ThreatQuotient

Elastic Security CDF User Guide

Version 1.0.1

January 16, 2024

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com
Support Web: https://support.threatq.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.1
Compatible with ThreatQ Versions	>= 5.18.0
Compatible with Elastic Security Versions	>=8.x
Support Tier	ThreatQ Supported

Introduction

The Elastic Security CDF allows the automatic ingestion of alerts and cases from Elastic Security into ThreatQ. This enables analysts in ThreatQ to stay up to date with the latest alerts and cases, as well as enabling platform to re-prioritize indicators based on sightings.

Elastic Security unifies SIEM, endpoint security, and cloud security on an open platform, arming SecOps teams to protect, detect, and respond at scale. These analytical and protection capabilities, leveraged by the speed and extensibility of Elasticsearch, enable analysts to defend their organization from threats before damage and loss occur.

The integration provides the following feeds:

- **Elastic Security Alerts** - pulls alerts from Elastic Security into ThreatQ.
- **Elastic Security Cases** - pulls cases from Elastic Security into ThreatQ.

The integration ingests the following system objects:

- Assets
- Attack Patterns
- Events
- Incidents
- Indicators

Prerequisites

The integration requires the following to run:

- Elastic Security v8.x and newer.
- Credentials for the Elasticsearch API
- Credentials for the Kibana API

Installation

Perform the following steps to install the integration:

> The same steps can be used to upgrade the integration to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the yaml file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the yaml file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the file on your local machine

   > ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.

6. When prompted, select the individual feeds to install and click **Install**. The feed(s) will be added to the integrations page.

You will still need to configure and then enable the feed(s).

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

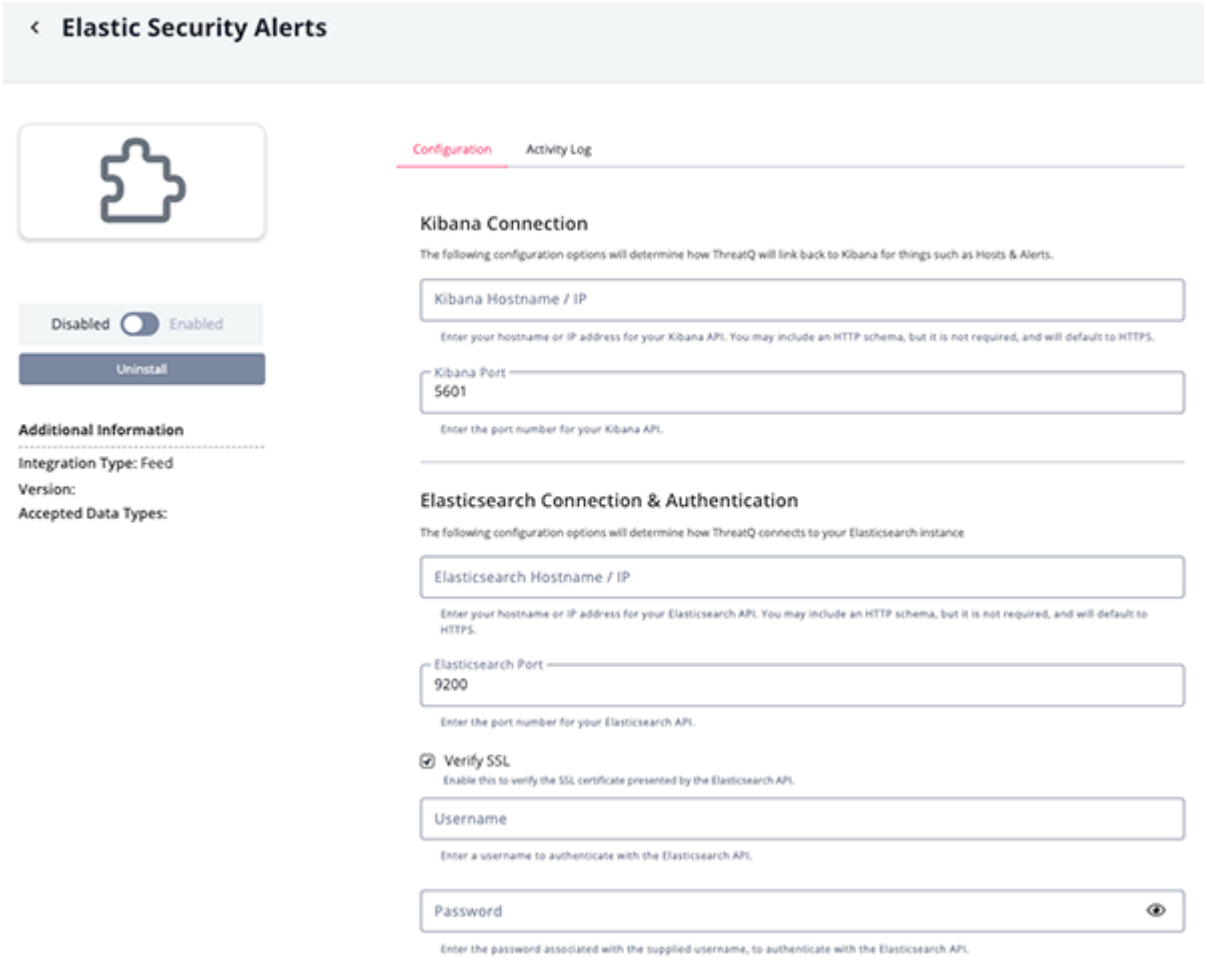
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

Elastic Security Alerts Parameters

PARAMETER	DESCRIPTION
Kibana Connection	
Kibana Hostname / IP	Enter your hostname or IP address for your Kibana API. > You may include an HTTP schema, but it is not required, and will default to HTTPS.
Kibana Port	Enter the port number for your Kibana API. The default value is 5601.
Elasticsearch Connection & Authentication	
Elasticsearch Hostname / IP	Enter your hostname or IP address for your Elasticsearch API. > You may include an HTTP schema, but it is not required, and will default to HTTPS.

