Mandiant

MANAGED DEFENSE API

Investigations API Documentation

baseUri: https://api.services.mandiant.com

protocols: HTTPS

Terms of Use

The terms of use for the Mandiant Intelligence API fall under the **Google Cloud terms of service (https://cloud.google.com/terms)**.

Investigation Page Elements Reference

Investigation Page

Ref	Description	API Object
Title	The Investigation Title	Investigation
ID	The Investigation ID	Investigation
Summary	The Investigation Summary	Investigation
Severity	Investigation Severity (High, Medium, Low, Information or Under Review)	Investigation
Status	Current status of the Investigation (Open, Closed, Rejected)	Investigation
Recommendations	Actions recommended by the analyst to prevent and contain the threat	Course of Action

Asset Details

Asset Details	Description	API Object
Asset	The Targeted system in your environment	Compromise Target
Related	Related Nodes	Compromise Target
Reported	Date Alert was reported	Compromise Target
Threat Type	The type of threat	-
Malware	The malware(s) associated with the threat or investigation	Malware

Findings

Investigation Findings	Description
Analysis Summary	Summary of the Investigation findings
Finding Details	Overview of the event details
Analysis Evidence	Alert evidence which shows artifact types and associated data

Authentication

Investigations API uses the OAuth 2 Authorization Framework, specifically, the client credentials grant, to grant access to the API endpoints. Before using an API endpoint, your client application must authenticate against the /token endpoint to receive a time-limited access token.

The service will respond with a JSON body containing 3 keys:

- **access_token:** The access_token will be used in the Authorization header as a bearer token.
- **token_type:** The type of the token issued as described in Section 7.1 of the OAuth 2 spec. The value is case insensitive. It will always be bearer.
- **expires_in:** The expires_in value indicates the lifetime in seconds of the access token, which is 1800 seconds by default. Unless the token has been revoked, this token may be used until it expires. Users must re-authenticate to receive a new access token.

CURL EXAMPLE

```
curl -X POST https://api.services.mandiant.com/token -H "Authorization: Basic apikeyhere" -d "grant_type=client_cred
entials"
```

SUCCESSFUL RESPONSE


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


Types

Alert

A report of one or more Events believed to be suspicious, along with some explanation of why the activity is believed to be suspicious.

TYPE DEFINITION

```
{
  "id": "../sdos/alert.json",
  "$schema": "http://json-schema.org/draft-04/schema#",
  "title": "alert",
  "description": "A report of one or more Events believed to be suspicious...",
  "type": "object",
  "allOf": [
    { "$ref": "../common/core.json" },
    {
      "properties": {
        "type": {
          "type": "string",
          "description": "The type of this object, which MUST be the literal x-fireeye-com-alert.",
          "enum": [ "x-fireeye-com-alert" ]
        },
        "id": { "title": "id", "pattern": "^x-fireeye-com-alert--" },
        "name": { "type": "string", "description": "The name used to identify the Alert." },
        "description": { "type": "string", "description": "A description that provides more details..." },
        "alert_context": { "description": "Specifies the status of the alert", "$ref": "../vocabularies/alert-context-ov.js
on" },
        "object_refs": {
          "type": "array",
          "description": "Specifies the STIX Objects that are referred to by this Alert.",
          "items": { "$ref": "../common/identifier.json" },
          "minItems": 1
        },
        "x_fireeye_com_alert_id": { "type": "string", "description": "The internal FireEye ID of the alert" }
      },
      "required": [ "name", "alert_context", "object_refs" ]
    }
  ]
}
```


Alert Context Ov

Open Vocabulary for expressing the Context of an Alert.


```
{
  "id": "../vocabularies/alert-context-ov.json",
  "$schema": "http://json-schema.org/draft-04/schema#",
  "title": "alert-context-ov",
  "description": "Open Vocabulary for expressing the Context of an Alert.",
  "oneOf": [
    { "type": "string", "description": "Any value not explicitly described by this open vocabulary." }
  ]
}
```


Artifact

The Artifact Object permits capturing an array of bytes (8-bits), as a base64-encoded string, or linking to a file-like payload.

```
{
  "id": "../observables/artifact.json",
  "$schema": "http://json-schema.org/draft-04/schema#",
  "title": "artifact",
  "description": "The Artifact Object permits capturing an array of bytes...",
  "type": "object",
  "allOf": [
    { "$ref": "../common/cyber-observable-core.json" },
    {
      "properties": {
        "type": {
          "type": "string",
          "description": "The value of this property MUST be artifact.",
          "enum": [ "artifact" ]
        },
        "mime_type": {
          "type": "string",
          "pattern": "^(application|audio|font|image|message|model|multipart|text|video)/[a-zA-Z0-9.+_-]+",
          "description": "The value of this property MUST be a valid MIME type..."
        }
      }
    }
  ],
  "oneOf": [
    {
      "properties": {
        "payload_bin": {
          "$ref": "../common/binary.json",
          "description": "Specifies the binary data contained in the artifact as a base64-encoded string."
        },
        "hashes": {
          "$ref": "../common/hashes-type.json",
          "description": "Specifies a dictionary of hashes..."
        }
      },
      "required": [ "payload_bin" ],
      "not": { "required": [ "url" ] }
    },
    {
      "properties": {
        "url": {
          "$ref": "../common/url-regex.json",
          "description": "The value of this property MUST be a valid URL..."
        },
        "hashes": {
          "$ref": "../common/hashes-type.json",
          "description": "Specifies a dictionary of hashes..."
        }
      },
      "required": [ "url", "hashes" ],
      "not": { "required": [ "payload_bin" ] }
    }
  ]
}
```


