Mandiant

THREAT INTELLIGENCE API V3

Introduction

The Intel APIv3 provides machine-to-machine integration with Mandiant's contextually rich threat intelligence. The Intel APIv3 offers the following:

- Access to indicators of compromise (IOCs) such as IP addresses, domain names, and hashes through the indicators endpoint
- Access to full-length finished intelligence in the reports endpoint
- Search capabilities for intelligence on the adversary with the search endpoint that will further enrich customer knowledge.

The Intel APIv3 is based on the OASIS Structured Threat Information Expression (**STIX**™) version 2.1 industry standard. STIX defines a language for expressing observable cyber threat information for exchange in a simple, scalable manner through a RESTful API and set of resource definitions. For additional information on STIX, see **STIX Introduction (https://oasis-open.github.io/cti-documentation/stix/intro)**.

For a deep dive into the STIX v2.1 standard, see the **STIX 2.1 specification (https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html)**.

For technical support including requests for APIv3 keys, contact **Support (https://docs.mandiant.com/home/mandiant-support-cases)**.

Intel APIv3 Endpoints

There are currently six endpoints on APIv3, some of which are collections while others are endpoints to interact with the APIv3 such as search and permissions.

Endpoint	Endpoint URL	Description	Is_collection?
Collections	**https://api.intelligence.mandiant.com/collections**	Description and technical data for collections	No
Reports	**https://api.intelligence.mandiant.com/collections/reports**	STIX 2.1, HTML, and PDF finished intelligence reports	**Yes**
Indicators	**https://api.intelligence.mandiant.com/collections/indicators**	STIX 2.1 indicators & observables	**Yes**
Search	**https://api.intelligence.mandiant.com/collections/search**	Threat Intelligence search endpoint	No

Authentication

Mandiant's Intel APIv3 uses the **OAuth 2.0 Authorization Framework (https://tools.ietf.org/html/rfc6749)**, with the **client credentials (https://tools.ietf.org/html/rfc6749#section-4.4)** grant to access APIv3 endpoints. Use the public key and private key client credentials to authenticate and receive a time-limited access token. This is accomplished by making a POST request to the Intel API /token endpoint, using HTTP Basic Authentication, as described in **Section 4.4 of RFC 6749 (https://tools.ietf.org/html/rfc6749#section-4.4)**.

Use the following code to authenticate with the Intel APIv3:

```
import requests
import json
from requests.auth import HTTPBasicAuth
APIv3_key='publickey'
APIv3_secret='privatekey'
API_URL = 'https://api.intelligence.mandiant.com/token'
headers = {
   'grant_type': 'client_credentials'
   }
r = requests.post(API_URL, auth=HTTPBasicAuth(APIv3_key, APIv3_secret), data=headers)
data = r.json()
auth_token = data.get('access_token')
print('Token request API response: %s' % r.status_code)
print('Authorization Token: %s' % auth_token)
```

If successful, the APIv3 responds with a JSON body containing the access token, the token type, and the expiration time expressed in seconds. Unless the token has been revoked, it may be used until it expires (generally 12 hours), after which you must authenticate to receive a new token.

Successful token APIv3 response:

```
{
 "access_token": "15d1814233c9e742342338576d39543c38c434b76f70f60041a81d0769fe2c42",
 "token_type": "bearer",
 "expires_in": 43200
}
```

Development Quick Starts

- **Intel APIv3 base url**: `https://api.intelligence.mandiant.com`
- **Obtain your Intel APIv3 Keys:** Contact **Support (https://docs.mandiant.com/home/mandiant-support-cases).**
- **Intel APIv3 token url**: `https://api.intelligence.mandiant.com/token`
- **Get a token from the Intel APIv3:** To make your first API call to the Intel APIv3, you must first authenticate with your APIv3 credentials at the Intel API token URL.

```
import requests
url = "https://api.intelligence.mandiant.com/collections/indicators/objects?added_after=1573491899"
payload = {}
headers = {
 'Accept': 'application/vnd.oasis.stix+json; version=2.1',
 'X-App-Name': '',
 'Authorization': 'Bearer {Your OAuth2 token here}'

}
response = requests.request("GET", url, headers=headers, data = payload)
print(response.text.encode('utf8'))
```

You must insert a valid `X-App-Name` string in your APIv3 calls and update the token value `{Your OAuth2 token here}` in the code with your received token.

- **Read the Pagination** section for the Intel APIv3 to understand how to set the length of objects returned and identify how to page the response.

- **Read the Collections section** to understand which Intel APIv3 endpoint provides what.
- **Read the query parameters for each collection** for filtering of the Intel APIv3 endpoints so you can make more effective and precise APIv3 calls.

Core Concepts

The following topics are fundamental to working with the Intel APIv3.

Typical APIv3 Interaction

End users typically interact with the Intel APIv3 by first obtaining a token from the token endpoint. You can then use a filter to grab Intel from a specific endpoint. One example would be retrieving indicators in the last 24 hours by using the `added_after` filter with the indicators endpoint. Doing so retrieves a bundle of STIX 2.1 indicators in a paged APIv3 response that can then be parsed using open source tools. For more information, see **STIX2 Python Docs (https://stix2.readthedocs.io/en/latest/)** or **cti-stix2-python (https://github.com/oasis-open/cti-python-stix2)**.

To populate a threat intelligence platform, you should look to consume both the indicators collection endpoint and the reports collection endpoint. Together, these provide both the indicator relationships and the report context relationships.

X-App-Name

The Mandiant Intel APIv3 uses the header variable **X-App-Name** for customers and partners to set a user-agent on all of their APIv3 calls. This **mandatory** field is typically a combination of the customer or partners organization name, its application name, and its version. A typical customer X-App-Name would be **'indicators.script.xyzcompany.v1.0'** or similar. The X-App-Name for *customers* should, at a minimum, have the calling organization name. For *partners*, it's required to have the company product name and version of the integration for troubleshooting purposes.

The X-App-Name variable is not required when calling the token endpoint, but it's required when calling all other APIv3 endpoints.

```
import requests
url = "https://api.intelligence.mandiant.com/collections/indicators/objects?added_after=1573491899"
payload = {}
headers = {
  'Accept': 'application/vnd.oasis.stix+json; version=2.1',
  'X-App-Name': '',
  'Authorization': 'Bearer {Your OAuth2 token here}'
}
response = requests.request("GET", url, headers=headers, data = payload)
print(response.text.encode('utf8'))
```

You must set an `X-App-Name` variable per the listed requirements, otherwise you will receive an APIv3 response denying your request.