PARAMETER	DESCRIPTION
Elastic Port	Enter the port number for your Elasticsearch API. The default value is 9200.
Verify SSL	Enter the port number for your Elasticsearch API. The default value is 9200.
Username	Enter a username to authenticate with the Elasticsearch API.
Password	Enter the password associated with the supplied username, to authenticate with the Elasticsearch API.
Search Options	
Custom Query	Optional - Enter a query in the Lucene query string syntax to filter the search results. This field does not support the full Elasticsearch Query DSL. This query will get appended to the time range query that is default to this feed.
Ingest Options	
Alert Context	Select which pieces of context you would like brought in with each alert. Options include: ◦ Related Indicators (default) ◦ Tags (default) ◦ Elastic Alert ID ◦ Elastic Alert Link ◦ Severity (default) ◦ Risk Score (default) ◦ MITRE Tactics (default) ◦ MITRE Techniques (default)
Alert Description Context	Select which pieces of context you would like brought into the description of each alert. Options include: ◦ Event Details (default) ◦ Rule Details (default) ◦ Raw Event Message (default) ◦ Winlog Details

PARAMETER	DESCRIPTION
Ingest Affected Hosts	Enable this parameter to ingest and relate the affected host with each alert. This parameter is enabled by default.
Host Context	If you have enabled the **Ingest Affected Hosts** parameter, select which pieces of context you would like brought in with each host. Options include: ◦ Elastic Host ID ◦ Elastic Host Link ◦ MAC Address ◦ Hostname (default) ◦ IP Address (default) ◦ Architecture ◦ Operating System (default) This section will only be displayed if you have enabled the **Ingest Affected Hosts** parameter.



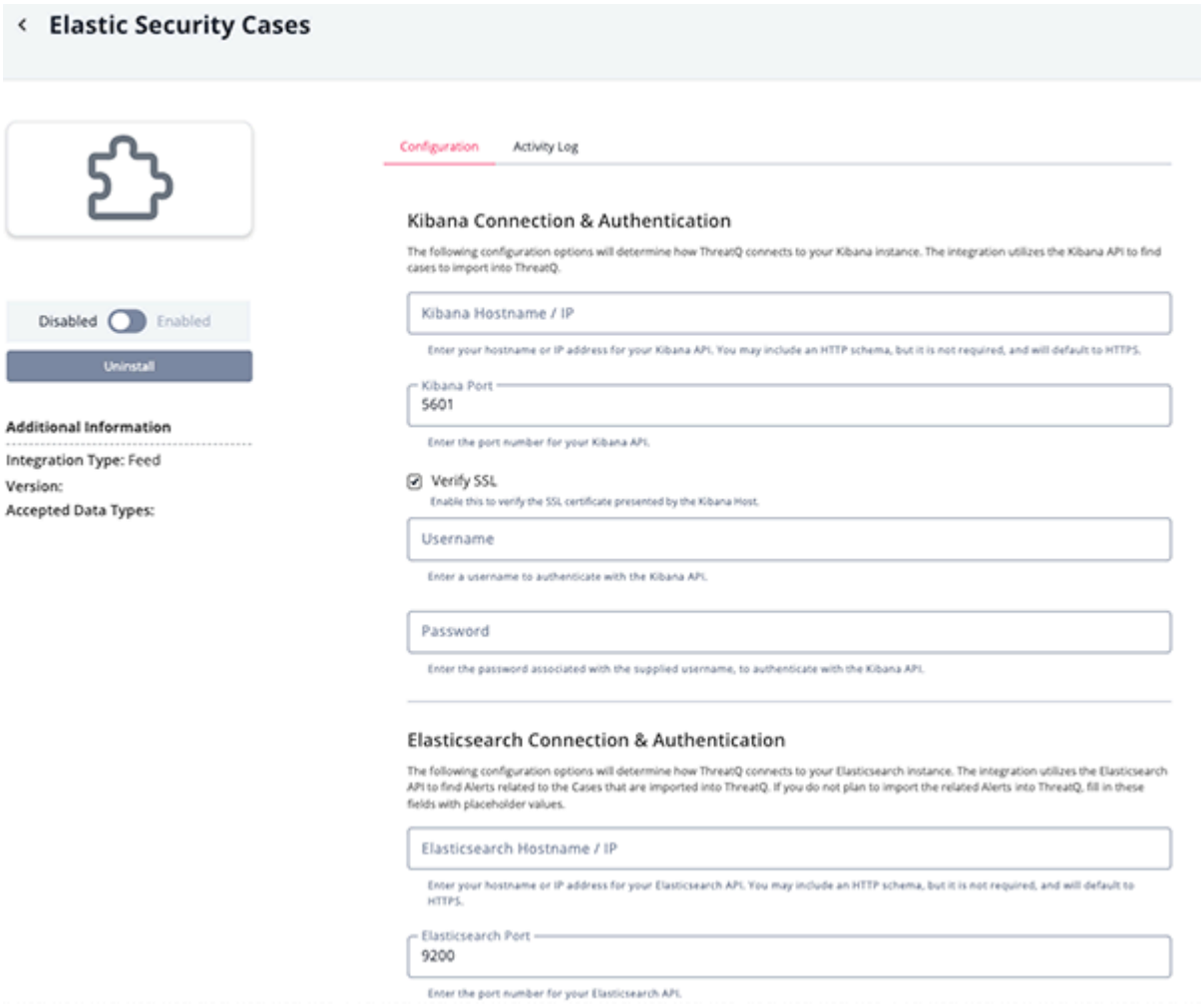
Elastic Security Cases Parameters

PARAMETER	DESCRIPTION
Kibana Connection & Authentication	
Kibana Hostname / IP	Enter your hostname or IP address for your Kibana API.  You may include an HTTP schema, but it is not required, and will default to HTTPS.
Kibana Port	Enter the port number for your Kibana API. The default value is 5601.
Verify SSL	Enable this to verify the SSL certificate presented by the Kibana API.
Username	Enter a username to authenticate with the Kibana API.
Password	Enter the password associated with the supplied username, to authenticate with the Kibana API.
Elasticsearch Connection & Authentication	
Elasticsearch Hostname / IP	Enter your hostname or IP address for your Elasticsearch API.  You may include an HTTP schema, but it is not required, and will default to HTTPS.
Elastic Port	Enter the port number for your Elasticsearch API. The default value is 9200.
Verify SSL	Enter the port number for your Elasticsearch API. The default value is 9200.
Username	Enter a username to authenticate with the Elasticsearch API.