Attack Pattern

Attack Patterns are a type of TTP that describe ways that adversaries attempt to compromise targets.


```
{
    "id": "../sdos/attack-pattern.json",
    "$schema": "http://json-schema.org/draft-04/schema#",
    "title": "attack-pattern",
    "description": "Attack Patterns are a type of TTP that describe ways that adversaries attempt to compromise target
s.",
    "type": "object",
    "allOf": [
        { "$ref": "../common/core.json" },
        {
            "properties": {
                "type": {
                    "type": "string",
                    "description": "The type of this object, which MUST be the literal attack-pattern.",
                    "enum": [ "attack-pattern" ]
                },
                "id": { "title": "id", "pattern": "^attack-pattern--" },
                "name": { "type": "string", "description": "The name used to identify the Attack Pattern." },
                "description": { "type": "string", "description": "A description that provides more details..." },
                "kill_chain_phases": {
                    "type": "array",
                    "description": "The list of kill chain phases for which this attack pattern is used.",
                    "items": { "$ref": "../common/kill-chain-phase.json" },
                    "minItems": 1
                }
            }
        }
    ],
    "required": [ "name" ]
}
```


Autonomous System

The AS object represents the properties of an Autonomous Systems (AS).

```
{
   "id": "../observables/autonomous-system.json",
   "$schema": "http://json-schema.org/draft-04/schema#",
   "title": "autonomous-system",
   "description": "The AS object represents the properties of an Autonomous Systems (AS).",
   "type": "object",
   "allOf": [
      { "$ref": "../common/cyber-observable-core.json" },
      {
         "properties": {
            "type": {
               "type": "string",
               "description": "The value of this property MUST be autonomous-system.",
               "enum": [ "autonomous-system" ]
            },
            "number": {
               "type": "integer",
               "description": "Specifies the number assigned to the AS..."
            },
            "name": { "type": "string", "description": "Specifies the name of the AS." },
            "rir": { "type": "string", "description": "Specifies the name of the Regional Internet Registry (RIR)..." }
         },
         "required": [ "number" ]
      }
   ]
}
```

Binary

The binary data type represents a sequence of bytes. In order to allow pattern matching on custom objects, for all properties that use the binary type, the property name MUST end with '_bin'. The JSON MTI serialization represents this as a base64-encoded string as specified in RFC4648.

```
{
   "id": "../common/binary.json",
   "$schema": "http://json-schema.org/draft-04/schema#",
   "title": "binary",
   "description": "The binary data type represents a sequence of bytes...",
   "type": "string",
   "pattern": "^([A-Za-z0-9+/]{4})*([A-Za-z0-9+/]{4}|[A-Za-z0-9+/]{3}=|[A-Za-z0-9+/]{2}==)$"
}
```

Bundle

A Bundle is a collection of arbitrary STIX Objects and Marking Definitions grouped together in a single container.

TYPE DEFINITION

```
{
   "id": "../common/bundle.json",
   "title": "bundle",
   "$schema": "http://json-schema.org/draft-04/schema#",
   "description": "A Bundle is a collection of arbitrary STIX Objects...",
   "type": "object",
   "properties": {
      "type": { "type": "string", "description": "The type of this object, which MUST be the literal bundle.", "enum": [ "b
undle" ] },
      "id": {
         "allOf": [
            { "$ref": "identifier.json", "description": "An identifier for this bundle..." },
            { "title": "id", "pattern": "^bundle--" }
         ]
      },
      "spec_version": { "type": "string", "enum": [ "2.0" ], "description": "The version of the STIX specification..." },
      "objects": {
         "type": "array",
         "description": "Specifies a set of one or more STIX Objects.",
         "items": {
            "anyOf": [
               {
                  "oneOf": [
                     { "$ref": "../sdos/attack-pattern.json" },
                     { "$ref": "../sdos/campaign.json" },
                     { "$ref": "../sdos/course-of-action.json" },
                     { "$ref": "../sdos/identity.json" },
                     { "$ref": "../sdos/indicator.json" },
                     { "$ref": "../sdos/intrusion-set.json" },
                     { "$ref": "../sdos/malware.json" },
                     { "$ref": "marking-definition.json" },
                     { "$ref": "../sdos/observed-data.json" },
                     { "$ref": "../sros/relationship.json" },
                     { "$ref": "../sdos/report.json" },
                     { "$ref": "../sros/sighting.json" },
                     { "$ref": "../sdos/threat-actor.json" },
                     { "$ref": "../sdos/tool.json" },
                     { "$ref": "../sdos/vulnerability.json" },
                     { "$ref": "../sdos/alert.json" },
                     { "$ref": "../sdos/investigation.json" },
                     { "$ref": "../sdos/note.json" },
                     { "$ref": "../sdos/compromise-target.json" }
                  ]
               }
            ]
         },
         "minItems": 1
      }
   },
   "required": [ "type", "id", "spec_version" ]
}
```


Campaign

A Campaign is a grouping of adversary behavior that describes a set of malicious activities or attacks that occur over a period of time against a specific set of targets.

```
{
  "id": "../sdos/campaign.json",
  "$schema": "http://json-schema.org/draft-04/schema#",
  "title": "campaign",
  "type": "object",
  "allOf": [
    { "$ref": "../common/core.json" },
    {
      "properties": {
        "type": { "type": "string", "enum": [ "campaign" ] },
        "id": { "title": "id", "pattern": "^campaign--" },
        "name": { "type": "string", "description": "The name used to identify the Campaign." },
        "description": { "type": "string" },
        "aliases": { "type": "array", "items": { "type": "string" } },
        "first_seen": { "$ref": "../common/timestamp.json" },
        "last_seen": { "$ref": "../common/timestamp.json" },
        "objective": { "type": "string" }
      }
    }
  ],
  "required": [ "name" ]
}
```

Capture Source Capability Ov

An open vocabulary that represents the different capture capabilities a Capture Source tool supports.