Request Headers

The Intel APIv3 supports requests for token endpoint headers and general endpoint headers.

- **Token Endpoint Headers**

`GET https://api.intelligence.mandiant.com/token`

Header Key	Header Value	Required
grant_type	client_credentials	Yes

- Sample Token Header call:

```
import requests
import json
from requests.auth import HTTPBasicAuth
APIv3_key='publickey'
APIv3_secret='privatekey'
API_URL = 'https://api.intelligence.mandiant.com/token'
headers = {
   'grant_type': 'client_credentials'
   }
r = requests.post(API_URL, auth=HTTPBasicAuth(APIv3_key, APIv3_secret), data=headers)
data = r.json()
auth_token = data.get('access_token')
print('Token request API response: %s' % r.status_code)
print('Authorization Token: %s' % auth_token)
```

- **General endpoint headers**

Header Key	Header Value	Required
Accept	application/vnd.oasis.stix+json; version=2.1	Yes
X-App-Name	{your app name here}	Yes
Authorization	Bearer {your received token here}	Yes

Rate Limiting

By default, the Intel APIv3 is rate limited to **50,000** queries per day, and **1000** queries per second.

> The preferred interaction with the Intel APIv3 is to download the required reports and indicators periodically (such as daily) and then perform a local, filtered lookup. Implementing a system where your tools perform ad hoc remote API lookups is far less efficient.

Length

To avoid rate limiting issues, widen the limit/length parameter in APIv3 queries to ensure that you receive the maximum amount of data per query.

> Length is a single integer value that indicates the maximum number of objects that the client would like to receive in a single response. If not specified, the default value is 50 and a maximum value of 1000. If the value of length is set to more than 1000, then only 1000 records will be returned.

API Query	Description
`https://api.intelligence.mandiant.com/collections/indicators/objects?added_after=1580600436&length=1000`	Query collections for new objects from February 1, 2020 and return 1000 objects in the response.

```
import requests
url = "https://api.intelligence.mandiant.com/collections/indicators/objects?added_after=1580764458&length=1000"
payload = {}
headers = {
  'Accept': 'application/stix+json; version=2.1',
  'X-App-Name': '',
  'Authorization': 'Bearer {Your OAuth2 token here}'
}
response = requests.request("GET", url, headers=headers, data = payload)
print(response.text.encode('utf8'))
```

Pagination - Collections

The Mandiant Intelligence APIv3 supports pagination of large result sets on endpoints. These endpoints return results sorted in ascending order by the date they were added to the collection. The server may limit the number of responses in response to a query. This could result from a server-specified limit or in response to a length parameter passed by the client as part of a query. The **length** parameter can be used to specify the number of objects to be returned in a single page. The maximum allowed is **length=1000 for the indicator collection**, and a maximum of **length=100 on the reports collection.**

```
while(True):
      r = requests.get(queryURL, headers=headers)
      if r.status_code == 204:
         logging.info('API Status Code: {0} No Content Available for this timeframe.'.format(r.status_code))
         break
      if r.status_code !=200:
         logging.error('API Status Code: {0} Error Reason: {1}'.format(r.status_code, r.text))
         break
      if r.status_code == 200:
         (parse successfull API response...)
         try:
            queryURL = r.links['next']['url']
         except KeyError:
            break
```

If more objects are available, the response header will contain an HTTP Link entity. This may occur either because you limited them by using the length parameter or because the APIv3 limited the response.

The HTTP Link entity-header provides a URL to the next page for results. The link to get the next set of data is set in the response header in the **"Link"** field. The URL before **"rel=next"** represented the next set of data, and the URL before **"rel=first"** will return the first page of data.

> In the URL, `lastidmodified_timestamp` is NOT the exact epoch timestamp and is a base64-encoded string the internal server uses for pagination.

The following table represents a sample output from the response header for the original call to the indicators collection using the added_after query parameter. Since this call represents more than one page of information, the Link response header is returned along with the **['next']['url'].** This shows you what to call next.

KEY	VALUE
Content-Type	application/stix+json; version=2.1
Content-Length	881399
Connection	keep-alive
Date	Mon, 10 Feb 2020 21:44:30 GMT
x-amzn-RequestId	b3769082-a4f9-4796-8922-dbb50afb61c9
x-amz-apigw-id	Hs06CGLPoAMFliQ=
Link	<https://api.intelligence.mandiant.com/collections/indicators/objects?length=1000&last_id_modified_timestamp=MTU4MDgwOTIxOTcyODY0NixpbmRpY2F0b3ItLTA5MWI3OWQxLTllOWQtNWExYS04ODMzLTZlNTkyZmNjMmM1NQ%3D%3D&added_after=1580764458>; rel=next, <https://api.intelligence.mandiant.com/collections/indicators/objects?length=1000&added_after=1580764458>; rel=first
X-Amzn-Trace-Id	Root=1-5e41cea6-ef2d4440f5b33f60f43c5ac0;Sampled=0
X-Cache	Miss from cloudfront
Via	1.1 56d3604ac04bb426a5e942749eccab1a.cloudfront.net (CloudFront)
X-Amz-Cf-Pop	LAX3-C4
X-Amz-Cf-Id	Fd_tjsEX4MgOrrwIZFMUA67h9NHPxj-GfZRnLsN9N5JWkxtFhJg3FA==

Pagination - Search

See Limit and Offset in the following search query. The limit maximum integer value can be 50 and the offset increments by 50 (starting with zero initially). This continues until you receive a 204 response from the APIv3, and they have successfully paged through the API response.

