ThreatQuotient

Infoblox Insights CDF User Guide

Version 1.0.0

February 20, 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	1.0.0
Compatible with ThreatQ Versions	>= 5.22.0
Support Tier	ThreatQ Supported

Introduction

The Infoblox Insights CDF ingest Incidents from Infoblox and its related data.

The integration provides the following feeds:

- **Infoblox SOC Insights** - retrieves the IDs of Infoblox incidents.
- **Infoblox Get Details (Supplemental)** - ingests all related data for an Infoblox incident.

The integration ingests the following system objects:

- Assets
- Incidents
- Indicators

Prerequisites

The following is required by the integration:

- An Infoblox Token.

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 integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
    - Drag and drop the file into the dialog box
    - Select **Click to Browse** to locate the integration 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.

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

Configuration

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

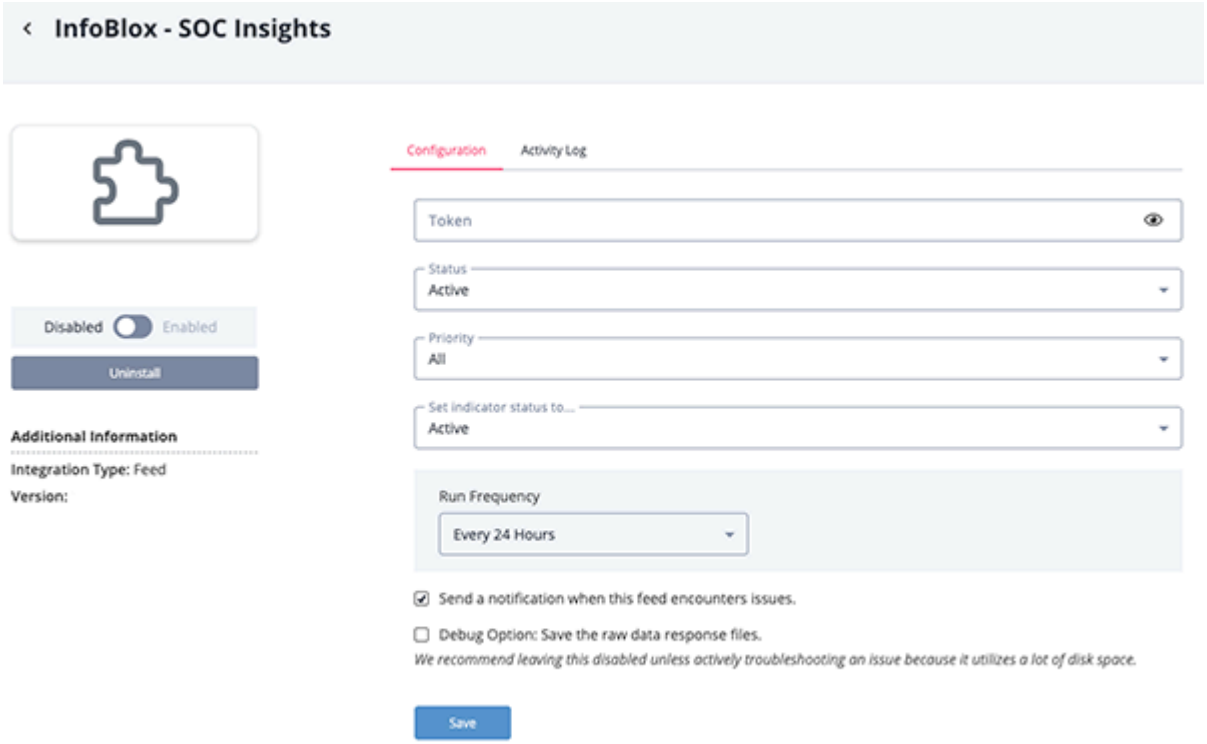
To configure the integration:

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:

PARAMETER	DESCRIPTION
Token	Enter your InfoBlox Token.
Status	Select the Status to receive. Options include **Open** and **Closed**. This field is set to Open by default.
Priority	Select the Priority to receive. Options include: ◦ High ◦ Medium ◦ Low ◦ All (default)



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

Infoblox SOC Insights

The Infoblox SOC Insights retrieves the ID of an incident based on the user's configuration settings.