PARAMETER	DESCRIPTION
Password	Enter the password associated with the supplied username, to authenticate with the Elasticsearch API.
Search Options	
Search	Optional - Enter a search term to filter cases by. This will search across both the title and description of each case.
Severity Filter	Select which cases to import into ThreatQ based on their severity level. Options include: ◦ Low ◦ Medium ◦ High (default) ◦ Critical (default)
Ingest Options	
Ingest Comments	Enable this parameter to ingest the comments from each case. This parameter is enabled by default.
Ingest Related Alerts	Enable this parameter to ingest and relate the related alerts with each case. This parameter is enabled by default.
Alert Context	Select which pieces of context you would like brought in with each alert. Options include: ◦ Related Indicators (default) ◦ Tags (default) ◦ Elastic Alert ID ◦ Elastic Alert Link ◦ Severity (default) ◦ Risk Score (default) ◦ MITRE Tactics (default) ◦ MITRE Techniques (default)

This section will only be displayed if you have enabled the **Ingest Related Alerts** option under *Ingest Options*.

PARAMETER	DESCRIPTION
Alert Description Context	Select which pieces of context you would like brought into the description of each alert. Options include: ◦ Event Details (default) ◦ Rule Details (default) ◦ Raw Event Message (default) ◦ Winlog Details This section will only be displayed if you have enabled the **Ingest Related Alerts** option under *Ingest Options*.
Ingest Affected Hosts	Enable this parameter to ingest and relate the affected host with each alert. This parameter is enabled by default.
Host Context	If you have enabled the **Ingest Affected Hosts** parameter, select which pieces of context you would like brought in with each host. Options include: ◦ Elastic Host ID ◦ Elastic Host Link ◦ MAC Address ◦ Hostname (default) ◦ IP Address (default) ◦ Architecture ◦ Operating System (default) This section will only be displayed if you have enabled the **Ingest Affected Hosts** parameter.



5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

Elastic Security Alerts

The Elastic Security Alerts feed periodically pulls alerts from Elastic Security's default alert index into ThreatQ. Alerts will include context about the rule that was triggered, as well as any Threat Intelligence indicator enrichment matches.

`GET https://{elasticsearch_host}:{elasticsearch_port}/.alerts-security.alerts-default/_search`