The main idea here and in reviewing the code is that limit is always 50 and offset begins at 0. With each successful APIv3 call receiving a 200 response, you add the limit + offset to provide the new offset, and then go back through the loop. This code has only basic error checking and you will likely require much heavier error checking in your production code.

```
{
"queries":  [
  {
    "type":"report",
    "query": "x_mandiant_com_metadata.report_type = 'malware'" }
 ],
 "limit": 50,
 "offset": 50,
 "sort_by":"name",
 "sort_order":"asc"
}

limit = 50
offset = 0
try:
   while True:
      payload = '''{
            "queries": [
            { "type": "%s" }
            ],
            "sort_by": "name",
            "sort_order": "asc",
            "limit" : %d,
            "offset" : %d
            } ''' %(requestType,limit,offset)
      r = requests.post(url, data=payload, headers=headers)
      if r.status_code != 200:
            raise Exception(r.text)
      if r.status_code == 200:
         (parse the request...)
      offset = limit + offset
```

Collections

The Intel APIv3 is designed around the concept of "collections." A collection provides an interface to a logical repository of Cyber Threat Intelligence data. Collections are organized as sets of specific data that are targeted to address certain areas, such as IOCs, reports, threat actors, malware, and others. The objects that make up a specific collection may also appear in another collection. This lets you pivot from a collection with minimal details about an object, such as a threat actor, to another collection that contains more details.

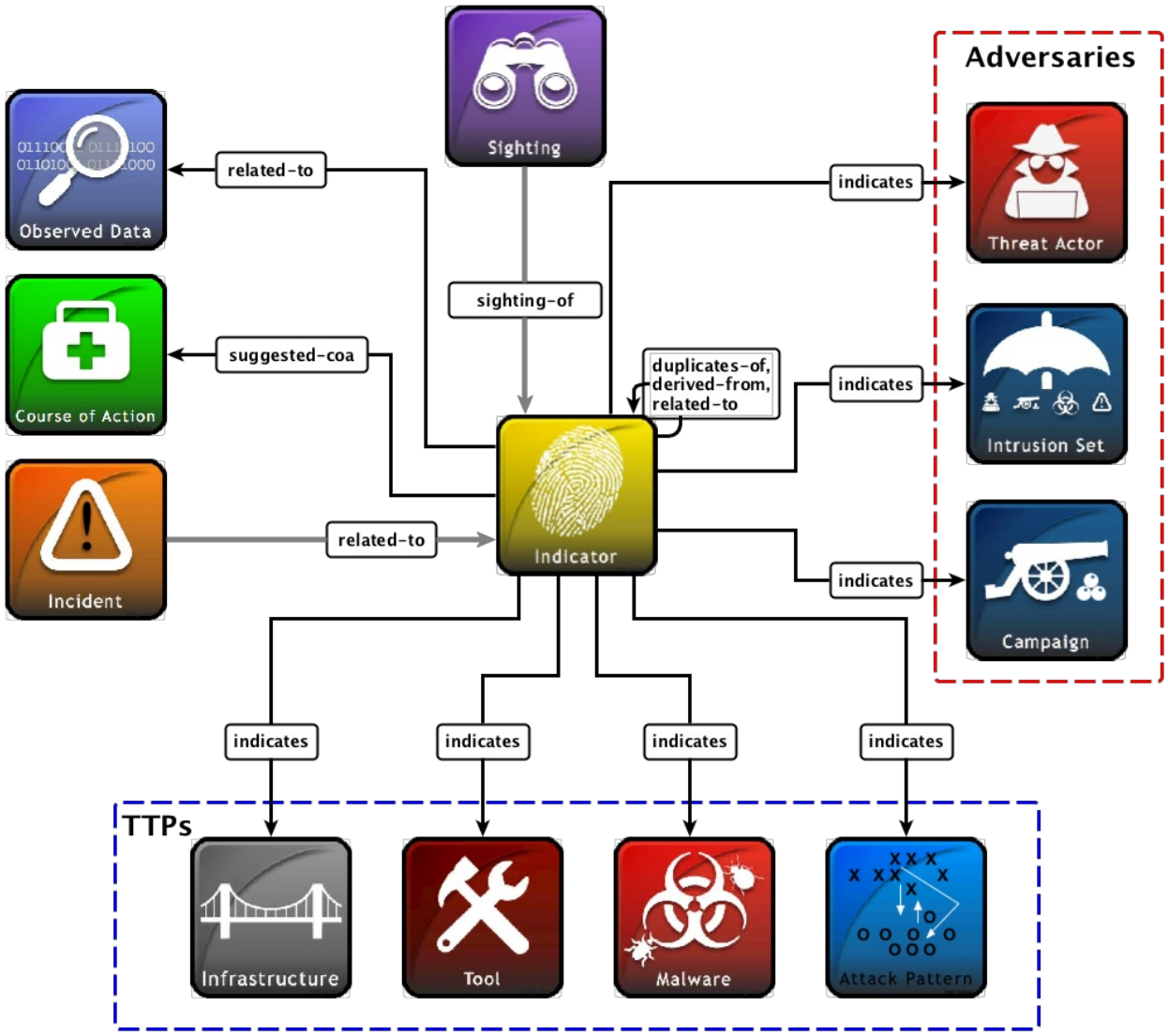
The Intel APIv3 currently provides various collections and is designed to allow new collections to be added without disrupting existing consumers. Each collection is assigned a unique identifier (UUID) and an alias name, either of which can be used when performing queries in the API.

A consumer can programmatically obtain a list of the current collections. The list contains a title, short description, the UUID, alias, and whether they are able to access or update the contents of a collection.

Indicators Collection

The Indicators Collection lets consumers easily retrieve indicators without sifting through a full report. Indicators are expressed in a pattern that can be used to detect the presence of a TTP in your environment along with relevant contextual information.

The following diagram from **STIX Documentation** **(https://stixproject.github.io/documentation/)** describes the STIX Indicator object and its relationships to various IOCs:



Collection Identifier	Alias Name
f5c927fa-4a5c-490a-ac83-31f64ddb4443	indicators

Get Indicators

This endpoint retrieves indicators from the Intel APIv3.

Response format is STIX2.1 as shown in the following media_types object code:

```
{
   "media_types": [
      "application/vnd.oasis.stix+json; version=2.1",
      "application/stix+json",
      "application/stix+json; version=2.1",
      "application/vnd.oasis.stix+json"
   ],
   "description": "This collection holds indicators, the corresponding observables used in detection, and attribution",
   "alias": "f5c927fa-4a5c-490a-ac83-31f64ddb4443",
   "title": "Indicators",
   "can_read": true,
   "can_write": false,
   "id": "indicators"
}
```


HTTP Request

GET (https://api.intelligence.mandiant.com/collections/indicators/objects)

`https://api.intelligence.mandiant.com/collections/indicators/objects`

Headers

See the general **request-headers** for the required headers.