Mandiant

```
{
   "id": "../vocabularies/capture-source-capability-ov.json",
   "title": "capture-source-capability-ov",
   "oneOf": [
      { "type": "string", "pattern": "^nids$" },
      { "type": "string", "pattern": "^nips$" },
      { "type": "string", "pattern": "^hids$" },
      { "type": "string", "pattern": "^hips$" },
      { "type": "string", "pattern": "^firewall$" },
      { "type": "string", "pattern": "^router$" },
      { "type": "string", "pattern": "^proxy$" },
      { "type": "string", "pattern": "^gateway$" },
      { "type": "string", "pattern": "^anti-virus$" },
      { "type": "string", "pattern": "^vuln-scanner$" },
      { "type": "string", "pattern": "^seim$" },
      { "type": "string", "pattern": "^digital-forensics$" },
      { "type": "string", "pattern": "^static-malware-analysis$" },
      { "type": "string", "pattern": "^dynamic-malware-analysis$" },
      { "type": "string", "pattern": "^incident-response$" },
      {
         "type": "string",
         "description": "Any value not explicitly described by this open vocabulary.",
         "not": {
            "enum": [
               "nids", "nips", "hids", "hips", "firewall", "router", "proxy", "gateway", "anti-virus",
               "vuln-scanner", "seim", "digital-forensics", "static-malware-analysis",
               "dynamic-malware-analysis", "incident-response"
            ]
         }
      }
   ]
}
```

Capture Source Method Ov

An open vocabulary that represents an enumeration different methods of capture.

```
{
   "id": "../vocabularies/capture-source-method-ov.json",
   "title": "capture-source-method-ov",
   "oneOf": [
      { "type": "string", "pattern": "^tool$", "description": "Specifies capture using various tools..." },
      { "type": "string", "pattern": "^analysis$", "description": "Specifies capture using analysis methods..." },
      { "type": "string", "pattern": "information-source", "description": "Specifies capture using other information sourc
es..." },
      {
         "type": "string",
         "not": { "enum": [ "tool", "analysis", "information-source" ] }
      }
   ]
}
```

Capture Source Status Ov

An open vocabulary that represents the status of a Capture Source.

```
{
   "id": "../vocabularies/capture-source-status-ov.json",
   "title": "capture-source-status-ov",
   "oneOf": [
      { "type": "string", "pattern": "^operational$" },
      { "type": "string", "pattern": "^non-operational$" },
      { "type": "string", "pattern": "^disabled$" },
      { "type": "string", "pattern": "^retired$" },
      { "type": "string", "pattern": "^unknown$" },
      {
         "type": "string",
         "not": { "enum": [ "operational", "non-operational", "disabled", "retired", "unknown" ] }
      }
   ]
}
```

Compromise Target

The CompromiseTarget object is used to represent the properties of the target of a compromise.

Property	Object	Description
Node Unique ID	"id"	The investigation ID. example: 1-15607
Name	"name"	The primary nodes name
Asset	"primary_target"	The primary node associated with the compromise target.
Related	"secondary_targets"	The related nodes associated with the compromise target.

```
{
   "id": "../sdos/compromise-target.json",
   "title": "compromise-target",
   "type": "object",
   "allOf": [
      { "$ref": "../common/core.json" },
      {
         "properties": {
            "type": { "type": "string", "enum": [ "x-fireeye-com-compromise-target" ] },
            "id": { "title": "id", "pattern": "^x-fireeye-com-compromise-target--" },
            "name": { "type": "string" },
            "description": { "type": "string" },
            "compromise_id": { "type": "string" },
            "primary_target": { "type": "string" },
            "secondary_targets": { "type": "array", "items": { "type": "string", "uniqueItems": true } },
            "time_of_compromise": { "$ref": "../common/timestamp.json" }
         },
         "required": [ "name", "primary_target" ]
      }
   ]
}
```

Core

Common properties and behavior across all STIX Domain Objects and STIX Relationship Objects.

```
{
   "id": "../common/core.json",
   "title": "core",
   "type": "object",
   "properties": {
      "type": { "type": "string", "pattern": "^\\-?[a-zA-Z0-9]+(-[a-zA-Z0-9]+)*\\-?$", "minLength": 3, "maxLength": 250
},
      "id": { "$ref": "identifier.json" },
      "created_by_ref": { "$ref": "identifier.json" },
      "labels": { "type": "array", "items": { "type": "string" }, "minItems": 1 },
      "created": { "allOf": [ { "$ref": "timestamp.json" }, { "pattern": "T\\d{2}:\\d{2}:\\d{2}\\.\\d{3}Z$" } ] },
      "modified": { "allOf": [ { "$ref": "timestamp.json" }, { "pattern": "T\\d{2}:\\d{2}:\\d{2}\\.\\d{3}Z$" } ] },
      "revoked": { "type": "boolean" },
      "external_references": { "type": "array", "items": { "$ref": "external-reference.json" }, "minItems": 1 },
      "object_marking_refs": { "type": "array", "items": { "$ref": "identifier.json" }, "minItems": 1 },
      "granular_markings": { "type": "array", "items": { "$ref": "granular-marking.json" }, "minItems": 1 }
   },
   "required": [ "type", "id", "created", "modified" ]
}
```