Sample Response:


```
{
  "took": 5,
  "timed_out": false,
  "_shards": {
    "total": 6,
    "successful": 6,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": {
      "value": 1,
      "relation": "eq"
    },
    "max_score": null,
    "hits": [
      {
        "_index": ".internal.alerts-security.alerts-default-000006",
        "_id":
"f56c18f3fa4f56ea8284357078fac19b30e1b465872cd5bbf110d5495e64bae9",
        "_score": null,
        "_source": {
          "kibana.alert.start": "2023-10-27T14:49:36.437Z",
          "kibana.alert.last_detected": "2023-10-27T14:49:36.437Z",
          "kibana.version": "8.8.2",
          "kibana.alert.rule.parameters": {
            "description": "Test",
            "risk_score": 57,
            "severity": "medium",
            "license": "",
            "meta": {
              "from": "5m",
              "kibana_siem_app_url": "http://192.168.50.126:5601/app/security"
            },
            "author": [],
```

```
"false_positives": [],
"from": "now-420s",
"rule_id": "91266588-3f85-4d56-a7f1-70bd57927a61",
"max_signals": 100,
"risk_score_mapping": [],
"severity_mapping": [],
"threat": [],
"to": "now",
"references": [],
"version": 1,
"exceptions_list": [],
"immutable": false,
"related_integrations": [],
"required_fields": [],
"setup": "",
"type": "threat_match",
"language": "kuery",
"index": ["winlog-*"],
"query": "*:*",
"filters": [],
"threat_filters": [
  {
    "meta": {
      "type": "combined",
      "relation": "AND",
      "params": [
        {
          "query": {
            "match_phrase": {
              "threat.indicator.type": "unknown"
            }
          },
          "meta": {
            "negate": true,
            "key": "threat.indicator.type",
            "field": "threat.indicator.type",
            "params": {
              "query": "unknown"
            },
            "type": "phrase",
            "disabled": false,
            "alias": null
          }
        },
        {
          "meta": {
            "negate": false,
            "key": "agent.name",
            "field": "agent.name",
            "params": {
```

```
                        "query": "ThreatQ"
                      },
                      "type": "phrase",
                      "disabled": false,
                      "alias": null
                    },
                    "query": {
                      "match_phrase": {
                        "agent.name": "ThreatQ"
                      }
                    }
                  }
                ],
                "disabled": false,
                "negate": false,
                "alias": null
              },
              "query": {},
              "$state": {
                "store": "appState"
              }
            }
          ],
          "threat_query": "",
          "threat_mapping": [
            {
              "entries": [
                {
                  "field": "destination_ip",
                  "type": "mapping",
                  "value": "threat.indicator.ip"
                }
              ]
            }
          ],
          "threat_language": "kuery",
          "threat_index": ["filebeat-*"],
          "threat_indicator_path": "threat.indicator"
        },
        "kibana.alert.rule.category": "Indicator Match Rule",
        "kibana.alert.rule.consumer": "siem",
        "kibana.alert.rule.execution.uuid": "1d3e21cf-
d611-4ccb-96d8-4e02bdf4259a",
        "kibana.alert.rule.name": "ThreatQ IOC Match",
        "kibana.alert.rule.producer": "siem",
        "kibana.alert.rule.revision": 3,
        "kibana.alert.rule.rule_type_id": "siem.indicatorRule",
        "kibana.alert.rule.uuid": "a2347660-74d4-11ee-9fe5-e706bbe42d7f",
        "kibana.space_ids": ["default"],
        "kibana.alert.rule.tags": [],
```

```
          "@timestamp": "2023-10-27T14:49:36.421Z",
          "destination_ip": "192.206.249.184",
          "timestamp": "2023-10-27T10:47:00",
          "threat": {
            "enrichments": [
              {
                "indicator": {
                  "confidence": "Low",
                  "ip": "192.206.249.184",
                  "type": "ipv4-addr",
                  "port": 80,
                  "provider": "ThreatQuotient"
                },
                "feed": {
                  "name": "[Filebeat] ThreatQuotient"
                },
                "matched": {
                  "atomic": "192.206.249.184",
                  "field": "destination_ip",
                  "id": "U8EufPnem4Atz+D7CHikv/Iepfw=",
                  "index": ".ds-filebeat-8.8.1-2023.10.03-000004",
                  "type": "indicator_match_rule"
                }
              }
            ]
          },
          "event.kind": "signal",
          "kibana.alert.original_time": "2023-10-27T14:47:00.000Z",
          "kibana.alert.ancestors": [
            {
              "id": "l1qacYsBjzKYdBVA3leI",
              "type": "event",
              "index": "winlog-5",
              "depth": 0
            }
          ],
          "kibana.alert.status": "active",
          "kibana.alert.workflow_status": "open",
          "kibana.alert.depth": 1,
          "kibana.alert.reason": "event created medium alert ThreatQ IOC
Match.",
          "kibana.alert.severity": "medium",
          "kibana.alert.risk_score": 57,
          "kibana.alert.rule.actions": [],
          "kibana.alert.rule.author": [],
          "kibana.alert.rule.created_at": "2023-10-27T14:25:10.525Z",
          "kibana.alert.rule.created_by": "admin",
          "kibana.alert.rule.description": "Test",
          "kibana.alert.rule.enabled": true,
          "kibana.alert.rule.exceptions_list": [],
```

```
          "kibana.alert.rule.false_positives": [],
          "kibana.alert.rule.from": "now-420s",
          "kibana.alert.rule.immutable": false,
          "kibana.alert.rule.interval": "2m",
          "kibana.alert.rule.indices": ["winlog-*"],
          "kibana.alert.rule.license": "",
          "kibana.alert.rule.max_signals": 100,
          "kibana.alert.rule.references": [],
          "kibana.alert.rule.risk_score_mapping": [],
          "kibana.alert.rule.rule_id": "91266588-3f85-4d56-a7f1-70bd57927a61",
          "kibana.alert.rule.severity_mapping": [],
          "kibana.alert.rule.threat": [],
          "kibana.alert.rule.to": "now",
          "kibana.alert.rule.type": "threat_match",
          "kibana.alert.rule.updated_at": "2023-10-27T14:39:24.973Z",
          "kibana.alert.rule.updated_by": "admin",
          "kibana.alert.rule.version": 1,
          "kibana.alert.uuid":
"f56c18f3fa4f56ea8284357078fac19b30e1b465872cd5bbf110d5495e64bae9",
          "kibana.alert.rule.meta.from": "5m",
          "kibana.alert.rule.meta.kibana_siem_app_url": "http://
192.168.50.126:5601/app/security",
          "kibana.alert.rule.risk_score": 57,
          "kibana.alert.rule.severity": "medium"
        },
        "sort": [1698418176421]
      }
    ]
  }
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.[kibana.alert.reason], .[kibana.alert.severity], .[kibana.alert.risk_score]`	Event Title	Alert	`{{ Data Path to Published Date }}`	`.[kibana.alert.start]`	Fields are concatenated together to form the title
`.[kibana.alert.rule.tags]`	Tag	N/A	N/A	N/A	N/A
`.[kibana.alert.uuid]`	Event Attribute	Elastic Alert ID	N/A	N/A	N/A
`.[kibana.alert.uuid]`	Event Attribute	Elastic Alert Link	N/A	N/A	Concatenated with the Kibana URL
`.[kibana.alert.severity]`	Event Attribute	Severity	N/A	`Medium`	Title-cased, Updated at ingestion

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.[kibana.alert.risk_score]`	Event Attribute	Risk Score	N/A	`97`	Updated at ingestion
`.[kibana.alert.rule.parameters].threat[].name`	Event Attribute	Tactic	N/A	`Medium`	If the `.framework` is `MITRE ATT&CK`
`.host.name`	Asset Value	N/A		N/A	N/A
`.host.id`	Asset Attribute	Elastic Host ID		N/A	N/A
`.host.id`	Asset Attribute	Elastic Host Link		N/A	Concatenated with the Kibana URL
`.host.mac`	Asset Attribute	MAC Address		N/A	N/A
`.host.hostname`	Asset Attribute	Hostname		N/A	N/A
`.host.ip`	Asset Attribute	IP Address		N/A	N/A
`.host.architecture`	Asset Attribute	Architecture		N/A	N/A
`.host.os.name`	Asset Attribute	Operating System		N/A	N/A
`.[kibana.alert.rule.parameters].threat[].technique.id`, `.[kibana.alert.rule.parameters].threat[].technique.name`	Attack Pattern	N/A	N/A	N/A	If the `.framework` is `MITRE ATT&CK`
`.threat.enrichments[].matched.atomic`	Indicator	`.threat.enrichments[].indicator.type`	N/A	N/A	Type is mapped from the ECS type to ThreatQ type
`.threat.enrichments[].indicator.confidence`	Indicator Attribute	Confidence	N/A	`Low`	Updated at ingestion
`.threat.enrichments[].indicator.port`	Indicator Attribute	Port	N/A	`80`	N/A
`.threat.enrichments[].indicator.provider`	Indicator Attribute	Provider	N/A	`ThreatQuotient`	N/A
`.threat.enrichments[].indicator.reference`	Indicator Attribute	External Reference	N/A	N/A	N/A
`.threat.enrichments[].indicator.marking.tlp`	Indicator TLP	N/A	N/A	`GREEN`	N/A
`.threat.enrichments[].indicator.description`	Indicator Description	N/A	N/A	N/A	N/A

Elastic Security Alerts Supplemental

The Elastic Security Alerts supplemental feed fetches alerts related to a given case.

`GET https://{kibana_host}:{kibana_port}/api/cases/{case_id}/alerts`

Sample Response:

```
[
  {
    "id": "77af630161ee049878781dde394e111a0acefeb69372bce2669104f6930a1f6c",
    "index": ".internal.alerts-security.alerts-default-000001",
    "attached_at": "2023-06-20T17:08:06.876Z"
  },
  {
    "id": "3ee4fa13be338ebc1eca707c46c255f5e469b39989ce9635080e80b96cc3fa21",
    "index": ".internal.alerts-security.alerts-default-000001",
    "attached_at": "2023-06-20T17:08:24.967Z"
  }
]
```

Mapping for this supplemental feed is handled by calling the Elastic Security Alerts primary feed.

Elastic Security Alerts by IDs Supplemental

The Elastic Security Alerts by IDs supplemental feed fetches the alert details for alerts related to a given case.

`GET https://{elasticsearch_host}:{elasticsearch_port}/.alerts-security.alerts-default/_search?q=_id:({alert_id})`

Sample Response:


```
{
  "took": 5,
  "timed_out": false,
  "_shards": {
    "total": 5,
    "successful": 5,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": {
      "value": 2,
      "relation": "eq"
    },
    "max_score": 1,
    "hits": [
      {
        "_index": ".internal.alerts-security.alerts-default-000001",
        "_id":
"77af630161ee049878781dde394e111a0acefeb69372bce2669104f6930a1f6c",
        "_score": 1,
        "_source": {
          "kibana.alert.severity": "critical",
          "agent": {
            "name": "DESKTOP-O0SATNR",
            "id": "74a8f1c0-f82b-46f2-9153-31805738d2f3",
            "type": "winlogbeat",
            "ephemeral_id": "13ddbc5f-1886-4d83-ae24-429be7b832ac",
            "version": "8.8.1"
          },
          "kibana.alert.rule.references": [
            "https://www.iana.org/assignments/iana-ipv4-special-registry/iana-
ipv4-special-registry.xhtml"
          ],
          "kibana.alert.rule.updated_by": "admin",
          "kibana.alert.case_ids": ["05efc8b0-0f8d-11ee-ac48-ad9ca4c1d49d"],
          "kibana.alert.rule.threat": [
            {
              "framework": "MITRE ATT&CK",
              "technique": [],
              "tactic": {
```

```
              "reference": "https://attack.mitre.org/tactics/TA0011/",
              "name": "Command and Control",
              "id": "TA0011"
            }
          },
          {
            "framework": "MITRE ATT&CK",
            "technique": [
              {
                "reference": "https://attack.mitre.org/techniques/T1021/",
                "name": "Remote Services",
                "subtechnique": [],
                "id": "T1021"
              }
            ],
            "tactic": {
              "reference": "https://attack.mitre.org/tactics/TA0008/",
              "name": "Lateral Movement",
              "id": "TA0008"
            }
          },
          {
            "framework": "MITRE ATT&CK",
            "technique": [
              {
                "reference": "https://attack.mitre.org/techniques/T1190/",
                "name": "Exploit Public-Facing Application",
                "subtechnique": [],
                "id": "T1190"
              }
            ],
            "tactic": {
              "reference": "https://attack.mitre.org/tactics/TA0001/",
              "name": "Initial Access",
              "id": "TA0001"
            }
          }
        ],
        "kibana.alert.original_event.original": "Process Create:\nRuleName:
technique_id=T1059,technique_name=Command-Line Interface\nUtcTime: 2023-06-20
17:03:09.368\nProcessGuid: {ef68b829-dbcd-6491-df33-000000000200}\nProcessId:
12328\nImage: C:\\Windows\\System32\\cmd.exe\nFileVersion: 10.0.19041.746
(WinBuild.160101.0800)\nDescription: Windows Command Processor\nProduct:
MicrosoftÂ® WindowsÂ® Operating System\nCompany: Microsoft
Corporation\nOriginalFileName: Cmd.Exe\nCommandLine: C:\\Windows\\system32\
\cmd.exe /c \"\"\\\\tsclient\\tmp\\naughty_malware.bat\"\"\nCurrentDirectory:
C:\\Users\\user\\Desktop\\\nUser: DESKTOP-O0SATNR\\user\nLogonGuid:
{ef68b829-647c-6490-c871-780700000000}\nLogonId: 0x77871C8\nTerminalSessionId:
7\nIntegrityLevel: Medium\nHashes:
SHA1=F1EFB0FDDC156E4C61C5F78A54700E4E7984D55D,MD5=8A2122E8162DBEF04694B9C3E0B6C
```

```
DEE,SHA256=B99D61D874728EDC0918CA0EB10EAB93D381E7367E377406E65963366C874450,IMP
HASH=272245E2988E1E430500B852C4FB5E18\nParentProcessGuid: {ef68b829-
bdea-6490-9c2e-000000000200}\nParentProcessId: 4252\nParentImage: C:\\Windows\
\System32\\WindowsPowerShell\\v1.0\\powershell.exe\nParentCommandLine: \"C:\
\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\" \nParentUser:
DESKTOP-O0SATNR\\user",
          "kibana.alert.original_event.code": "1",
          "kibana.alert.rule.description": "This rule detects network events
that may indicate the use of RDP traffic from the Internet. RDP is commonly
used by system administrators to remotely control a system for maintenance or
to use shared resources. It should almost never be directly exposed to the
Internet, as it is frequently targeted and exploited by threat actors as an
initial access or backdoor vector.",
          "kibana.alert.rule.tags": [
            "Elastic",
            "Host",
            "Network",
            "Threat Detection",
            "Command and Control",
            "Host"
          ],
          "kibana.alert.rule.producer": "siem",
          "kibana.alert.rule.to": "now",
          "kibana.alert.rule.created_by": "admin",
          "kibana.alert.rule.timestamp_override": "event.ingested",
          "ecs": {
            "version": "8.0.0"
          },
          "kibana.alert.risk_score": 99,
          "host": {
            "hostname": "DESKTOP-O0SATNR",
            "os": {
              "build": "19045.2965",
              "kernel": "10.0.19041.2965 (WinBuild.160101.0800)",
              "name": "Windows 10 Pro",
              "type": "windows",
              "family": "windows",
              "version": "10.0",
              "platform": "windows"
            },
            "ip": ["10.206.249.163"],
            "name": "DESKTOP-O0SATNR",
            "id": "ef68b829-ef72-44c6-ad80-c6e4a44afa2d",
            "mac": ["1E-6D-03-FE-ED-C3"],
            "architecture": "x86_64"
          },
          "kibana.alert.rule.name": "Powershell Code Execution",
          "event.kind": "signal",
          "event.original": "Process Create:\nRuleName:
technique_id=T1059,technique_name=Command-Line Interface\nUtcTime: 2023-06-20
17:03:09.368\nProcessGuid: {ef68b829-dbcd-6491-df33-000000000200}\nProcessId:
```