Indicator Query Parameters

Parameter	Valid	Description
added_after	integer	An epoch timestamp that filters objects to only include those added to the collection after the specified timestamp. If no added_after URL query parameter is provided, the APIv3 returns the oldest objects matching the request first.
length	integer	Length: specifies the maximum number of objects to include in a page. If not specified, the **default value is 50**. Maximum value is **1000**.
match.id	STIX UUID	Specifies the STIX ID of the object that you would like to receive.
match.status	active, revoked	Filters on whether the indicator is in an active state or has been revoked.

Sample APIv3 Call with parameters

API Query	Description
`https://api.intelligence.mandiant.com/collections/indicators/objects?added_after=1580600436&length=1000`	Query the indicators collection for **new objects from Feb 1, 2020** and return 1000 objects in the response.

Sample Indicators Output:


```
{
   "spec_version": "2.1",
   "objects": [
      {
         "id": "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82",
         "type": "marking-definition",
         "created": "2017-01-20T00:00:00.000Z",
         "definition_type": "tlp",
         "definition": {
            "tlp": "amber"
```

```
      "tlp": "amber"
    }
  },
  {
    "external_references": [
      {
        "source_name": "fireeye-intel",
        "external_id": "18-00010024",
        "description": "FLUXXY Malware Overview"
      },
      {
        "source_name": "fireeye-intel",
        "external_id": "18-00011411",
        "description": "Fluxxy Malware Profile"
      }
    ],
    "object_marking_refs": [
      "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82"
    ],
    "id": "malware--552dfe3c-9179-57fb-97a0-b672b77c9cb9",
    "name": "fluxxy",
    "type": "malware",
    "created": "2018-10-02T23:32:17.000Z",
    "modified": "2020-02-04T09:35:14.000Z",
    "malware_types": [
      "unknown"
    ],
    "is_family": true,
    "labels": [
      "fastflux-bot",
      "unknown"
    ],
    "revoked": false,
    "spec_version": "2.1"
  },
  {
    "object_marking_refs": [],
    "id": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "name": "The MITRE Corporation",
    "type": "identity",
    "created": "2017-06-01T00:00:00.000Z",
    "modified": "2017-06-01T00:00:00.000Z",
    "revoked": false,
    "identity_class": "organization",
    "lang": "en",
    "spec_version": "2.1"
  },
  {
    "id": "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82",
    "type": "marking-definition",
    "created": "2017-01-20T00:00:00.000Z",
    "definition_type": "tlp",
    "definition": {
      "tlp": "amber"
    }
  },
  {
    "id": "relationship--ddbd0913-aa55-524e-9cd7-bc3346f4122b",
```

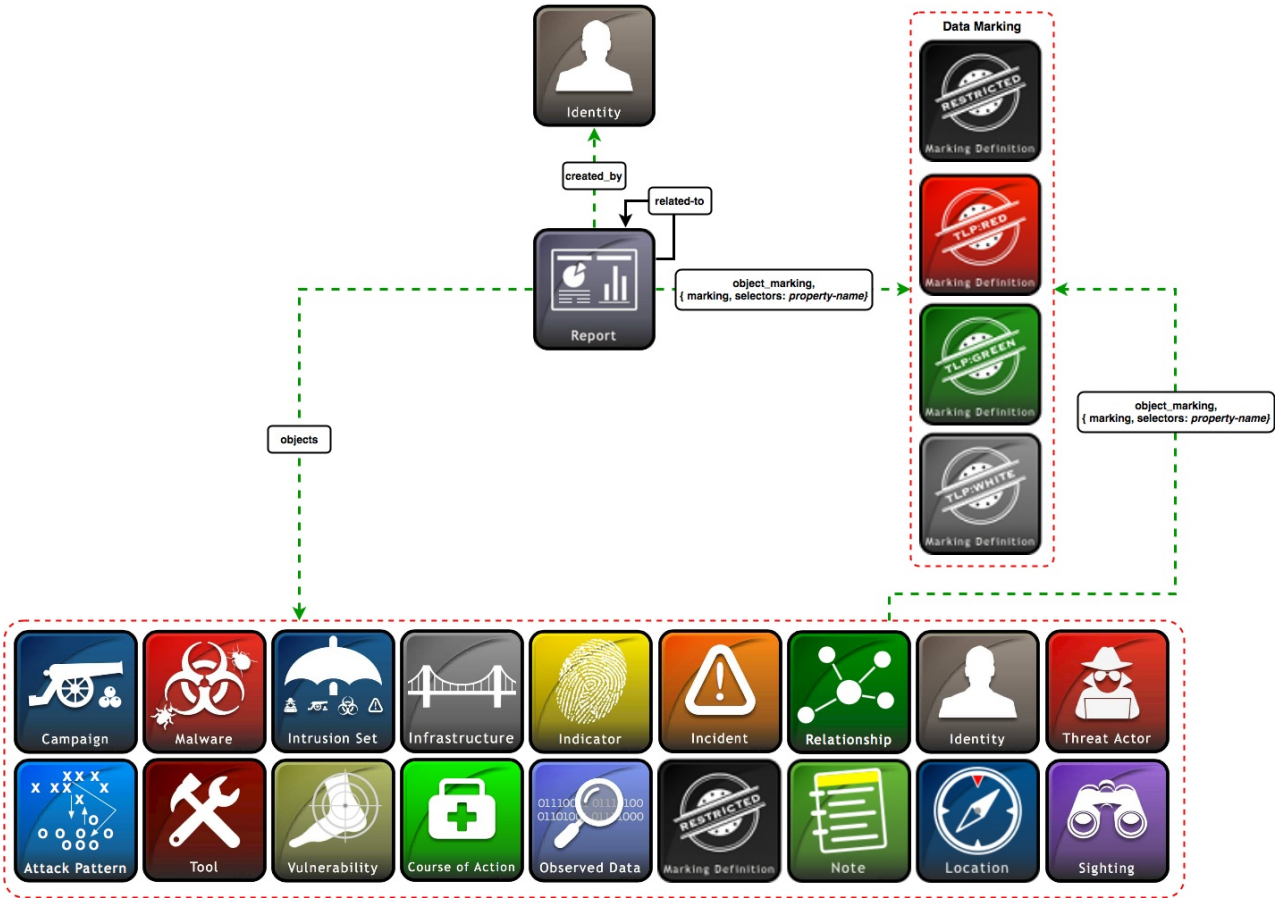
```
    "source_ref": "indicator--93537359-68bf-5920-b474-97efdfb4eb39",
    "target_ref": "malware--552dfe3c-9179-57fb-97a0-b672b77c9cb9",
    "type": "relationship",
    "created": "2020-02-04T09:35:14.000Z",
    "modified": "2020-02-04T09:35:14.000Z",
    "revoked": false,
    "relationship_type": "indicates",
    "spec_version": "2.1"
  },
  {
    "x_fireeye_com_metadata": {
      "subscriptions": [
        "fusion"
      ]
    },
    "indicator_types": [
      "malicious-activity"
    ],
    "pattern_type": "stix",
    "object_marking_refs": [
      "marking-tlp--f88d31f6-486f-44da-b317-01333bde0b82"
    ],
    "id": "indicator--93537359-68bf-5920-b474-97efdfb4eb39",
    "type": "indicator",
    "created": "2020-02-04T09:35:14.000Z",
    "modified": "2020-02-04T09:35:14.000Z",
    "revoked": false,
    "valid_from": "2020-02-04T09:35:14.000Z",
    "confidence": 90,
    "pattern": "[domain-name:value='b.bidomrfrog.org']",
    "labels": [
      "malicious-activity"
    ],
    "valid_until": "2020-02-11T09:35:15.000Z",
    "spec_version": "2.1"
  },
  {
    "id": "marking-definition--63ffe2ce-a941-42cf-923b-7c2d1286b657",
    "type": "marking-definition",
    "created": "2019-05-08T20:30:00.000Z",
    "created_by_ref": "identity--93607fcf-a0cc-472f-bcc6-92082f856b37",
    "definition_type": "statement",
    "spec_version": "2.1",
    "definition": {
      "statement": "Copyright 2019, Mandiant, Inc. All rights reserved."
    }
  },
  {
    "object_marking_refs": [
      "marking-definition--63ffe2ce-a941-42cf-923b-7c2d1286b657"
    ],
    "id": "identity--93607fcf-a0cc-472f-bcc6-92082f856b37",
    "name": "Mandiant, Inc.",
    "type": "identity",
    "created": "2019-05-08T20:30:00.000Z",
    "modified": "2019-05-08T20:30:00.000Z",
    "identity_class": "organization",
```

```
        "spec_version": "2.1"
      }
    ],
    "id": "bundle--c0b6a21f-27e8-45dd-8f9d-85648bc95f42",
    "type": "bundle"
}
```