`GET https://csp.infoblox.com/api/v1/insights`

Sample Response:


```
{
    "insightList": [
        {
            "storageId": "2300798",
            "tClass": "TI-CONFIGURATIONISSUE",
            "tFamily": "NXDOMAIN",
            "insightId": "1a712155-e808-44c1-86da-e2489bd08c4e",
            "feedSource": "Insight Detection Framework",
            "startedAt": "2023-11-21T05:00:00Z",
            "threatType": "NXDomain",
            "status": "Active",
            "confidenceLevel": 3,
            "numEvents": "6166",
            "mostRecentAt": "2023-11-21T05:03:00Z",
            "threatLevel": 1,
            "notBlockedCount": "6166",
            "dateChanged": "0001-01-01T00:00:00Z",
            "priority": 3,
            "priorityText": "LOW"
        }
    ]
}
```

Get Details (Supplemental)

The Get Details supplemental feed retrieves all the details for each Incident.

`GET https://csp.infoblox.com/api/v1/insights/{{insightId}}/exports`

Sample Response:


```
{
  "insight-1a712155-e808-44c1-86da-e2489bd08c4e/machine-readable/asset-
data.json": {
    "result": {
      "data": [
        {
          "AggIPSummary.cid": ":f0acaeff3036fc21e02b846d1fb47255",
          "AggIPSummary.cmac": null,
          "AggIPSummary.confidenceLevelMax": 3,
          "AggIPSummary.count": 6166,
          "AggIPSummary.location": "Ashburn,United States",
          "AggIPSummary.os_version": null,
          "AggIPSummary.qip": "54.158.53.120",
          "AggIPSummary.qipDistinctCount": 1,
          "AggIPSummary.threatIndicatorDistinctCount": 1,
          "AggIPSummary.threatLevelMax": 1,
          "AggIPSummary.timestampMax": "2023-11-21T05:00:00.000",
          "AggIPSummary.timestampMin": "2023-11-21T05:00:00.000",
          "AggIPSummary.user": null
        }
      ],
      "query": {
        "dimensions": [
          "AggIPSummary.qip"
        ],
        "filters": [
          {
            "member": "AggIPSummary.tclass",
            "operator": "equals",
            "values": [
              "TI-CONFIGURATIONISSUE"
            ]
          },
          {
            "member": "AggIPSummary.tfamily",
            "operator": "equals",
            "values": [
              "NXDOMAIN"
            ]
          }
        ],
        "limit": 10000,
```

```
        "measures": [
          "AggIPSummary.count"
        ],
        "offset": 0,
        "order": {
          "AggIPSummary.timestampMax": "desc"
        },
        "timeDimensions": [
          {
            "dateRange": [
              "2023-11-21T05:00:00.000",
              "2023-11-21T05:03:00.000"
            ],
            "dimension": "AggIPSummary.timestamp",
            "granularity": ""
          }
        ]
      }
    }
  },
  "insight-1a712155-e808-44c1-86da-e2489bd08c4e/machine-readable/event-
data.json": {
    "result": {
      "data": [
        {
          "DnsLogs.confidence": "High",
          "DnsLogs.device_country": "",
          "DnsLogs.device_name": "",
          "DnsLogs.device_region": "",
          "DnsLogs.dhcp_fingerprint": "",
          "DnsLogs.dns_view": "",
          "DnsLogs.feed_name": "",
          "DnsLogs.mac_address": "",
          "DnsLogs.network": "IR_Network",
          "DnsLogs.os_version": "",
          "DnsLogs.policy_action": "Allow - No Log",
          "DnsLogs.policy_name": "Default Global Policy",
          "DnsLogs.qip": "54.158.53.120",
          "DnsLogs.qname": "atu5741.io.happymail.com",
          "DnsLogs.query_type": "A",
          "DnsLogs.response": "",
          "DnsLogs.response_country": "",
          "DnsLogs.response_region": "",
          "DnsLogs.severity": "Low",
          "DnsLogs.tclass": "TI-CONFIGURATIONISSUE",
          "DnsLogs.tfamily": "NXDOMAIN",
          "DnsLogs.threat_indicator": "",
