ThreatQuotient

McAfee MVISION Cloud CDF Guide

Version 1.0.0

February 07, 2023

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	>= 4.35.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/mcafee-mvision-cloud-cdf

Introduction

The McAfee MVISION Cloud CDF for ThreatQ allows a user to ingest indicators, events, and event attributes into the ThreatQ platform.

The integration provides the following feed, which utilizes two supplemental feeds to retrieve and ingest data into ThreatQ.

- McAfee MVISION Cloud
  - **McAfee MVISION Cloud - Auth** (Supplemental) - retrieves the `access_token` and `tenantID`.
  - **McAfee MVISION Cloud - Object** (Supplemental) - retrieves Events data.

See the ThreatQ Mapping section for more details on these feeds and how they work.

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

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
McAfee Base URL	Your McAfee MVISION Cloud Base URL.
McAfee MVISION Cloud Username	Your McAfee MVISION Cloud Username.
McAfee MVISION Cloud Password	Your McAfee MVISION Cloud Password.
McAfee MVISION Cloud Tenant	You McAfee MVISION Cloud Tenant.
Severity	Select which severities for events you want to ingest into ThreatQ.
Incident Types	Select which Incident Types you want to ingest into ThreatQ.

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

McAfee MVISION Cloud

The McAfee MVISION Cloud feed utilizes two supplemental feeds, Auth and Object, to retrieve the data.

The following endpoint is used to retrieve the `access_token`:

```
POST https://iam.mcafee-cloud.com/iam/v1.1/token?
grant_type=password&client_id=0oae8q9q2y0IZOYUm0h7&username={username}&password={password}
&tenant_id={bps-tenant-id}&scope=shn.con.r web.adm.x web.rpt.x web.rpt.r web.lst.x
web.plc.x web.xprt.x web.cnf.x uam:admin
```

Sample Response:


```
{
    "tid": 1824642420,
    "token_type": "Bearer",
    "expires_in": 3600,
    "access_token":
"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6IjM4anlkcjFOdGltTHljV0lYTnZmbTUyXzQyYyIsImtpZCI6IjM4anlkcjFOdGltTHljV0lY
TnZmbTUyXzQyYyJ9.eyJpc3MiOiJodHRwczovL2lhbS5tY2FmZWUtY2xvdWQuY29tL2lhbS92MS4wIiwibm9uY2UiOiIiLCJhdWQiOiJtY2FmZWUiLCJn
aXZlbl9uYW1lIjoiWmFjaCIsImNsaWVudF9pZCI6IjBvYWU4cTlxMnkwSVpPWVVtMGg3IiwibG9jYWxlIjoiZW5fVVMiLCJleHAiOjE2NTUyOTc5MjQsI
mlkcCI6IjAwb2hwMWRtM3JnemdBUXYzMnA2IiwiZW1haWwiOiJ6YWNoLnNoYW1lc0B0aHJlYXRxLmNvbSIsIm5iZiI6MTY1NTI5NDMxNCwic3ViIjoiMD
B1YmNvdDRtbXdyTTRXMkIycDciLCJzY29wZSI6InNobi5jb24uciBvcGVuaWQiLCJ0ZW5hbnRfaWQiOiI4Q0NBNTY2RS1CMTY4LTQwMTktQkE3RS1DOTU
yNUYzNjdCNTQiLCJmYW1pbHlfbmFtZSI6IlNoYW1lcyIsInRva2VuX2lkIjoieG16LVZJX0RPenMyQkVoanRCMDlhaE9lZSIsInpvbmVpbmZvIjoiIiwi
bG9naW5faGludCI6InphY2guc2hhbWVzQHRocmVhdHEuY29tIn0.CLS-
PpM0J0RdD5QBpsZ5MnrK1fZspu40qYF7t5eUCgOvOk5DX7VEXrAszpy_N7UiA4Yx02K1pAOkY1KY9IJ5s5m4gOYArA9NHvML4Zp8L8uMQ8NVsdAH7WQaL
t_nKgLrlOBJbi_lcne1xVeIlv1b_D8fbVGjguNIOqwn1ffeksvjuGPu3Qvuj0fz0Ks43PLZJXNhNrrcG2oZ--
ZL7gCpxWitpvvIrxykbeen81XolTQdEWDvkbnAkeESQhnwbC0n5T7EW29y08m6b1cUubzLzUplknXeWIV_Kv94_Z-
Ml6spczOtabTwY8D3hQMZQzQeWk1l56pJqML27YewK0y6xQ"
}
```

McAfee MVISION Cloud Auth

The McAfee MVISION Cloud - Auth supplemental feed is used to retrieve the `access_token` and `tenantID`.

```
POST https://{base_url}/neo/neo-auth-service/oauth/token?grant_type=iam_token
```