Reports Collection

The Reports Collection allows consumers to retrieve finished intelligence reports (FINTEL) in a machine-readable format that can be directly inserted into another system. The Reports Collection also lets you retrieve a Report in HTML or PDF format.

The following diagram from **STIX Documentation** (https://stixproject.github.io/documentation/) describes the STIX Report object. It includes topic objects such as Adversaries and TTPs and the use of Data Marking classification through the traffic light protocol (TLP):



Collection Identifier	Alias Name
a7ee60d2-f8d5-4f75-b8fc-886e5a478b95	reports

Get Reports

This endpoint retrieves finished intelligence reports from the Intel APIv3.

Response formats are STIX2.1, PDF, and HTML as shown in the following media_types object code:

```
{
   "media_types": [
      "application/vnd.oasis.stix+json; version=2.1",
      "application/stix+json",
      "application/stix+json; version=2.1",
      "application/vnd.oasis.stix+json",
      "application/pdf",
      "text/html"
   ],
   "description": "This collection holds reports, the corresponding observables used in detection, and attribution",
   "alias": "a7ee60d2-f8d5-4f75-b8fc-886e5a478b95",
   "title": "Reports",
   "can_read": true,
   "can_write": false,
   "id": "reports"
}
```


HTTP Request

GET (https://api.intelligence.mandiant.com/collections/reports/objects)

https://api.intelligence.mandiant.com/collections/reports/objects

Headers

See the general **request-headers** for the required headers.

Report Query Parameters

Parameter	Valid	Description
added_after	integer	An epoch timestamp that filters objects to only include those added to the collection after the specified timestamp. If no added_after URL query parameter is provided, the APIv3 returns the oldest objects matching the request first.
length	integer	Length: specifies the maximum number of objects to include in a page. If not specified, the **default value is 50**. Maximum value for reports is **100**.
match.report_id	STIX UUID	Specifies the STIX ID of the object that you would like to receive. For example, report--5e55ad2e-803e-54b0-94d7-2b5bc2aac4a0.
match.document_id	report#	Filters this endpoint to a single report using the reportID, for example 20-00000710
match.status	active, revoked	Filters on whether the report is active or has been revoked.
match.subscription	cyber-crime, cyber-espionage, hacktivism, cyber-physical, strategic, fusion, operational, vulnerability, standard	Filters on a specific subscription of reports either ThreatScape or role-based Intel.
match.report_type	reportType	Filters on a reportType, for use with multiple report types.

Parameter	Valid	Description
match.actor_name	actorName	Filters the report results down to a specific actor, to return all matching reports for that actor.
match.malware_name	malwareFamily	Filters the report results down to a specific malware family, to return all matching reports for that malware family.

Sample APIv3 Call with parameters

API Query	Description
`https://api.intelligence.mandiant.com/collections/reports/objects?added_after=1580600436&length=100`	Query the reports collection for **new objects from Feb 1, 2020** and return 1000 objects in the response.
`https://api.intelligence.mandiant.com/collections/reports/objects?match.actor_name=apt28&length=100`	Query the reports collection for **reports related to APT28** and return 1000 objects in the response.