          "DnsLogs.timestamp": "2023-11-21 05:02:00 +0000 UTC",
          "DnsLogs.tproperty": "io.happymail.com",
          "DnsLogs.user": "unknown"
```

```
      }
    ],
    "query": {
      "dimensions": [
        "DnsLogs.timestamp"
      ],
      "filters": [
        {
          "member": "DnsLogs.type",
          "operator": "contains",
          "values": [
            "2",
            "3",
            "4"
          ]
        },
        {
          "member": "DnsLogs.tclass",
          "operator": "equals",
          "values": [
            "TI-CONFIGURATIONISSUE"
          ]
        },
        {
          "member": "DnsLogs.tfamily",
          "operator": "equals",
          "values": [
            "NXDOMAIN"
          ]
        }
      ],
      "limit": 10000,
      "measures": null,
      "offset": 0,
      "order": {
        "DnsLogs.timestamp": "desc"
      },
      "timeDimensions": [
        {
          "dateRange": [
            "2023-11-21T05:00:00.000",
            "2023-11-21T05:03:00.000"
          ],
          "dimension": "DnsLogs.timestamp",
          "granularity": "day"
        }
      ],
      "ungrouped": true
    }
  }
```

```
  },
  "insight-1a712155-e808-44c1-86da-e2489bd08c4e/machine-readable/
indicators.json": {
    "result": {
      "data": [
        {
          "AggIPSummary.action": "Not Blocked",
          "AggIPSummary.cmac": null,
          "AggIPSummary.confidenceLevelMax": 3,
          "AggIPSummary.count": 6166,
          "AggIPSummary.location": "Ashburn,United States",
          "AggIPSummary.os_version": null,
          "AggIPSummary.qipDistinctCount": 1,
          "AggIPSummary.threatLevelMax": 1,
          "AggIPSummary.threat_indicator": "happymail.com",
          "AggIPSummary.timestampMax": "2023-11-21T05:00:00.000",
          "AggIPSummary.timestampMin": "2023-11-21T05:00:00.000",
          "AggIPSummary.user": null
        }
      ],
      "query": {
        "dimensions": [
          "AggIPSummary.threat_indicator"
        ],
        "filters": [
          {
            "member": "AggIPSummary.tclass",
            "operator": "equals",
            "values": [
              "TI-CONFIGURATIONISSUE"
            ]
          },
          {
            "member": "AggIPSummary.tfamily",
            "operator": "equals",
            "values": [
              "NXDOMAIN"
            ]
          }
        ],
        "limit": 10000,
        "measures": [
          "AggIPSummary.count"
        ],
        "offset": 0,
        "order": {
          "AggIPSummary.timestampMax": "desc"
        },
        "timeDimensions": [
          {
```

```
            "dateRange": [
              "2023-11-21T05:00:00.000",
              "2023-11-21T05:03:00.000"
            ],
            "dimension": "AggIPSummary.timestamp",
            "granularity": ""
          }
        ]
      }
    }
  },
  "insight-1a712155-e808-44c1-86da-e2489bd08c4e/machine-readable/insight-
summary/asset-count.json": {
    "result": {
      "data": [
        {
          "AggIPSummary.qip": "54.158.53.120",
          "AggIPSummary.qipDistinctCount": 1,
          "AggIPSummary.threatIndicatorDistinctCount": 1
        }
      ],
      "query": {
        "dimensions": [
          "AggIPSummary.qip"
        ],
        "filters": [
          {
            "member": "AggIPSummary.tclass",
            "operator": "equals",
            "values": [
              "TI-CONFIGURATIONISSUE"
            ]
          },
          {
            "member": "AggIPSummary.tfamily",
            "operator": "equals",
            "values": [
              "NXDOMAIN"
            ]
          }
        ],
        "limit": 10000,
        "measures": [
          "AggIPSummary.threatIndicatorDistinctCount",