Sample Response:


```
{
    "access_token":
"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0ZW5hbnROYW1lIjoiTWNBZmVlLUVCQyIsInVzZXJfbmFtZSI6InphY2guc2hhbWVzK01jQWZlZS1
FQkNAdGhyZWF0cS5jb20iLCJzY29wZSI6WyJyZWFkIiwid3JpdGUiXSwidGVuYW50SUQiOjczMTMwLCJleHAiOjE2NTUyOTQzOTUsInVzZXIiOiJ6YWNo
LnNoYW1lcytNY0FmZWUtRUJDQHRocmVhdHEuY29tIiwidXNlcklkIjoxNTY5MzcsImp0aSI6IjFlNWJiNTc1LTJmZjktNDU5OC1hNTc5LWE5NWRlNTUzM
DAwZiIsImVtYWlsIjoiemFjaC5zaGFtZXMrTWNBZmVlLUVCQ0B0aHJlYXRxLmNvbSIsImNsaWVudF9pZCI6InRydXN0ZWQtYXBwIn0.SIDn7vsV8jtIEO
A-tZL-LDGZb21_nJyGOquiPZ8OOzZxynGgqUouPQ4DBV5IFpOmlWNX5A93l1YPsnpO2DeeV6-WqXL-
C8F6_07ScYSnZPVNCH1WyuYWB8g4GE6M0DtbfkyiZc4qLpu6Y2QK1W2ObaHWpEbcPN2ylufy9hgPRGQ",
    "token_type": "bearer",
    "refresh_token":
"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0ZW5hbnROYW1lIjoiTWNBZmVlLUVCQyIsInVzZXJfbmFtZSI6InphY2guc2hhbWVzK01jQWZlZS1
FQkNAdGhyZWF0cS5jb20iLCJzY29wZSI6WyJyZWFkIiwid3JpdGUiXSwiYXRpIjoiMWU1YmI1NzUtMmZmOS00NTk4LWE1NzktYTk1ZGU1NTMwMDBmIiwi
dGVuYW50SUQiOjczMTMwLCJleHAiOjE2NTUzNzk4OTUsInVzZXIiOiJ6YWNoLnNoYW1lcytNY0FmZWUtRUJDQHRocmVhdHEuY29tIiwidXNlcklkIjoxN
TY5MzcsImp0aSI6IjFjYzBlNzYwLWZjZDEtNDQ2My05YmVmLWZhYTVmZTczNGRmNCIsImVtYWlsIjoiemFjaC5zaGFtZXMrTWNBZmVlLUVCQ0B0aHJlYX
RxLmNvbSIsImNsaWVudF9pZCI6InRydXN0ZWQtYXBwIn0.kcFus-
oDJVLOuxXzWqdU0ZNRGvblfpIn-8pZr4RhZa3o5dnqMphx0Y-4KpWkaxQDdolxJt5VqaRWX4VcILYhT_OpP6FdInadtgSw_Gv5ZWHPhrdKwO-bMZmt-
M6rbXKz48ckEPqvKEZA36beSC4Ryad9wJKlFVZ7W7wKjrf12Vk",
    "expires_in": 60,
    "scope": "read write",
    "tenantName": "McAfee-EBC",
    "tenantID": 99999,
    "user": "xxxxxxxxxxxxxxxx",
    "userId": 999999,
    "email": "xxxxxxxxxxxxxxx",
    "jti": "1e5bb575-2ff9-4598-a579-a95de553000f"
}
```

McAfee MVISION Cloud Object

The McAfee MVISION Cloud - Object supplemental feed is used to retrieve Events data.