Sample Report Output:


```
{
 "id": "bundle--1ced526a-6c63-40b5-8a63-f11ebffef349",
 "type": "bundle",
 "objects": [
  {
   "type": "report",
   "spec_version": "2.1",
   "id": "report--b8d51df0-c292-53fa-86c7-fd50b27089ef",
   "created_by_ref": "identity--93607fcf-a0cc-572f-bcc6-92082f856b37",
   "created": "2019-03-07T22:06:46.993Z",
   "modified": "2019-03-07T22:07:20.973Z",
   "name": "Title - d63e74bf 79718c50313d05a2-1551996406",
   "description": "Overview 32cf81c8 62058946c0b4b9bb",
   "report_types": [ "threat-report" ],
   "published": "2019-03-07T22:07:20.972Z",
   "object_marking_refs": [
    "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82"
   ],
   "x_fireeye_com_additional_description_sections": {
    "analysis": [
     "Analysis 6588be26 ff899819d7d71267"
    ],
    "key_points": [
     "Key Points 26d5ce20 5f33fb7bdc206b4a"
    ]
   },
   "object_refs": [
    "relationship--cd1fa28b-ff23-53bd-8375-887efabecba3",
    "relationship--60128523-d01c-5b31-9047-b39fcdaf7642",
    "relationship--b4d545c9-557f-5842-9b08-0670b5e30b86",
    "relationship--a1e8f651-ee6c-5b63-841e-fae621b033d7",
    "x-fireeye-com-url--267f7633-f503-58f0-8189-9669c4388ac9",
    "relationship--83479639-2b33-54d4-ae92-43191bdc4b42",
    "relationship--fb7948f2-56d0-5c31-b817-488278ea786b",
    "x-fireeye-com-domain-name--718e7095-2568-5234-83b6-d6e4ff8a38bd",
    "relationship--f333c380-3758-5280-a270-485255786a31",
    "relationship--bc587c58-50ad-54f6-8a5d-13d0e4c8c0c2",
    "x-fireeye-com-socket-addr--e65095dc-81a2-5bbf-9418-192dc806c3cc",
```

```
      "relationship--be07123f-33a1-5f40-a4f8-bdb5c0088679",
      "relationship--b9783779-059a-582f-8c6e-2b07ce8dc077",
      "x-fireeye-com-email-message--a867827d-9c13-5970-9496-1927ce9d9361",
      "x-fireeye-com-file--dd42f582-65db-50c1-9828-fb2c8344da22",
      "indicator--7c8b0f77-912a-5157-a38f-5a2affb03328",
      "x-fireeye-com-network-traffic--51d3d3bb-f2a8-47b3-830b-956fa578420b",
      "malware--4bfa8fe6-2b58-5f53-85bf-3b4c3b15508a",
      "threat-actor--1f59bb93-105c-51d8-8a3c-42dc3385638a",
      "indicator--778ff5fe-535c-51ef-81ed-387e957d58ad",
      "indicator--da678751-8012-517a-9107-ebd41db31e85",
      "relationship--f0cd5cbe-f89d-55a1-8571-ae214c278028",
      "relationship--c259307a-9855-5710-96f1-342500c5ab44",
      "indicator--3521c406-47d8-567f-aae1-fb1c75fef0f8",
      "relationship--71f88376-644c-5aed-8e58-8456f8771607",
      "relationship--6e2572c6-fe7e-56f3-9ac0-2ce20dc94258",
      "x-fireeye-com-ipv4-addr--5b84ac6a-0b2e-5a17-ab2d-c56f392d88dd",
      "relationship--13b8994c-689e-5a9e-846d-211ef2d9014c",
      "relationship--806b8e4a-6d41-58ed-bd5d-21d4f33478cb",
      "x-fireeye-com-windows-registry-key--bf8aa637-e474-5ede-ac6e-2ccfedb4eecb",
      "x-fireeye-com-whois--683946bf-6c4b-579e-b455-601b4f0e72d7",
      "relationship--cb5e390a-7e54-5a25-bc7b-aed8218a71d7",
      "relationship--6a87e2fc-a803-5ae8-8b0a-6fda68889518",
      "relationship--2a8f70c9-2364-531f-b4a6-6c40cbf6f933",
      "relationship--0d9fbca5-ee76-5467-a846-a25cfd7b2d0a",
      "relationship--fddf9f27-05c3-59ab-9f03-bf9bb53a0e86",
      "relationship--38886d24-2e0e-5398-9990-7f0154427127",
      "relationship--53db6133-b823-5ad4-861b-a99169a00938",
      "relationship--ec0c58af-32c2-5b3d-be3f-e8fe60cb0562",
      "relationship--f0f5cc78-3ef1-531b-94d1-6000d1a088f8",
      "x-fireeye-com-autonomous-system--e116fedf-9ade-5899-9a71-a51d38a60ca9",
      "relationship--1bc5e0e6-c2e0-563e-8eaa-0fb3af1a4ad8",
      "relationship--ab7be335-b210-5fb6-bf16-1b14f6f3b95a",
      "x-fireeye-com-ipv4-netmask--cae8efc7-08a5-5e67-b648-8d2f3db51ecc",
      "relationship--d62ba347-bf25-5b48-9e9c-0ede1069de23"
    ],
    "x_fireeye_com_tracking_info": {
      "document_version": "1.0",
      "current_release_date": "2019-03-07T22:07:20.972Z",
      "document_id": "19-00014859",
    },
    "x_fireeye_com_metadata": {
      "product_type": [
        "Intelligence Report"
      ],
      "subscriptions": [
        "operational"
        "cyber-espionage"
      ]
    }
   }
  ]
}
```


Search

This APIv3 endpoint lets you search all collections for objects of interest. You can query all objects in all collections, which provides you with a large response. Or you can choose to filter searches on the support object type listed for objects such

as a threat-actor, report, ipv4-addr, URL, vulnerability, and others.

Endpoint Identifier	Alias Name
g7ee60d2-f8d5-4f75-b8fc-886e5a478b96	search

POST Search

This endpoint supports searches across all collections.

HTTP Request

POST (https://api.intelligence.mandiant.com/collections/search)

`https://api.intelligence.mandiant.com/collections/search`

Description: This endpoint is used to search data in Intelligence APIv3.