```
12328\nImage: C:\\Windows\\System32\\cmd.exe\nFileVersion: 10.0.19041.746
(WinBuild.160101.0800)\nDescription: Windows Command Processor\nProduct:
MicrosoftÂ® WindowsÂ® Operating System\nCompany: Microsoft
Corporation\nOriginalFileName: Cmd.Exe\nCommandLine: C:\\Windows\\system32\
\cmd.exe /c \"\"\\\\tsclient\\tmp\\naughty_malware.bat\"\"\nCurrentDirectory:
C:\\Users\\user\\Desktop\\\nUser: DESKTOP-O0SATNR\\user\nLogonGuid:
{ef68b829-647c-6490-c871-780700000000}\nLogonId: 0x77871C8\nTerminalSessionId:
7\nIntegrityLevel: Medium\nHashes:
SHA1=F1EFB0FDDC156E4C61C5F78A54700E4E7984D55D,MD5=8A2122E8162DBEF04694B9C3E0B6C
DEE,SHA256=B99D61D874728EDC0918CA0EB10EAB93D381E7367E377406E65963366C874450,IMP
HASH=272245E2988E1E430500B852C4FB5E18\nParentProcessGuid: {ef68b829-
bdea-6490-9c2e-000000000200}\nParentProcessId: 4252\nParentImage: C:\\Windows\
\System32\\WindowsPowerShell\\v1.0\\powershell.exe\nParentCommandLine: \"C:\
\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\" \nParentUser:
DESKTOP-O0SATNR\\user",
          "kibana.alert.workflow_status": "open",
          "kibana.alert.rule.uuid": "b0439140-0f81-11ee-ac48-ad9ca4c1d49d",
          "kibana.alert.original_event.created": "2023-06-20T17:03:10.536Z",
          "kibana.alert.rule.risk_score_mapping": [],
          "kibana.alert.rule.interval": "5m",
          "kibana.alert.reason": "event on DESKTOP-O0SATNR created critical
alert Powershell Code Execution.",
          "kibana.alert.rule.type": "query",
          "tags": ["beats_input_codec_plain_applied"],
          "kibana.alert.start": "2023-06-20T17:04:15.485Z",
          "event.provider": "Microsoft-Windows-Sysmon",
          "kibana.alert.rule.immutable": false,
          "event.code": "1",
          "kibana.alert.rule.timeline_title": "Comprehensive Network Timeline",
          "event.created": "2023-06-20T17:03:10.536Z",
          "kibana.alert.depth": 1,
          "kibana.alert.rule.enabled": true,
          "kibana.alert.rule.version": 100,
          "kibana.alert.rule.from": "now-540s",
          "kibana.alert.rule.parameters": {
            "severity_mapping": [],
            "references": [
              "https://www.iana.org/assignments/iana-ipv4-special-registry/
iana-ipv4-special-registry.xhtml"
            ],
            "description": "This rule detects network events that may indicate
the use of RDP traffic from the Internet. RDP is commonly used by system
administrators to remotely control a system for maintenance or to use shared
resources. It should almost never be directly exposed to the Internet, as it is
frequently targeted and exploited by threat actors as an initial access or
backdoor vector.",
            "language": "kuery",
            "type": "query",
            "timestamp_override_fallback_disabled": false,
            "exceptions_list": [],
            "timestamp_override": "event.ingested",
```

```
            "from": "now-540s",
            "timeline_id": "300afc76-072d-4261-864d-4149714bf3f1",
            "severity": "critical",
            "max_signals": 100,
            "risk_score": 99,
            "risk_score_mapping": [],
            "author": ["Elastic"],
            "query": "technique_name=PowerShell AND naughty* AND powershell*",
            "index": ["winlogbeat-*"],
            "filters": [],
            "version": 100,
            "rule_id": "0d2f3215-97de-4dca-b367-f635c3466ff8",
            "license": "Elastic License v2",
            "required_fields": [],
            "immutable": false,
            "related_integrations": [],
            "timeline_title": "Comprehensive Network Timeline",
            "meta": {
              "from": "4m"
            },
            "setup": "",
            "false_positives": [
              "Some network security policies allow RDP directly from the
Internet but usage that is unfamiliar to server or network owners can be
unexpected and suspicious. RDP services may be exposed directly to the Internet
in some networks such as cloud environments. In such cases, only RDP gateways,
bastions or jump servers may be expected expose RDP directly to the Internet
and can be exempted from this rule. RDP may be required by some work-flows such
as remote access and support for specialized software products and servers.
Such work-flows are usually known and not unexpected."
            ],
            "threat": [
              {
                "framework": "MITRE ATT&CK",
                "technique": [],
                "tactic": {
                  "reference": "https://attack.mitre.org/tactics/TA0011/",
                  "name": "Command and Control",
                  "id": "TA0011"
                }
              },
              {
                "framework": "MITRE ATT&CK",
                "technique": [
                  {
                    "reference": "https://attack.mitre.org/techniques/T1021/",
                    "name": "Remote Services",
                    "subtechnique": [],
                    "id": "T1021"
                  }
```