Course Of Action

A Course of Action is an action taken either to prevent an attack or to respond to an attack that is in progress.

```
{
   "id": "../sdos/course-of-action.json",
   "title": "course-of-action",
   "type": "object",
   "allOf": [
      { "$ref": "../common/core.json" },
      {
         "properties": {
            "type": { "type": "string", "enum": [ "course-of-action" ] },
            "id": { "title": "id", "pattern": "^course-of-action--" },
            "name": { "type": "string" },
            "description": { "type": "string" }
         }
      }
   ],
   "required": [ "name" ]
}
```

Cyber Observable Core

Common properties and behavior across all Cyber Observable Objects.

```
{
   "id": "../common/cyber-observable-core.json",
   "title": "cyber-observable-core",
   "type": "object",
   "properties": {
      "type": { "type": "string", "pattern": "^\\-?[a-z0-9]+(-[a-z0-9]+)*\\-?$" },
      "extensions": { "$ref": "dictionary.json" }
   },
   "patternProperties": {
      "^[a-z0-9_]{0,246}_bin$": { "$ref": "binary.json" },
      "^[a-z0-9_]{3,250}$": { "anyOf": [ { "type": "array" }, { "type": "string" }, { "type": "integer" }, { "type": "boole
an" }, { "type": "number" }, { "type": "object" } ] }
   },
   "required": [ "type" ]
}
```

Dictionary

A dictionary captures a set of key/value pairs

```
{
   "id": "../common/dictionary.json",
   "title": "dictionary",
   "type": "object",
   "patternProperties": {
      "^[a-zA-Z0-9_-]{3,256}$": { "anyOf": [ { "type": "array" }, { "type": "string" }, { "type": "integer" }, { "type": "b
oolean" }, { "type": "number" }, { "type": "object" } ] }
   }
}
```

Directory

The Directory Object represents the properties common to a file system directory.

```
{
   "id": "../observables/directory.json",
   "title": "directory",
   "type": "object",
   "allOf": [
      { "$ref": "../common/cyber-observable-core.json" },
      {
         "properties": {
            "type": { "type": "string", "enum": [ "directory" ] },
            "path": { "type": "string" },
            "path_enc": { "type": "string", "pattern": "^[a-zA-Z0-9/\\.+_:-]{2,250}$" },
            "created": { "$ref": "../common/timestamp.json" },
            "modified": { "$ref": "../common/timestamp.json" },
            "accessed": { "$ref": "../common/timestamp.json" },
            "contains_refs": { "type": "array", "items": { "type": "string" }, "minItems": 1 }
         },
         "required": [ "path" ]
      }
   ]
}
```

Domain Name

The Domain Name represents the properties of a network domain name.

```
{
  "id": "../observables/domain-name.json",
  "title": "domain-name",
  "type": "object",
  "allOf": [
    { "$ref": "../common/cyber-observable-core.json" },
    {
      "properties": {
        "type": { "type": "string", "enum": [ "domain-name" ] },
        "value": { "type": "string" },
        "resolves_to_refs": { "type": "array", "items": { "type": "string" } }
      },
      "required": [ "value" ]
    }
  ]
}
```

Email Addr

The Email Address Object represents a single email address.

```
{
  "id": "../observables/email-addr.json",
  "title": "email-addr",
  "type": "object",
  "allOf": [
    { "$ref": "../common/cyber-observable-core.json" },
    {
      "properties": {
        "type": { "type": "string", "enum": [ "email-addr" ] },
        "value": { "type": "string", "pattern": "(^[a-zA-Z0-9_.+-]+@[a-zA-Z0-9-]+\\.[a-zA-Z0-9-.]+$)" },
        "display_name": { "type": "string" },
        "belongs_to_ref": { "type": "string" }
      },
      "required": [ "value" ]
    }
  ]
}
```

Email Message

The Email Message Object represents an instance of an email message.

```
{
  "id": "../observables/email-message.json",
  "title": "email-message",
  "type": "object",
  "allOf": [
    { "$ref": "../common/cyber-observable-core.json" },
    {
      "properties": {
        "type": { "type": "string", "enum": [ "email-message" ] },
        "date": { "$ref": "../common/timestamp.json" },
        "content_type": { "type": "string" },
        "from_ref": { "type": "string" },
        "sender_ref": { "type": "string" },
        "to_refs": { "type": "array", "items": { "type": "string" } },
        "cc_refs": { "type": "array", "items": { "type": "string" } },
        "bcc_refs": { "type": "array", "items": { "type": "string" } },
        "subject": { "type": "string" },
        "received_lines": { "type": "array", "items": { "type": "string" } },
        "additional_header_fields": { "$ref": "#/definitions/email-additional-header-fields" },
        "raw_email_ref": { "type": "string" }
      }
    }
  ],
  "oneOf": [
    {
      "properties": {
        "is_multipart": { "type": "boolean", "enum": [ false ] },
        "body": { "type": "string" }
      },
      "required": [ "is_multipart" ]
    },
    {
      "properties": {
        "is_multipart": { "type": "boolean", "enum": [ true ] },
        "body_multipart": { "type": "array", "items": { "$ref": "#/definitions/mime-part-type" } }
      },
      "required": [ "is_multipart" ]
    }
  ]
}
```