Headers

See the general **request-headers** for the required headers.


```
{
   "media_types": [
      "application/stix+json",
      "application/stix+json; version=2.1",
      "application/vnd.oasis.stix+json",
      "application/vnd.oasis.stix+json; version=2.1"
   ],
   "description": "This endpoint supports searches across all collections.",
   "alias": "g7ee60d2-f8d5-4f75-b8fc-886e5a478b96",
   "title": "Search",
   "can_read": true,
   "can_write": false,
   "id": "search"
}
```


Search Template

This is the full JSON search template for use in searching against the Intel APIv3. Not all of these components are required; see **Search Template Breakdown** for a description of the required fields.

```
{
 "queries": [
  {
   "type":"<support object type>",
   "query":"<query expression on properties>"
  }
 ],
 "include_connected_objects":"<true|false>",
 "connected_objects": [
  {
   "connection_type":"reference",
   "connected_type":"<source or target>",
   "object_type":"<supported object type>",
   "property":"objects"
  },
  {
   "connection_type":"relationship",
   "connected_type":"<source or target>",
   "object_type":"<supported object type>",
   "relationship_type":"<relationship_type>"
  }
 ],
 "sort_by":"<supported property>",
 "sort_order":"<asc|desc>"
}```
```

Search Template Breakdown

- **queries**: A single query object. The query object includes the type and query properties.
- **type**: The type specifies the object to search.

  The following are all allowed **support object type** values for use with search, which are actually **object_refs**:
  - "domain-name"
  - "file"
  - "identity"
  - "indicator"
  - "ipv4-addr"
  - "malware"
  - "report"
  - "threat-actor"
  - "url"
  - "vulnerability"

- **query**: A query contains a Query Search Expression. Multiple query search expressions are joined by boolean AND or OR operators. Query search expressions consist of three parts: Property Path, a Comparison Operator, and an Operand.
  - **Comparison Operators**: `=, !=, >, <, >=, <=, IN, LIKE`
  - **Date**: Allowed date format is- '%Y-%m-%dT%H:%M:%S.%fZ'. The date value should be specified in single quotes (for example, created='2016-10-20T17:39:05.101Z').

- **include_connected_objects**
  Required: False
  Type: Boolean

Default Value: false
Description: Indicates whether objects connected to matching objects, through a reference or relationship, will be included in the search result.

- **connected_objects**
  Required: False
  Type: List of connections
  Default Value: -
  Description: Lists all connections, which all contain the following fields:
- **connection_type**: Value of connection_type can be one of the following:
  - **reference:** The connected object should be referenced from the matching object or reference the matching object.
  - **relationship:** The connected object should be related to the matching object through a relationship where the matching object is the source or the target. If it is not specified, both types are returned.
- **connected_type**: Value can be one of the following:
  - **source**: Returns the connected object that is the connection source. If connection_type is reference, the matching object is the target of the reference and will therefore return the source object that is referenced by matching object. If `connection_type` is **relationship**, the matching object is the target of the relationship and will return the object that is the source of the relationship, and the relationship object itself.
  - **target**: Returns the connected object that is the connection target. if `connection_type` is **reference**, the matching object is the source of the reference and will therefore return the target object that is referenced by the matching object. If `connection_type` is **relationship**, the matching object is the source of the relationship and will therefore return the object that is the target of the relationship, and the relationship object itself.
- **object_type**: Object type returns the connected_objects of type specified in the `object_type` field.
  - If `result_type` contains "connected_objects," the resulting connections are restricted only to those connections that match one of the connection objects in this list. If `result_type` contains "connected_objects" and this list is empty or the field is not present, all connections will be returned.
- **property**: property is used when `connection_type` is "reference." When `connection_type` is "source," this field returns the connected objects that reference the matching objects through the given property. When `connection_type` is "target," this field returns the connected objects that are referenced by matching object through the given property.
  - If this field is not specified, it matches any property by which the reference exists. This field is ignored when `connection_type` is relationship.
- **relationship_type**: This field is used when `connection_type` is relationship. This field returns only the related objects that are involved in relationships of the specified relationship_type.
  - If not specified, all relationship types are considered for matching. This field is ignored when `connection_type` is **reference.**
- **sort_by**
  Required: False
  Type: string
  Default Value: -
  Description: `sort_by` specifies the property of the object on which results are to be sorted. `sort_by` is applicable only when the `include_connected_object` flag is set to **false**.
- **sort_order**
  Required: False
  Type: string
  Default Value: -
  Description: This field specifies the direction of sort. Sort order can be set to "asc" (ascending) or "desc" (descending). If the sort order is not specified, it will default to ascending. Note that the sort_order is only applicable

when the `include_connected_object` flag is set to **false**.

Search Examples

The following are examples of common search queries.

Report types containing malware

This query will return both report_types for **Malware Profile** and **Malware Overview** reports in search. This value of `malware` is **NOT** applicable for the report collection filter.

```
{
"queries":  [
  {
   "type":"report",
   "query": "x_fireeye_com_metadata.report_type = 'malware'" }
 ],
 "limit": 50,
 "offset": 50,
 "sort_by":"name",
 "sort_order":"asc"
}
```

Actor with a name LIKE APT27

This query will search for a **`threat-actor`** using name **`LIKE`** APT27. Note the single ticks and the % signs around the term apt27, and return all relationships for that actor.

```
{
"queries": [
 {
 "type": "threat-actor",
 "query" : "name LIKE '%APT27%'"}
 ],
"include_connected_objects": true,
"connected_objects" : [
 {"connection_type" : "relationship"},
 {"connection_type" : "reference"}]
}
```

Actor with name equals APT27

This query will search for a **`threat-actor`** whose name is exactly **APT27**, and return all relationships for that actor.

```
{
"queries": [
   {
   "type": "threat-actor",
   "query" : "name = 'APT27'"}
 ],
 "include_connected_objects": true,
 "connected_objects" : [
   {"connection_type" : "relationship"},
   {"connection_type" : "reference"}]
}
```

Indicator matching IPv4 address

This query will search for an indicator matching an IPv4 address with connected objects and relationships.

```
{
   "queries": [
   {
      "type": "indicator",
      "query": "pattern LIKE = '%164.132.67.216%'"
   }
  ],
  "include_connected_objects": true
}
```

