com/multi-tenant/organization/{organization_id}/user/{assigned_user_id}?role_id={assigned_role_id }
Description	Assigns the user to the organization with a given role. Use for a managed/tracked organization.
Method	POST

Parameters

Parameter	Required	Type	Description
assigned_user_id	Yes	string	User ID
organization_id	Yes	string	Organization ID
role_id	Yes	string	For each user type use the following value: <ul style="list-style-type: none">> Viewer: 5d23342df5feaf006a8a8929> Analyst: 5d23342df5feaf006a8a8928> Owner: 5d23342df5feaf006a8a8927

 The role_id must be added as a parameter to the URL.

Responses

Example: Response 200 - Fetch result of assigning user.

```
{
  "user_id": "aaa111bbb222ccc333ddd444",
  "user_name": "John Doe",
```

```
"user_email": "john@doe.com",  
"role_id": "5d23342df5feaf006a8a8929",  
"role_name": "viewer"  
}
```

Example: Response 401 - User is not authenticated.

```
{  
  "message": "Authentication failure",  
  "status_code": 401  
}
```

organization/{organization_id}/user/{assigned_user_id} (get)

General

Item	Details
URL	https://api.cybersixgill.com/multi-tenant/organization/{organization_id}/user/{assigned_user_id}
Description	Gets user with roles by organization ID. Use for a managed/tracked organization.
Method	GET

Parameters

Parameter	Required	Type	Description
assigned_user_id	Yes	string	User ID
organization_id	Yes	string	Organization ID

Responses

Example: Response 200 - Fetch list of assigned_user.

```
{
  "user_id": "aaa111bbb222ccc333ddd444",
  "user_name": "John Doe",
  "user_email": "john@doe.com",
  "role_id": "5d23342df5feaf006a8a8929",
  "role_name": "viewer"
}
```

Example: Response 401 - User is not authenticated.

```
{
  "message": "Authentication failure",
  "status_code": 401
}
```


organization/{organization_id}/user/{assigned_user_id} (put)

General

Item	Details
URL	https://api.cybersixgill.com/multi-tenant/organization/{organization_id}/user/{assigned_user_id}?new_role_id={assigned_new_role_id }
Description	Assigns the user a new role in the organization. Use for a managed/tracked organization.
Method	PUT

Parameters

Parameter	Required	Type	Description
assigned_user_id	Yes	string	User ID
new_role_id	Yes	string	For each user type use the following value: <ul style="list-style-type: none">> Viewer: 5d23342df5feaf006a8a8929> Analyst: 5d23342df5feaf006a8a8928> Owner: 5d23342df5feaf006a8a8927
organization_id	Yes	string	Organization ID

 The new_role_id must be added as a parameter to the URL.

Responses

Example: Response 200 - Fetch assigned user update result.

```
{
  "items_modified": [
    "id1",
    "id2",
    "id3"
  ],
  "items_modified_count": 20,
  "message": "modified successfully",
  "status_code": 200
}
```

Example: Response 401 - User is not authenticated.

```
{
  "message": "Authentication failure",
  "status_code": 401
}
```

organization/{organization_id}/user/{assigned_user_id} (delete)

General

Item	Details
URL	https://api.cybersixgill.com/multi-tenant/organization/{organization_id}/user/{assigned_user_id}
Description	Deletes the user's assignment to the organization. Use for a managed/tracked organization.
Method	DELETE

Parameters

Parameter	Required	Type	Description
assigned_user_id	Yes	string	User ID
organization_id	Yes	string	Organization ID

Responses

Example: Response 200 - Fetch assigned user removal result.

```
{
  "items_modified": [
    "id1",
    "id2",
    "id3"
  ],
  "items_modified_count": 20,
  "message": "modified successfully",
  "status_code": 200
}
```

Example: Response 401 - User is not authenticated.

```
{
```

Example: Response 401 - User is not authenticated.

```
"message": "Authentication failure",  
"status_code": 401  
}
```

Appendix A - How to Query

Building Cybersixgill Search Queries

You can search using simple and advanced queries and subqueries. Queries use operators and filters to complete the required syntax.

- > **Simple queries** use only keywords. For example, search for "Fraud" OR "European Union".
- > **Advanced queries** use combinations of keywords to include specific results and exclude others. Advanced queries use fields, operators, and subqueries, in addition to keywords.
- > **Operators** include Booleans combining search terms and special characters to further refine queries. Use operators to target combinations of keywords. For example, search for underground activity whose title contains "Fraud" OR "European Union". See [Using Operators in Queries](#).
- > **Filters** identify parts of posts, including post titles, content, and dates. Use filters to target specific values. For example, search for underground content whose title contains "Fraud". See [Using Filters in Queries](#).
- > **Subqueries** are queries combining two or more queries into one search. Use subqueries to build complex searches. For example, search for "Fraud" in titles, but only underground activity in the date range of January 1, 2016 to December 31, 2016, and excluding activity containing "European Union" in the date range January 1, 2016 to January 31, 2016. For examples, see [Using Subqueries in Queries](#).

The following tables give full instructions and examples on how to query