          "AggIPSummary.qipDistinctCount"
        ],
        "offset": 0,
        "order": {
          "AggIPSummary.timestamp": "desc"
        },
```

```
        "timeDimensions": [
          {
            "dateRange": [
              "2023-11-21T05:00:00.000",
              "2023-11-21T05:03:00.000"
            ],
            "dimension": "AggIPSummary.timestamp",
            "granularity": ""
          }
        ]
      }
    }
  },
  "insight-1a712155-e808-44c1-86da-e2489bd08c4e/machine-readable/insight-
summary/event-count.json": {
    "result": {
      "annotation": {
        "dimensions": {
          "InsightDetails.confidenceLevel": {
            "shortTitle": "Confidence Level",
            "title": "Insight Details Confidence Level",
            "type": "number"
          },
          "InsightDetails.description": {
            "shortTitle": "Description",
            "title": "Insight Details Description",
            "type": "string"
          },
          "InsightDetails.feedSource": {
            "shortTitle": "Feed Source",
            "title": "Insight Details Feed Source",
            "type": "string"
          },
          "InsightDetails.insightId": {
            "shortTitle": "Insight Id",
            "title": "Insight Details Insight Id",
            "type": "string"
          },
          "InsightDetails.insightStatus": {
            "shortTitle": "Insight Status",
            "title": "Insight Details Insight Status",
            "type": "string"
          },
          "InsightDetails.persistent": {
            "shortTitle": "Persistent",
            "title": "Insight Details Persistent",
            "type": "boolean"
          },
          "InsightDetails.persistentDate": {
            "shortTitle": "Persistent Date",
```

```
        "title": "Insight Details Persistent Date",
        "type": "time"
      },
      "InsightDetails.spreading": {
        "shortTitle": "Spreading",
        "title": "Insight Details Spreading",
        "type": "boolean"
      },
      "InsightDetails.spreadingDate": {
        "shortTitle": "Spreading Date",
        "title": "Insight Details Spreading Date",
        "type": "time"
      },
      "InsightDetails.startedAt": {
        "shortTitle": "Started at",
        "title": "Insight Details Started at",
        "type": "time"
      },
      "InsightDetails.tClass": {
        "shortTitle": "T Class",
        "title": "Insight Details T Class",
        "type": "string"
      },
      "InsightDetails.tFamily": {
        "shortTitle": "T Family",
        "title": "Insight Details T Family",
        "type": "string"
      },
      "InsightDetails.threatLevel": {
        "shortTitle": "Threat Level",
        "title": "Insight Details Threat Level",
        "type": "number"
      },
      "InsightDetails.threatType": {
        "shortTitle": "Threat Type",
        "title": "Insight Details Threat Type",
        "type": "string"
      }
    },
    "measures": {
      "InsightDetails.blockedCount": {
        "drillMembers": [],
        "drillMembersGrouped": {
          "dimensions": [],
          "measures": []
        },
        "shortTitle": "Blocked Count",
        "title": "Insight Details Blocked Count",
        "type": "number"
      },
```

```
        "InsightDetails.mostRecentAt": {
          "drillMembers": [],
          "drillMembersGrouped": {
            "dimensions": [],
            "measures": []
          },
          "shortTitle": "Most Recent at",
          "title": "Insight Details Most Recent at",
          "type": "number"
        },
        "InsightDetails.notBlockedCount": {
          "drillMembers": [],
          "drillMembersGrouped": {
            "dimensions": [],
            "measures": []
          },