External Reference

External references are used to describe pointers to information represented outside of STIX.

```
{
  "id": "../common/external-reference.json",
  "title": "external-reference",
  "type": "object",
  "properties": {
    "description": { "type": "string" },
    "url": { "$ref": "url-regex.json" },
    "hashes": { "$ref": "hashes-type.json" }
  },
  "oneOf": [
    {
      "properties": {
        "source_name": { "type": "string", "pattern": "^cve$" },
        "external_id": { "type": "string", "pattern": "^CVE-\\d{4}-(0\\d{3}|[1-9]\\d{3,})$" }
      },
      "required": [ "source_name", "external_id" ]
    },
    {
      "properties": {
        "source_name": { "type": "string", "pattern": "^capec$" },
        "external_id": { "type": "string", "pattern": "^CAPEC-\\d+$" }
      },
      "required": [ "source_name", "external_id" ]
    },
    {
      "properties": {
        "source_name": { "type": "string", "not": { "pattern": "^(cve)|(capec)$" } },
        "external_id": { "type": "string" }
      },
      "required": [ "source_name" ]
    }
  ]
}
```

File

The File Object represents the properties of a file.

```
{
   "id": "../observables/file.json",
   "title": "file",
   "type": "object",
   "allOf": [
      { "$ref": "../common/cyber-observable-core.json" },
      {
         "properties": {
            "type": { "type": "string", "enum": [ "file" ] },
            "extensions": { "$ref": "#/definitions/file-extensions-dictionary" },
            "hashes": { "$ref": "../common/hashes-type.json" },
            "size": { "type": "integer", "minimum": 0 },
            "name": { "type": "string" },
            "name_enc": { "type": "string" },
            "magic_number_hex": { "$ref": "../common/hex.json" },
            "mime_type": { "type": "string" },
            "created": { "$ref": "../common/timestamp.json" },
            "modified": { "$ref": "../common/timestamp.json" },
            "accessed": { "$ref": "../common/timestamp.json" },
            "parent_directory_ref": { "type": "string" },
            "contains_refs": { "type": "array", "items": { "type": "string" }, "minItems": 1 },
            "content_ref": { "type": "string" }
         }
      }
   ]
}
```

Granular Marking

The granular-marking type defines how the list of marking-definition objects referenced by the marking_refs property to apply to a set of content identified by the list of selectors in the selectors property.

```
{
   "id": "../common/granular-marking.json",
   "title": "granular-marking",
   "type": "object",
   "properties": {
      "selectors": { "type": "array", "items": { "type": "string", "pattern": "^[a-z0-9_-]{3,250}(\\.(\\[\\d+\\]|[a-z0-9_-]{1,
250}))*$" }, "minItems": 1 },
      "marking_ref": { "allOf": [ { "$ref": "identifier.json" }, { "pattern": "^marking-definition--" } ] }
   },
   "required": [ "selectors", "marking_ref" ]
}
```

Hashes

A dictionary captures a set of key/value pairs

```
{
  "id": "../common/hashes-type.json",
  "title": "hashes",
  "type": "object",
  "patternProperties": {
    "^[a-zA-Z0-9_-]{3,256}$": { "type": "string", "description": "Custom hash key" },
    "^MD5$": { "type": "string", "pattern": "^[a-fA-F0-9]{32}$" },
    "^MD6$": { "type": "string" },
    "^RIPEMD-160$": { "type": "string", "pattern": "^[a-fA-F0-9]{40}$" },
    "^SHA-1$": { "type": "string", "pattern": "^[a-fA-F0-9]{40}$" },
    "^SHA-224$": { "type": "string", "pattern": "^[a-fA-F0-9]{56}$" },
    "^SHA-256$": { "type": "string", "pattern": "^[a-fA-F0-9]{64}$" },
    "^SHA-384$": { "type": "string", "pattern": "^[a-fA-F0-9]{96}$" },
    "^SHA-512$": { "type": "string", "pattern": "^[a-fA-F0-9]{128}$" },
    "^SHA3-224$": { "type": "string", "pattern": "^[a-fA-F0-9]{56}$" },
    "^SHA3-256$": { "type": "string", "pattern": "^[a-fA-F0-9]{64}$" },
    "^SHA3-384$": { "type": "string", "pattern": "^[a-fA-F0-9]{96}$" },
    "^SHA3-512$": { "type": "string", "pattern": "^[a-fA-F0-9]{128}$" },
    "^ssdeep$": { "type": "string", "pattern": "^[a-zA-Z0-9/+:.]{1,128}$" },
    "^WHIRLPOOL$": { "type": "string", "pattern": "^[a-fA-F0-9]{128}$" }
  }
}
```

Hex

The hex data type encodes an array of octets (8-bit bytes) as hexadecimal.

```
{
  "id": "../common/hex.json",
  "title": "hex",
  "type": "string",
  "pattern": "^([a-fA-F0-9]{2})+$"
}
```

Identifier

Represents identifiers across the CTI specifications.

```
{
  "id": "../common/identifier.json",
  "title": "identifier",
  "type": "string",
  "pattern": "^[a-z][a-z-]+[a-z]--[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$"
}
```