```
              ],
              "tactic": {
                "reference": "https://attack.mitre.org/tactics/TA0008/",
                "name": "Lateral Movement",
                "id": "TA0008"
              }
            },
            {
              "framework": "MITRE ATT&CK",
              "technique": [
                {
                  "reference": "https://attack.mitre.org/techniques/T1190/",
                  "name": "Exploit Public-Facing Application",
                  "subtechnique": [],
                  "id": "T1190"
                }
              ],
              "tactic": {
                "reference": "https://attack.mitre.org/tactics/TA0001/",
                "name": "Initial Access",
                "id": "TA0001"
              }
            }
          ],
          "to": "now"
        },
        "kibana.alert.rule.revision": 2,
        "log": {
          "level": "information"
        },
        "kibana.alert.status": "active",
        "kibana.alert.last_detected": "2023-06-20T17:04:15.485Z",
        "kibana.alert.ancestors": [
          {
            "depth": 0,
            "index": "winlogbeat-8.8.1",
            "id": "hH7C2YgBjzKYdBVAzrH9",
            "type": "event"
          }
        ],
        "kibana.alert.rule.exceptions_list": [],
        "kibana.alert.rule.actions": [],
        "kibana.alert.rule.rule_type_id": "siem.queryRule",
        "kibana.alert.original_event.provider": "Microsoft-Windows-Sysmon",
        "kibana.alert.rule.timeline_id":
"300afc76-072d-4261-864d-4149714bf3f1",
        "@version": "1",
        "kibana.alert.rule.license": "Elastic License v2",
        "kibana.alert.original_event.kind": "event",
        "kibana.alert.rule.severity_mapping": [],
```

```
          "winlog": {
            "computer_name": "DESKTOP-O0SATNR",
            "process": {
              "pid": 7876,
              "thread": {
                "id": 6992
              }
            },
            "channel": "Microsoft-Windows-Sysmon/Operational",
            "event_data": {
              "Company": "Microsoft Corporation",
              "ParentImage": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\
\powershell.exe",
              "LogonGuid": "{ef68b829-647c-6490-c871-780700000000}",
              "User": "DESKTOP-O0SATNR\\user",
              "Description": "Windows Command Processor",
              "OriginalFileName": "Cmd.Exe",
              "TerminalSessionId": "7",
              "IntegrityLevel": "Medium",
              "ParentProcessId": "4252",
              "Product": "MicrosoftÂ® WindowsÂ® Operating System",
              "ParentUser": "DESKTOP-O0SATNR\\user",
              "Image": "C:\\Windows\\System32\\cmd.exe",
              "ProcessGuid": "{ef68b829-dbcd-6491-df33-000000000200}",
              "UtcTime": "2023-06-20 17:03:09.368",
              "CurrentDirectory": "C:\\Users\\user\\Desktop\\",
              "CommandLine": "C:\\Windows\\system32\\cmd.exe /c \"\"\\\\
\tsclient\\tmp\\naughty_malware.bat\"\"",
              "Hashes":
"SHA1=F1EFB0FDDC156E4C61C5F78A54700E4E7984D55D,MD5=8A2122E8162DBEF04694B9C3E0B6
CDEE,SHA256=B99D61D874728EDC0918CA0EB10EAB93D381E7367E377406E65963366C874450,IM
PHASH=272245E2988E1E430500B852C4FB5E18",
              "FileVersion": "10.0.19041.746 (WinBuild.160101.0800)",
              "ProcessId": "12328",
              "ParentProcessGuid": "{ef68b829-bdea-6490-9c2e-000000000200}",
              "ParentCommandLine": "\"C:\\Windows\\System32\\WindowsPowerShell\
\v1.0\\powershell.exe\" ",
              "LogonId": "0x77871c8",
              "RuleName": "technique_id=T1059,technique_name=Command-Line
Interface"
            },
            "opcode": "Info",
            "version": 5,
            "record_id": 57378,
            "event_id": "1",
            "task": "Process Create (rule: ProcessCreate)",
            "provider_guid": "{5770385f-c22a-43e0-bf4c-06f5698ffbd9}",
            "api": "wineventlog",
            "provider_name": "Microsoft-Windows-Sysmon",
            "user": {
```

```
            "identifier": "S-1-5-18",
            "domain": "NT AUTHORITY",
            "name": "SYSTEM",
            "type": "User"
          }
        },
        "kibana.alert.rule.max_signals": 100,
        "kibana.alert.rule.updated_at": "2023-06-20T17:04:10.727Z",
        "kibana.alert.rule.risk_score": 99,
        "kibana.alert.rule.author": ["Elastic"],
        "kibana.alert.rule.false_positives": [
          "Some network security policies allow RDP directly from the
Internet but usage that is unfamiliar to server or network owners can be
unexpected and suspicious. RDP services may be exposed directly to the Internet
in some networks such as cloud environments. In such cases, only RDP gateways,
bastions or jump servers may be expected expose RDP directly to the Internet
and can be exempted from this rule. RDP may be required by some work-flows such
as remote access and support for specialized software products and servers.
Such work-flows are usually known and not unexpected."
        ],
        "message": "Process Create:\nRuleName:
technique_id=T1059,technique_name=Command-Line Interface\nUtcTime: 2023-06-20
17:03:09.368\nProcessGuid: {ef68b829-dbcd-6491-df33-000000000200}\nProcessId:
12328\nImage: C:\\Windows\\System32\\cmd.exe\nFileVersion: 10.0.19041.746
(WinBuild.160101.0800)\nDescription: Windows Command Processor\nProduct:
MicrosoftÂ® WindowsÂ® Operating System\nCompany: Microsoft
Corporation\nOriginalFileName: Cmd.Exe\nCommandLine: C:\\Windows\\system32\
\cmd.exe /c \"\"\\\\tsclient\\tmp\\naughty_malware.bat\"\"\nCurrentDirectory:
C:\\Users\\user\\Desktop\\\nUser: DESKTOP-O0SATNR\\user\nLogonGuid:
{ef68b829-647c-6490-c871-780700000000}\nLogonId: 0x77871C8\nTerminalSessionId:
7\nIntegrityLevel: Medium\nHashes:
SHA1=F1EFB0FDDC156E4C61C5F78A54700E4E7984D55D,MD5=8A2122E8162DBEF04694B9C3E0B6C
DEE,SHA256=B99D61D874728EDC0918CA0EB10EAB93D381E7367E377406E65963366C874450,IMP
HASH=272245E2988E1E430500B852C4FB5E18\nParentProcessGuid: {ef68b829-
bdea-6490-9c2e-000000000200}\nParentProcessId: 4252\nParentImage: C:\\Windows\
\System32\\WindowsPowerShell\\v1.0\\powershell.exe\nParentCommandLine: \"C:\
\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\" \nParentUser:
DESKTOP-O0SATNR\\user",
        "kibana.alert.rule.consumer": "siem",
        "kibana.alert.rule.indices": ["winlogbeat-*"],
        "kibana.alert.rule.category": "Custom Query Rule",
        "event.action": "Process Create (rule: ProcessCreate)",
        "@timestamp": "2023-06-20T17:04:15.475Z",
        "kibana.alert.rule.created_at": "2023-06-20T15:46:57.754Z",
        "kibana.alert.original_event.action": "Process Create (rule:
ProcessCreate)",
        "kibana.alert.rule.severity": "critical",
        "kibana.alert.rule.execution.uuid": "cffe64f8-ee5a-4a30-
a9ee-97648c304490",
        "kibana.space_ids": ["default"],
```