Actor IOC Search

Using the query "id IN" with the threat-actor-ID's, you can retrieve all domains associated with these specified actors. This example includes a time period search as well.

```
{
 "queries": [
 { "type": "threat-actor" ,"query" :"id IN ('threat-actor--e9e0b284-572e-57bd-925b-71fabf9e8a65','threat-actor--90ecd6c1-abb7-5137-9160-e68f29239a3f','threat-actor--ce850ca5-61cf-53cb-9b17-2e4396b4c3a2','threat-actor--a09f768d-7733-5e01-a42e-d2f356dbca10','threat-actor--1c3be4c1-fd7f-530e-9275-e4350f557591','threat-actor--30d897ea-3c4f-5a63-be30-cd6ab8313f5f','threat-actor--02e6e376-e6ec-5a74-9a03-233f4fbaad2d','threat-actor--b617ea48-6569-54b7-8015-0291b4b66ede','threat-actor--5f57586d-8a5c-5c48-adbb-9c01ed079c8a') AND modified > '2019-04-01T00:00:00.000Z' " }
 ],
 "include_connected_objects": true,
 "connected_objects" : [
 {
 "connection_type" : "relationship",
 "object_type" : "domain-name"
 }
 ]
}
```

Field Definitions

The field definitions page is designed to provide a maximum amount of detail available for these items.

```
{
   "reportTypes": [
         "Actor Overview",
         "Actor Profile",
         "Country Profile",
         "Credit Card Shop Report",
         "Event Coverage/Implication",
         "Executive Perspective",
         "Mandiant Labs Research",
         "Horizons",
         "ICS Security Roundup",
         "Industry Intelligence Quarterly",
         "Industry Reporting",
         "Malicious Activity Report",
         "Malware Overview",
         "Malware Profile",
         "Malware Quarterly Industry Report",
         "Net Assessment",
```

```
        "Network Activity Reports",
        "Operational Net-Assessment",
        "TTP Deep Dive",
        "Tactical Threat Report",
        "Targeted Malware Lures",
        "Threat Activity Alert",
        "Threat Activity Report",
        "Trends and Forecasting",
        "Vulnerability",
        "Vulnerability Report",
        "Weekly Vulnerability Exploitation Report"
    ],
    "threatScape": [
        "fusion",
        "operational",
        "strategic",
        "vulnerability",
        "cyber-espionage",
        "cyber-crime",
        "cyber-physical",
        "hacktivisim",
        "standard"
    ],
    "relationship_type": [
        "affects",
        "associated-with",
        "attributed-to",
        "characterized-by",
        "contained_within",
        "has-characteristic",
        "indicates",
        "located-at",
        "member-of",
        "modifies",
        "related-to",
        "resolves-to",
        "source-geography",
        "targeted-geography",
        "targets",
        "undefined",
        "used-by",
        "used_against",
        "uses"
    ],
    "object_refs": {
        "attack-pattern": "no",
        "autonomous-system": "no",
        "campaign": "no",
        "course-of-action": "no",
        "domain-name": "yes",
        "file": "yes",
        "indicator": "yes",
        "infrastructure": "no",
        "intel-note": "no",
        "intrusion-set": "no",
        "ipv4-addr": "yes",
        "kill-chain-phase": "no",
```

```
        "malware": "yes",
        "network-traffic": "no",
        "remedy-action": "no",
        "report": "yes",
        "socket-addr": "no",
        "software": "no",
        "tactic": "no",
        "threat-actor": "yes",
        "tool": "no",
        "url": "yes",
        "vulnerability": "yes",
        "weakness": "no",
        "whois": "no",
        "x-fireeye-com-cpe": "yes",
        "x-fireeye-com-exploit": "no",
        "x-fireeye-com-exploitation": "yes"
    },
    "searchable_properties": {
    "domain-name": [
        "id",
        "value",
        "created",
        "modified"
    ],
    "file": [
        "id",
        "name",
        "ctime",
        "mtime",
        "hashes.MD5",
        "hashes.SHA-1",
        "hashes.SHA-256"
    ],
    "indicator": [
        "id",
        "name",
        "created",
        "modified",
        "valid_from",
        "valid_until",
        "confidence",
        "description",
        "pattern",
        "labels"
    ],
    "ipv4-addr": [
        "id",
        "value",
        "created",
        "modified"
    ],
    "malware": [
        "id",
        "name",
        "labels",
        "created",
        "modified",
```

```
        "aliases",
        "is_family",
        "description",
        "os_execution_envs"
    ],
    "report": [
        "id",
        "name",
        "labels",
        "created",
        "modified",
        "published",
        "object_refs",
        "description",
        "x_fireeye_com_tracking_info.document_id",
        "x_fireeye_com_metadata.report_type",
        "x_fireeye_com_metadata.affected_it_systems",
        "x_fireeye_com_metadata.risk_rating",
        "x_fireeye_com_exploitation_rating",
        "x_fireeye_com_metadata.intended_effect",
        "x_fireeye_com_additional_description_sections.analysis",
        "x_fireeye_com_metadata.target_geographies",
        "x_fireeye_com_metadata.affected_industries",
        "x_fireeye_com_additional_description_sections.key_points",
        "x_fireeye_com_metadata.targeted_information",
        "x_fireeye_com_metadata.motivation",
        "x_fireeye_com_metadata.subscriptions",
        "x_fireeye_com_metadata.source_geographies",
        "x_fireeye_com_risk_rating_justification",
        "x_fireeye_com_metadata.affected_ot_systems"
    ],
    "threat-actor": [
        "id",
        "name",
        "aliases",
        "created",
        "labels",
        "modified",
        "description",
        "primary_motivation",
        "secondary_motivations",
        "sophistication",
        "x_fireeye_com_intended_effect",
        "x_fireeye_com_planning_and_operational_support"
    ],
    "url": [
        "id",
        "created",
        "modified",
        "value"
    ],
    "vulnerability": [
        "id",
        "name",
        "created",
        "modified",
        "x_fireeye_com_identifier.value",
```

```
        "x_fireeye_com_identifier.naming_authority"
        ],
    }
}```
```

Response Status Codes

The following table lists response status codes and their meanings.

Error Code	Meaning	Reason
200	Everything worked correctly	We gave you data.
204	Everything worked correctly	No data was provided.
400	Bad Request	Your request is invalid.
401	Unauthorized	Your account is expired or the dates are wrong.
403	Forbidden - User is not authorized to access this resource with an explicit deny.	Your token was rejected.
500	Internal Server Error	We had a problem with our application server, contact **Support (https://docs.mandiant.com/home/mandiant-support-cases)**.
502	Gateway Error	We had a problem with our gateway server, contact **Support (https://docs.mandiant.com/home/mandiant-support-cases)**.
504	Gateway Error	We had a problem with our gateway server, contact **Support (https://docs.mandiant.com/home/mandiant-support-cases)**.