Identity

Identities can represent actual individuals, organizations, or groups.

```
{
   "id": "../sdos/identity.json",
   "title": "identity",
   "type": "object",
   "allOf": [
      { "$ref": "../common/core.json" },
      {
         "properties": {
            "type": { "type": "string", "enum": [ "identity" ] },
            "id": { "title": "id", "pattern": "^identity--" },
            "labels": { "type": "array", "items": { "type": "string" }, "minItems": 1 },
            "name": { "type": "string" },
            "description": { "type": "string" },
            "identity_class": { "type": "string" },
            "sectors": { "type": "array", "items": { "type": "string" }, "minItems": 1 },
            "contact_information": { "type": "string" }
         },
         "required": [ "name", "identity_class" ]
      }
   ]
}
```


Indicator

Indicators contain a pattern that can be used to detect suspicious or malicious cyber activity.


```
{
   "id": "../sdos/indicator.json",
   "title": "indicator",
   "type": "object",
   "allOf": [
      { "$ref": "../common/core.json" },
      {
         "properties": {
            "type": { "type": "string", "enum": [ "indicator" ] },
            "id": { "title": "id", "pattern": "^indicator--" },
            "labels": { "type": "array", "items": { "type": "string" }, "minItems": 1 },
            "name": { "type": "string" },
            "description": { "type": "string" },
            "pattern": { "type": "string" },
            "valid_from": { "$ref": "../common/timestamp.json" },
            "valid_until": { "$ref": "../common/timestamp.json" },
            "kill_chain_phases": { "type": "array", "items": { "$ref": "../common/kill-chain-phase.json" }, "minItems": 1 }
         }
      }
   ],
   "required": [ "pattern", "labels", "valid_from" ]
}
```


Intrusion Set

An Intrusion Set is a grouped set of adversary behavior and resources with common properties that is believed to be orchestrated by a single organization.

```
{
  "id": "../sdos/intrusion-set.json",
  "title": "intrusion-set",
  "type": "object",
  "allOf": [
    { "$ref": "../common/core.json" },
    {
      "properties": {
        "type": { "type": "string", "enum": [ "intrusion-set" ] },
        "id": { "title": "id", "pattern": "^intrusion-set--" },
        "name": { "type": "string" },
        "description": { "type": "string" },
        "aliases": { "type": "array", "items": { "type": "string" }, "minItems": 1 },
        "first_seen": { "$ref": "../common/timestamp.json" },
        "last_seen": { "$ref": "../common/timestamp.json" },
        "goals": { "type": "array", "items": { "type": "string" }, "minItems": 1 },
        "resource_level": { "type": "string" },
        "primary_motivation": { "type": "string" },
        "secondary_motivations": { "type": "array", "items": { "type": "string" }, "minItems": 1 }
      }
    }
  ],
  "required": [ "name" ]
}
```

Investigation

Investigations are an exploration of the facts involved in a cyber-relevant set of suspicious activity.

Property	Object	Description
Investigation ID	"id"	The investigation ID. example: 1-15607
Title	"name"	The title of the investigation
Summary	"description"	The summary that provides more context and details about the investigation.
Status	"investigation_status"	The status of the investigation shown on the top right of the page.

```
{
   "id": "../sdos/investigation.json",
   "title": "investigation",
   "type": "object",
   "allOf": [
      { "$ref": "../common/core.json" },
      {
         "properties": {
            "type": { "type": "string", "enum": [ "x-fireeye-com-investigation" ] },
            "id": { "title": "id", "pattern": "^x-fireeye-com-investigation--" },
            "name": { "type": "string" },
            "description": { "type": "string" },
            "investigation_status": { "$ref": "../vocabularies/investigation-status-ov.json" },
            "investigation_form": { "$ref": "../vocabularies/investigation-form-ov.json" },
            "focus": { "type": "string" },
            "start_time": { "$ref": "../common/timestamp.json" },
            "end_time": { "$ref": "../common/timestamp.json" },
            "object_refs": { "type": "array", "items": { "$ref": "../common/identifier.json" }, "minItems": 1 }
         }
      }
   ],
   "required": [ "name", "investigation_status", "investigation_form", "object_refs" ]
}
```

Investigation Failure Response

Response for a failed request for investigations

```
{
   "id": "../investigations/failure-response.json",
   "title": "investigation-failure-response",
   "type": "object",
   "properties": {
      "errors": { "type": "array", "items": { "type": "string" } }
   },
   "required": [ "errors" ]
}
```

Investigation Form Ov

Open Vocabulary for expressing the form of an Investigation.

```
{
   "id": "../vocabularies/investigation-form-ov.json",
   "title": "investigation-form-ov",
   "oneOf": [
      { "type": "string", "pattern": "^suspicious-activity$" },
      { "type": "string", "pattern": "^incident$" },
      { "type": "string", "pattern": "^case$" },
      { "type": "string", "pattern": "^in-depth-intel-analysis$" },
      { "type": "string", "not": { "enum": [ "suspicious-activity", "incident", "case", "in-depth-intel-analysis" ] } }
   ]
}
```

Investigation Status Ov

Open Vocabulary for expressing the status of an Investigation.

```
{
  "id": "../vocabularies/investigation-status-ov.json",
  "title": "investigation-status-ov",
  "oneOf": [
    { "type": "string", "pattern": "^open$" },
    { "type": "string", "pattern": "^active$" },
    { "type": "string", "pattern": "^paused$" },
    { "type": "string", "pattern": "^closed-resolved$" },
    { "type": "string", "pattern": "^closed-false-positive$" },
    { "type": "string", "pattern": "^dismissed$" },
    { "type": "string", "not": { "enum": [ "open", "active", "paused", "closed-resolved", "closed-false-positive", "dismi
ssed" ] } }
  ]
}
```