```
          "kibana.alert.uuid":
"77af630161ee049878781dde394e111a0acefeb69372bce2669104f6930a1f6c",
          "kibana.version": "8.8.1",
          "kibana.alert.rule.meta.from": "4m",
          "kibana.alert.original_time": "2023-06-20T17:03:09.380Z",
          "kibana.alert.rule.rule_id": "0d2f3215-97de-4dca-b367-f635c3466ff8"
        }
      }
    ]
  }
}
```

Mapping for this supplemental feed is handled by calling the Elastic Security Alerts primary feed.

Elastic Security Cases

The Elastic Security Cases feed periodically pulls cases from Elastic Security's default alert index into ThreatQ.

`GET https://{kibana_host}:{kibana_port}/api/cases/_find`

Sample Response:


```
{
  "page": 1,
  "per_page": 1,
  "total": 3,
  "cases": [
    {
      "id": "1b5eed40-1053-11ee-ac48-ad9ca4c1d49d",
      "version": "WzcyNjA2Miw2XQ==",
      "comments": [],
      "totalComment": 0,
      "totalAlerts": 2,
      "title": "Investigating possible Lockbit Campaign",
      "tags": [],
      "description": "...",
      "settings": {
        "syncAlerts": true
      },
      "owner": "securitySolution",
      "duration": null,
      "closed_at": null,
      "closed_by": null,
      "created_at": "2023-06-21T16:46:02.263Z",
      "created_by": {
        "username": "admin",
        "full_name": "",
        "email": "",
        "profile_uid": "u_jGl25bVBBBW96Qi9Te4V37Fnqchz_Eu4qB9vKrRIqRg_0"
      },
      "updated_at": "2023-06-21T16:46:41.936Z",
      "updated_by": {
        "full_name": "",
        "profile_uid": "u_jGl25bVBBBW96Qi9Te4V37Fnqchz_Eu4qB9vKrRIqRg_0",
        "email": "",
        "username": "admin"
      },
      "assignees": [],
      "connector": {
        "id": "none",
        "name": "none",
        "type": ".none",
        "fields": null
```

```
      },
      "external_service": null,
      "severity": "low",
      "status": "open"
    }
  ],
  "count_open_cases": 3,
  "count_in_progress_cases": 0,
  "count_closed_cases": 0
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.title`	Incident Title	N/A	`.created_at`	N/A	N/A
`.created_by.full_name`, `.created_by.username`, `.created_by.email`	Incident Attribute	Created By	`.created_at`	N/A	N/A
`.closed_by.full_name`, `.closed_by.username`, `.closed_by.email`	Incident Attribute	Closed By	`.created_at`	N/A	N/A
`.closed_at`	Incident Attribute	Closed At	`.created_at`	N/A	N/A
`.owner`	Incident Attribute	Owner	`.created_at`	N/A	N/A
`.updated_by.full_name`, `.updated_by.username`, `.updated_by.email`	Incident Attribute	Updated By	`.created_at`	N/A	Updated at ingestion
`.updated_at`	Incident Attribute	Updated At	`.created_at`	N/A	Updated at ingestion

This feed also may bring in Alerts. The mapping for those can be found in the Elastic Security Alerts Mapping section.

Elastic Security Cases Supplemental

The Elastic Security Cases supplemental feed fetches alerts related to a given case.

`GET https://{kibana_host}:{kibana_port}/api/cases/{case_id}/alerts`

Sample Response:

```
[
  {
    "id": "77af630161ee049878781dde394e111a0acefeb69372bce2669104f6930a1f6c",
    "index": ".internal.alerts-security.alerts-default-000001",
    "attached_at": "2023-06-20T17:08:06.876Z"
  },
  {
    "id": "3ee4fa13be338ebc1eca707c46c255f5e469b39989ce9635080e80b96cc3fa21",
    "index": ".internal.alerts-security.alerts-default-000001",
    "attached_at": "2023-06-20T17:08:24.967Z"
  }
]
```

Mapping for this supplemental feed is handled by calling the primary Elastic Security Cases feed.

Average Feed Run

> Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

Elastic Security Alerts

METRIC	RESULT
Run Time	1 minute
Indicators	1
Events	32
Event Attributes	128
Assets	1

Elastic Security Cases

METRIC	RESULT
Run Time	1 minute
Incidents	2
Incident Attributes	8
Events	3
Event Attributes	15
Attack Patterns	2
Assets	1

Change Log

- **Version 1.0.1**
  - Updated the configuration screen logic for both feeds.
    - Both feeds - the **Host Context** fields will now only be displayed if you have selected the **Ingest Affected Hosts** parameter.
    - Security Cases Feed - the **Alert Context** and **Alert Description Context** sections will now only be displayed if you have selected **Ingest Related Alerts** under **Ingest Options**.
- **Version 1.0.0**
  - Initial release