          "shortTitle": "Not Blocked Count",
          "title": "Insight Details Not Blocked Count",
          "type": "number"
        },
        "InsightDetails.numEvents": {
          "drillMembers": [],
          "drillMembersGrouped": {
            "dimensions": [],
            "measures": []
          },
          "shortTitle": "Num Events",
          "title": "Insight Details Num Events",
          "type": "number"
        }
      },
      "segments": {},
      "timeDimensions": {}
    },
    "data": [
      {
        "InsightDetails.blockedCount": "0",
        "InsightDetails.confidenceLevel": 3,
        "InsightDetails.description": "",
        "InsightDetails.feedSource": "Insight Detection Framework",
        "InsightDetails.insightId": "1a712155-e808-44c1-86da-e2489bd08c4e",
        "InsightDetails.insightStatus": "Active",
        "InsightDetails.mostRecentAt": "2023-11-21T05:03:00.000",
        "InsightDetails.notBlockedCount": "6166",
        "InsightDetails.numEvents": "6166",
        "InsightDetails.persistent": false,
        "InsightDetails.persistentDate": null,
        "InsightDetails.spreading": false,
        "InsightDetails.spreadingDate": null,
        "InsightDetails.startedAt": "2023-11-21T05:00:00.000",
```

```
        "InsightDetails.tClass": "TI-CONFIGURATIONISSUE",
        "InsightDetails.tFamily": "NXDOMAIN",
        "InsightDetails.threatLevel": 1,
        "InsightDetails.threatType": "NXDomain"
      }
    ],
    "dataSource": "POSTGRES_INSIGHTS",
    "dbType": "postgres",
    "extDbType": "cubestore",
    "external": false,
    "lastRefreshTime": "2023-12-07T10:29:03.269Z",
    "query": {
      "dimensions": [
        "InsightDetails.insightId"
      ],
      "filters": [
        {
          "member": "InsightDetails.insightId",
          "operator": "equals",
          "values": [
            "1a712155-e808-44c1-86da-e2489bd08c4e"
          ]
        }
      ],
      "limit": 10000,
      "measures": [
        "InsightDetails.blockedCount"
      ],
      "order": [
        {
          "desc": true,
          "id": "InsightDetails.mostRecentAt"
        }
      ],
      "rowLimit": 10000,
      "timeDimensions": [
        {
          "dateRange": [
            "2023-11-21T05:00:00.000",
            "2023-11-21T05:03:00.000"
          ],
          "dimension": "InsightDetails.eventSummaryHour"
        }
      ],
      "timezone": "UTC"
    },
    "slowQuery": false,
    "total": null
  }
},
```

```
  "insight-1a712155-e808-44c1-86da-e2489bd08c4e/machine-readable/insight-
summary/indicator-count.json": {
    "result": {
      "data": [
        {
          "AggIPSummary.action": "Not Blocked",
          "AggIPSummary.threatIndicatorDistinctCount": 1
        }
      ],
      "query": {
        "dimensions": [
          "AggIPSummary.action"
        ],
        "filters": [
          {
            "member": "AggIPSummary.tclass",
            "operator": "equals",
            "values": [
              "TI-CONFIGURATIONISSUE"
            ]
          },
          {
            "member": "AggIPSummary.tfamily",
            "operator": "equals",
            "values": [
              "NXDOMAIN"
            ]
          }
        ],
        "limit": 10000,
        "measures": [
          "AggIPSummary.threatIndicatorDistinctCount"
        ],
        "offset": 0,
        "timeDimensions": [
          {
            "dateRange": [
              "2023-11-21T05:00:00.000",
              "2023-11-21T05:03:00.000"
            ],
            "dimension": "AggIPSummary.timestamp",
            "granularity": ""
          }
        ]
      }
    }
  },
  "insight-1a712155-e808-44c1-86da-e2489bd08c4e/machine-readable/insight-
summary/infected-devices-count.json": {
    "result": {
```

```