Investigation Successful Response

A successful response for a group of investigations, or a single investigation.

```
{
  "id": "../investigations/successful-response.json",
  "title": "investigation-successful-response",
  "type": "object",
  "properties": {
    "data": { "$ref": "../common/bundle.json" },
    "meta": { "type": "object", "additionalProperties": true }
  },
  "required": [ "data" ]
}
```

Ipv4 Addr

The IPv4 Address Object represents one or more IPv4 addresses expressed using CIDR notation.

```
{
  "id": "../observables/ipv4-addr.json",
  "title": "ipv4-addr",
  "type": "object",
  "allOf": [
    { "$ref": "../common/cyber-observable-core.json" },
    {
      "properties": {
        "type": { "type": "string", "enum": [ "ipv4-addr" ] },
        "value": { "type": "string" },
        "resolves_to_refs": { "type": "array", "items": { "type": "string" }, "minItems": 1 },
        "belongs_to_refs": { "type": "array", "items": { "type": "string" }, "minItems": 1 }
      },
      "required": [ "value" ]
    }
  ]
}
```

Ipv6 Addr

The IPv6 Address Object represents one or more IPv6 addresses expressed using CIDR notation.

```
{
  "id": "../observables/ipv6-addr.json",
  "title": "ipv6-addr",
  "type": "object",
  "allOf": [
    { "$ref": "../common/cyber-observable-core.json" },
    {
      "properties": {
        "type": { "type": "string", "enum": [ "ipv6-addr" ] },
        "value": { "type": "string" },
        "resolves_to_refs": { "type": "array", "items": { "type": "string" }, "minItems": 1 },
        "belongs_to_refs": { "type": "array", "items": { "type": "string" }, "minItems": 1 }
      },
      "required": [ "value" ]
    }
  ]
}
```

Kill Chain Phase

The kill-chain-phase represents a phase in a kill chain.

```
{
  "id": "../common/kill-chain-phase.json",
  "title": "kill-chain-phase",
  "type": "object",
  "properties": {
    "kill_chain_name": { "type": "string" },
    "phase_name": { "type": "string" }
  },
  "required": [ "kill_chain_name", "phase_name" ]
}
```

Mac Addr

The MAC Address Object represents a single Media Access Control (MAC) address.

```
{
  "id": "../observables/mac-addr.json",
  "title": "mac-addr",
  "type": "object",
  "allOf": [
    { "$ref": "../common/cyber-observable-core.json" },
    {
      "properties": {
        "type": { "type": "string", "enum": [ "mac-addr" ] },
        "value": { "type": "string", "pattern": "^([0-9a-f]{2}[:]){5}([0-9a-f]{2})$" }
      },
      "required": [ "value" ]
    }
  ]
}
```

Malware

Malware is a type of TTP that is also known as malicious code and malicious software, refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system (OS) or of otherwise annoying or disrupting the victim.


```
{
   "id": "../sdos/malware.json",
   "title": "malware",
   "type": "object",
   "allOf": [
      { "$ref": "../common/core.json" },
      {
         "properties": {
            "type": { "type": "string", "enum": [ "malware" ] },
            "id": { "title": "id", "pattern": "^malware--" },
            "labels": { "type": "array", "items": { "type": "string" }, "minItems": 1 },
            "name": { "type": "string" },
            "description": { "type": "string" },
            "kill_chain_phases": { "type": "array", "items": { "$ref": "../common/kill-chain-phase.json" }, "minItems": 1 }
         }
      }
   ],
   "required": [ "name", "labels" ]
}
```


Marking Definition

The marking-definition object represents a specific marking.

```
{
  "id": "../common/marking-definition.json",
  "title": "marking-definition",
  "type": "object",
  "properties": {
    "type": { "type": "string", "enum": [ "marking-definition" ] },
    "created_by_ref": { "$ref": "identifier.json" },
    "created": { "$ref": "timestamp.json" },
    "external_references": { "type": "array", "items": { "$ref": "external-reference.json" }, "minItems": 1 },
    "object_marking_refs": { "type": "array", "items": { "allOf": [ { "$ref": "identifier.json" }, { "pattern": "^marking-definition--" } ] }, "minItems": 1 },
    "granular_markings": { "type": "array", "items": { "$ref": "granular-marking.json" }, "minItems": 1 }
  },
  "oneOf": [
    {
      "properties": {
        "id": { "allOf": [ { "$ref": "identifier.json" }, { "title": "id", "pattern": "^marking-definition--" } ] },
        "definition_type": { "type": "string" },
        "definition": { "type": "object" }
      },
      "required": [ "id", "type", "definition", "definition_type", "created" ]
    },
    {
      "properties": {
        "definition_type": { "type": "string", "enum": [ "tlp" ] }
      },
      "oneOf": [
        { "$ref": "#/definitions/tlp_white" },
        { "$ref": "#/definitions/tlp_green" },
        { "$ref": "#/definitions/tlp_amber" },
        { "$ref": "#/definitions/tlp_red" }
      ]
    }
  ]
}
```

Mutex

The Mutex Object represents the properties of a mutual exclusion (mutex) object.

```
{
  "id": "../observables/mutex.json",
  "title": "mutex",
  "type": "object",
  "allOf": [
    { "$ref": "../common/cyber-observable-core.json" },
    {
      "properties": {
        "type": { "type": "string", "enum": [ "mutex" ] },
        "name": { "type": "string" }
      },
      "required": [ "name" ]
    }
  ]
}
```

Network Traffic

The Network Traffic Object represents arbitrary network traffic that originates from a source and is addressed to a destination.


```json
{
  "id": "../observables/network-traffic.json",
  "title": "network-traffic",
  "type": "object",
  "allOf": [
    { "$ref": "../common/cyber-observable-core.json" },
    {
      "properties": {
        "type": { "type": "string", "enum": [ "network-traffic" ] },
        "extensions": { "$ref": "#/definitions/network-traffic-extensions-dictionary" },
        "start": { "$ref": "../common/timestamp.json" },
        "end": { "$ref": "../common/timestamp.json" },
        "src_ref": { "type": "string" },
        "dst_ref": { "type": "string" },
        "src_port": { "type": "integer", "minimum": 0, "maximum": 65535 },
        "dst_port": { "type": "integer", "minimum": 0, "maximum": 65535 },
        "protocols": { "type": "array", "items": { "type": "string" }, "minItems": 1 },
        "src_byte_count": { "type": "integer" },
        "dst_byte_count": { "type": "integer" },
        "src_packets": { "type": "integer" },
        "dst_packets": { "type": "integer" },
        "ipfix": { "type": "object" },
        "src_payload_ref": { "type": "string" },
        "dst_payload_ref": { "type": "string" },
        "encapsulates_refs": { "type": "array", "items": { "type": "string" } },
        "encapsulated_by_ref": { "type": "string" }
      }
    }
  ],
  "required": [ "protocols" ]
}
```


Note

A Note is a comment or note containing informative text to help explain the context of one or more STIX Objects (SDOs or SROs) or to provide additional analysis that is not contained in the original object.

```
{
  "id": "../sdos/note.json",
  "title": "note",
  "type": "object",
  "allOf": [
    { "$ref": "../common/core.json" },
    {
      "properties": {
        "type": { "type": "string", "enum": [ "x-fireeye-com-note" ] },
        "id": { "title": "id", "pattern": "^x-fireeye-com-note--" },
        "x_fireeye_com_note_type": { "$ref": "../vocabularies/note-type-ov.json" },
        "description": { "type": "string" },
        "summary": { "type": "string" },
        "authors": { "type": "array", "items": { "type": "string" } },
        "object_refs": { "type": "array", "items": { "$ref": "../common/identifier.json" }, "minItems": 1 }
      }
    }
  ],
  "required": [ "description", "object_refs" ]
}
```

Note Type Ov

Open Vocabulary for expressing the type of a Note.

```
{
  "id": "../vocabularies/note-type-ov.json",
  "title": "note-type-ov",
  "oneOf": [
    { "type": "string", "pattern": "^comment$" },
    { "type": "string", "pattern": "^finding$" },
    { "type": "string", "not": { "enum": [ "comment", "finding" ] } }
  ]
}
```

Observed Data

Observed data conveys information that was observed on systems and networks, such as log data or network traffic, using the Cyber Observable specification.

```
{
  "id": "../sdos/observed-data.json",
  "title": "observed-data",
  "type": "object",
  "allOf": [
    { "$ref": "../common/core.json" }
  ]
}
```

Filtering

The Investigations API supports a `filter` query parameter to narrow down results based on specific timestamps and investigation states. Filters use a simple query language consisting of fields, conditional operators, and logical conjunctions.

Filter parameters

Component	Accepted Values
Fields	`published`, `modified`, `investigation_status`
Operators	`>=` (Greater than or equal), `<=` (Less than or equal), `=` (Equal)
Conjunction	`AND` (Note: `OR` and `NOT` are not supported)

Investigation status values

The `investigation_status` field accepts the following case-insensitive values:

- `open`
- `resolved`
- `false-positive`
- `disputed`

Filter examples

Query Type	Example URL Path
Published After	`/investigations?filter="published >= yyyy-mm-ddTHH:MM:SSZ"`
Status Filter	`/investigations?filter="investigation_status = 'open'"`
Complex Filter	`/investigations?filter="published >= 2023-01-01T00:00:00Z AND investigation_status = 'resolved'"`
Date Range (Modified)	`/investigations?filter="modified >= [Start] AND modified <= [End]"`

Error Handling

If the filter parameter is improperly formatted, uses unsupported operators, or contains invalid values, the API returns a **400 Bad Request** response:

```
{
  "errors": ["Invalid filter parameters. Please refer to the API documentation for the correct parameter format."]
}
```

Investigation Status Ov

Open Vocabulary for expressing the status of an Investigation:

```
{
  "id": "../vocabularies/investigation-status-ov.json",
  "title": "investigation-status-ov",
  "oneOf": [
    { "type": "string", "pattern": "^open$" },
    { "type": "string", "pattern": "^resolved$" },
    { "type": "string", "pattern": "^false-positive$" },
    { "type": "string", "pattern": "^disputed$" }
  ]
}
```

/investigations

/investigations get

Mandiant

GET: `/investigations` (secured)

Returns a STIX Bundle containing a group of Investigation objects. Pointers to objects that the investigation references are included in the `object_refs` property of each Investigation object, but the referenced objects are not themselves included. Each page returns 10 investigations by default.

Query Parameters

- **filter**: (optional, type: string) Restricts results based on `published`, `modified`, or `investigation_status`.
- **page**: (optional, type: integer) The page value to return.

Possible Responses: 200, 400, 500

CURL EXAMPLE (With Pagination)

```
curl -X GET "https://api.services.mandiant.com/investigations?filter=%22investigation_status%20%3D%20'open'%22&page=2" \
  -H "Authorization: Bearer string"
```