    "data": [
      {
        "AggIPSummary.cidDistinctCount": 1
      }
    ],
    "query": {
      "dimensions": null,
      "filters": [
        {
          "member": "AggIPSummary.tclass",
          "operator": "equals",
          "values": [
            "TI-CONFIGURATIONISSUE"
          ]
        },
        {
          "member": "AggIPSummary.tfamily",
          "operator": "equals",
          "values": [
            "NXDOMAIN"
          ]
        },
        {
          "member": "AggIPSummary.cid",
          "operator": "set",
          "values": null
        }
      ],
      "limit": 10000,
      "measures": [
        "AggIPSummary.cidDistinctCount"
      ],
      "offset": 0,
      "order": {
        "AggIPSummary.timestamp": "desc"
      },
      "timeDimensions": [
        {
          "dateRange": [
            "2023-11-21T05:00:00.000",
            "2023-11-21T05:03:00.000"
          ],
          "dimension": "AggIPSummary.timestamp",
          "granularity": ""
        }
      ]
    }
  }
},
"insight-1a712155-e808-44c1-86da-e2489bd08c4e/machine-readable/insight-
```

```
summary/timeline-device-count-last-month.json": {
    "result": {
      "data": [
        {
          "AggIPSummary.qipDistinctCount": 0,
          "AggIPSummary.timestamp": "2023-11-07T00:00:00.000"
        }
      ],
      "query": {
        "dimensions": null,
        "filters": [
          {
            "member": "AggIPSummary.tclass",
            "operator": "equals",
            "values": [
              "TI-CONFIGURATIONISSUE"
            ]
          },
          {
            "member": "AggIPSummary.tfamily",
            "operator": "equals",
            "values": [
              "NXDOMAIN"
            ]
          }
        ],
        "limit": 10000,
        "measures": [
          "AggIPSummary.qipDistinctCount"
        ],
        "offset": 0,
        "order": {
          "AggIPSummary.timestamp": "desc"
        },
        "timeDimensions": [
          {
            "dateRange": [
              "2023-11-07T10:35:44.953",
              "2023-12-07T10:35:44.953"
            ],
            "dimension": "AggIPSummary.timestamp",
            "granularity": "day"
          }
        ]
      }
    }
  },
  "insight-1a712155-e808-44c1-86da-e2489bd08c4e/machine-readable/insight-
summary/timeline-event-summary-per-day-last-month.json": {
    "result": {
      "annotation": {
```

```
    "dimensions": {
      "InsightDetails.insightId": {
        "shortTitle": "Insight Id",
        "title": "Insight Details Insight Id",
        "type": "string"
      }
    },
    "measures": {
      "InsightDetails.numEvents": {
        "drillMembers": [],
        "drillMembersGrouped": {
          "dimensions": [],
          "measures": []
        },
        "shortTitle": "Num Events",
        "title": "Insight Details Num Events",
        "type": "number"
      }
    },
    "segments": {},
    "timeDimensions": {
      "InsightDetails.eventSummaryHour": {
        "shortTitle": "Event Summary Hour",
        "title": "Insight Details Event Summary Hour",
        "type": "time"
      },
      "InsightDetails.eventSummaryHour.day": {
        "shortTitle": "Event Summary Hour",
        "title": "Insight Details Event Summary Hour",
        "type": "time"
      }
    }
  },
  "data": [
    {
      "InsightDetails.eventSummaryHour": "2023-11-21T00:00:00.000",
      "InsightDetails.eventSummaryHour.day": "2023-11-21T00:00:00.000",
      "InsightDetails.insightId": "1a712155-e808-44c1-86da-e2489bd08c4e",
      "InsightDetails.numEvents": "6166"
    }
  ],
  "dataSource": "POSTGRES_INSIGHTS",
  "dbType": "postgres",
  "extDbType": "cubestore",
  "external": false,
  "lastRefreshTime": "2023-12-07T10:29:02.151Z",
  "query": {
    "dimensions": [
      "InsightDetails.insightId"
    ],
```

```
        "filters": [
          {
            "member": "InsightDetails.insightId",
            "operator": "equals",
            "values": [
              "1a712155-e808-44c1-86da-e2489bd08c4e"
            ]
          }
        ],
        "limit": 10000,
        "measures": [
          "InsightDetails.numEvents"
        ],
        "order": [
          {
            "desc": false,
            "id": "InsightDetails.mostRecentAt"
          }
        ],
        "rowLimit": 10000,
        "timeDimensions": [
          {
            "dateRange": [
              "2023-11-21T05:00:00.000",
              "2023-11-21T05:03:00.000"
            ],
            "dimension": "InsightDetails.eventSummaryHour",
            "granularity": "day"
          }
        ],
        "timezone": "UTC"
      },
      "slowQuery": false,
      "total": null
    }
  }
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`insight-{{insightId}}/machine-readable/asset-data.json.result.data[].AggIPSummary.qip`	Related Asset.Value	N/A	`insight-{{insightId}}/machine-readable/asset-data.json.result.data[].AggIPSummary.timestampMin`	`54.158.53.120`	N/A
`insight-{{insightId}}/machine-readable/asset-data.json.result.data[].AggIPSummary.location`	Related Asset.Attribute	Location	`insight-{{insightId}}/machine-readable/asset-data.json.result.data[].AggIPSummary.timestampMin`	`Ashburn,United States`	N/A
`insight-{{insightId}}/machine-readable/asset-data.json.result.data[].AggIPSummary.confidenceLevelMax`	Related Asset.Attribute	Confidence	`insight-{{insightId}}/machine-readable/asset-data.json.result.data[].AggIPSummary.timestampMin`	`3`	If the attribute already exists, the value will be updated
`insight-{{insightId}}/machine-readable/asset-data.json.result.data[].AggIPSummary.count`	Related Asset.Attribute	Count	`insight-{{insightId}}/machine-readable/asset-data.json.result.data[].AggIPSummary.timestampMin`	`6166`	If the attribute already exists, the value will be updated
`insight-{{insightId}}/machine-readable/asset-data.json.result.data[].AggIPSummary.threatLevelMax`	Related Asset.Attribute	Threat Level	`insight-{{insightId}}/machine-readable/asset-data.json.result.data[].AggIPSummary.timestampMin`	`1`	If the attribute already exists, the value will be updated
`insight-{{insightId}}/machine-readable/indicators.json.result.data[].AggIPSummary.threat_indicator`	Related Indicator.Value	FQDN	`insight-{{insightId}}/machine-readable/indicators.json.result.data[].AggIPSummary.timestampMin`	`happymail.com`	N/A
`insight-{{insightId}}/machine-readable/indicators.json.result.data[].AggIPSummary.location`	Related Indicator.Attribute	Location	`insight-{{insightId}}/machine-readable/indicators.json.result.data[].AggIPSummary.timestampMin`	`Ashburn,United States`	N/A
`insight-{{insightId}}/machine-readable/indicators.json.result.data[].AggIPSummary.confidenceLevelMax`	Related Indicator.Attribute	Confidence	`insight-{{insightId}}/machine-readable/indicators.json.result.data[].AggIPSummary.timestampMin`	`3`	If the attribute already exists, the value will be updated
`insight-{{insightId}}/machine-readable/`	Related Indicator.Attribute	Action	`insight-{{insightId}}/machine-readable/indicators.json.result.`	`Not Blocked`	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
indicators.json.result.data[].AggIPSummary.action			data[].AggIPSummary.timestampMin		
insight-{{insightId}}/machine-readable/indicators.json.result.data[].AggIPSummary.count	Related Indicator.Attribute	Count	insight-{{insightId}}/machine-readable/indicators.json.result.data[].AggIPSummary.timestampMin	6166	If the attribute already exists, the value will be updated
insight-{{insightId}}/machine-readable/indicators.json.result.data[].AggIPSummary.threatLevelMax	Related Indicator.Attribute	Threat Level	insight-{{insightId}}/machine-readable/indicators.json.result.data[].AggIPSummary.timestampMin	1	If the attribute already exists, the value will be updated
insight-{{insightId}}/machine-readable/event-data.json.result.data[].DnsLogs.tclass + tfamily + tproperty	Incident.Value	N/A	insight-{{insightId}}/machine-readable/event-data.json.result.data[].DnsLogs.timestamp	TI-CONFIGURATION ISSUE - NXDOMAIN - io.happymail.com	We concatenate the 3 values so the Incident value is unique
insight-{{insightId}}/machine-readable/event-data.json.result.data[].DnsLogs.confidence	Incident.Attribute	Confidence	insight-{{insightId}}/machine-readable/event-data.json.result.data[].DnsLogs.timestamp	High	If the attribute already exists, the value will be updated
insight-{{insightId}}/machine-readable/event-data.json.result.data[].DnsLogs.network	Incident.Attribute	Network	insight-{{insightId}}/machine-readable/event-data.json.result.data[].DnsLogs.timestamp	IR_Network	N/A
insight-{{insightId}}/machine-readable/event-data.json.result.data[].DnsLogs.policy_action	Incident.Attribute	Policy Action	insight-{{insightId}}/machine-readable/event-data.json.result.data[].DnsLogs.timestamp	Allow - No Log	N/A
insight-{{insightId}}/machine-readable/event-data.json.result.data[].DnsLogs.policy_name	Incident.Attribute	Policy Name	insight-{{insightId}}/machine-readable/event-data.json.result.data[].DnsLogs.timestamp	Default Global Policy	N/A
insight-{{insightId}}/machine-readable/event-data.json.result.data[].DnsLogs.tclass	Incident.Attribute	Class	insight-{{insightId}}/machine-readable/event-data.json.result.data[].DnsLogs.timestamp	TI-CONFIGURATION ISSUE	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`insight-{{insightId}}/machine-readable/event-data.json.result.data[].DnsLogs.tfamily`	Incident.Attribute	Family	`insight-{{insightId}}/machine-readable/event-data.json.result.data[].DnsLogs.timestamp`	`NXDOMAIN`	N/A
`insight-{{insightId}}/machine-readable/event-data.json.result.data[].DnsLogs.qip`	Related Indicator.Value	IP Address	`insight-{{insightId}}/machine-readable/event-data.json.result.data[].DnsLogs.timestamp`	`54.158.53.120`	N/A
`insight-{{insightId}}/machine-readable/event-data.json.result.data[].DnsLogs.qname`	Related Indicator.Value	FQDN	`insight-{{insightId}}/machine-readable/event-data.json.result.data[].DnsLogs.timestamp`	`atu5741.io.happymail.com`	N/A
`insight-{{insightId}}/machine-readable/event-data.json.result.data[].DnsLogs.tproperty`	Related Indicator.Value	FQDN	`insight-{{insightId}}/machine-readable/event-data.json.result.data[].DnsLogs.timestamp`	`io.happymail.com`	N/A
`insight-{{insightId}}/machine-readable/event-data.json.result.data[].DnsLogs.timestamp`	Incident.Ended_at	N/A	`N/A`	`2023-11-21 05:02:00`	N/A
`insightList[].startedAt`	Incident.Started_at	N/A	`N/A`	`2023-11-21T05:00:00Z`	N/A
`insightList[].priority + priorityText`	Incident.Attribute	Priority	`insightList[].startedAt`	`3 - LOW`	We concatenate the 2 values
`insightList[].status`	Incident.Attribute	Status	`insightList[].startedAt`	`Active`	If the attribute already exists, the value will be updated
`insightList[].storageId`	Incident.Attribute	Storage ID	`insightList[].startedAt`	`2300798`	N/A
`insightList[].threatLevel`	Incident.Attribute	Threat Level	`insightList[].startedAt`	`1`	If the attribute already exists, the value will be updated
`insightList[].threatType`	Incident.Attribute	Threat Type	`insightList[].startedAt`	`NXDomain`	N/A

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.

METRIC	RESULT
Run Time	1 minute
Asset	1
Asset Attributes	8
Incidents	4
Incident Attributes	40
Indicators	9
Indicator Attributes	20

Change Log

- **Version 1.0.0**
  - Initial release