`POST https://{base_url}/neo/watchtower/ui/v1/{tenantID}/incident/search`

Sample Response:


```
{
    "total": 14,
    "results": [
        {
            "incident_id":
"6:73130:2048:79d47eaaaed06229901e7b9c4d3cf67d77932242:ff8f8e30d1d53ba521be7ae02fb314eabd8607b9:1451406:1643712260704
",
            "tenant_id": 73130,
            "type": "malware_policy_violation",
            "severity": 2,
            "created_on_date": "2022-02-01T10:44:20.704Z",
            "inserted_on_date": "2022-02-01T10:46:02.389Z",
            "workflow": {
                "type": "workflow",
                "id": "57",
                "status": "new",
                "status_id": "2001",
                "consolidation_id": "2133",
                "last_executed_response_label": "Quarantined",
                "quarantine_detail": {
                    "type": "quarantine_detail",
                    "quarantine_item_status": "New"
                }
            },
            "incident_detail": {
                "type": "malware_policy_violation_detail",
                "event_id": "7313020486291:940035197275:nrt-dlp-malware#eicar_com.zip",
                "source": "api",
                "response": {
                    "type": "response",
                    "actions": [
                        {
                            "type": "policy_violation_response_action",
                            "response_label": "Quarantined",
                            "remediation_label": "Quarantine",
                            "weight": 4,
                            "name": "QUARANTINE"
                        }
                    ]
                },
                "activities": [
                    {
                        "type": "activity",
                        "name": "Created"
                    }
                ],
                "collaboration": {
                    "type": "collaboration",
```

```
                "shared_link": false,
                "collaborators": [],
                "internal_collaborators": []
            },
            "service": {
                "type": "service",
                "name": "Amazon S3",
                "id": 2048,
                "instance": {
                    "type": "instance",
                    "instance_id": 6291,
                    "instance_name": "AWS-Cloud Sec"
                },
                "accountIds": null
            },
            "user": {
                "type": "user",
                "name": "AWS:AIDAJRUAWGWUMBQ3JLMDU",
                "key": "940035197275"
            },
            "content": {
                "type": "content",
                "item": {
                    "type": "item",
                    "id": "nrt-dlp-malware#eicar_com.zip",
                    "name": "eicar_com.zip",
                    "item_type": "file",
                    "parent_name": "nrt-dlp-malware",
                    "hierarchy": "nrt-dlp-malware",
                    "created_on_date": "2022-02-01T10:44:20.704Z",
                    "modified_on_date": "2022-02-01T10:44:20.704Z",
                    "size": 184
                },
                "policy_result": {
                    "type": "policy_result",
                    "policy_id": 1451406,
                    "policy_name": "Workload Malware Scan",
                    "extracted_item_types": [
                        "ZIP Archive",
                        "ASCII Text"
                    ],
                    "matches": [],
                    "total_match_count": 0,
                    "total_unique_content_match_count": 0,
                    "match_counts": {},
                    "match_file_names": [],
                    "comprehensive_result": {
                        "type": "comprehensive_result",
                        "incident_consolidation_type": "secondary",
                        "primary_policy_id": 355727,
                        "has_secondary": true
                    },
                    "does_incident_have_match_highlights": false
                }
            },
            "additional_details": {
                "cloudFileMetadata": "{\n  \"id\" : \"nrt-dlp-malware#eicar_com.zip\",\n  \"ownerId\" :
\"AWS:AIDAJRUAWGWUMBQ3JLMDU\",\n  \"isDirectory\" : false,\n  \"name\" : \"eicar_com.zip\",\n  \"createdAt\" :
\"2022-02-01T10:44:20.704Z\",\n  \"modifiedAt\" : \"2022-02-01T10:44:20.704Z\",\n  \"checksum\" : {\n
\"checksum\" : \"6ce6f415d8475545be5ba114f208b0ff\",\n    \"algorithm\" : \"MD5\"\n  },\n  \"subfileChecksum\" : {\n
\"eicar.com\" : [ {\n      \"checksum\" : \"3395856ce81f2b7382dee72602f798b642f14140\",\n      \"algorithm\" :
```

```
\"SHA1\"\n    }, {\n      \"checksum\" : \"275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f\",\n
\"algorithm\" : \"SHA256\"\n    }, {\n      \"checksum\" : \"44d88612fea8a8f36de82e1278abb02f\",\n
\"algorithm\" : \"MD5\"\n    } ]\n  },\n  \"size\" : 184,\n  \"downloadUrl\" : \"nrt-dlp-malware#eicar_com.zip\",\n
\"folder\" : {\n    \"id\" : \"/nrt-dlp-malware\",\n    \"name\" : \"nrt-dlp-malware\"\n  },\n  \"folderHierarchy\" :
[ {\n    \"id\" : \"/nrt-dlp-malware\",\n    \"name\" : \"nrt-dlp-malware\"\n  } ],\n  \"isSharedLinkEnabled\" :
false,\n  \"isFileSharedExternally\" : false,\n  \"isTrashed\" : false,\n  \"eTag\" :
\"6ce6f415d8475545be5ba114f208b0ff\",\n  \"sharedLinks\" : [ ],\n  \"additionalInfo\" : { },\n  \"checksumMap\" : {\n
\"MD5\" : {\n      \"checksum\" : \"6ce6f415d8475545be5ba114f208b0ff\",\n      \"algorithm\" : \"MD5\"\n    },\n
\"SHA1\" : {\n      \"checksum\" : \"da39a3ee5e6b4b0d3255bfef95601890afd80709\",\n      \"algorithm\" :
\"SHA1\"\n    },\n    \"SHA256\" : {\n      \"checksum\" :
\"e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855\",\n      \"algorithm\" : \"SHA256\"\n    }\n  },
\n  \"folderPath\" : \"nrt-dlp-malware\",\n  \"folderIdPath\" : \"/nrt-dlp-malware\",\n  \"folderIdHierarchy\" :
[ \"/nrt-dlp-malware\" ],\n  \"folderNameHierarchy\" : [ \"nrt-dlp-malware\" ],\n  \"checksums\" : [ {\n
\"checksum\" : \"6ce6f415d8475545be5ba114f208b0ff\",\n    \"algorithm\" : \"MD5\"\n  }, {\n    \"checksum\" :
\"da39a3ee5e6b4b0d3255bfef95601890afd80709\",\n    \"algorithm\" : \"SHA1\"\n  }, {\n    \"checksum\" :
\"e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855\",\n    \"algorithm\" : \"SHA256\"\n  } ],\n
\"etag\" : \"6ce6f415d8475545be5ba114f208b0ff\"\n}",
                    "createdOn_timestamp": "1643712362369"
                },
                "account_id": "940035197275",
                "storage": {
                    "type": "storage",
                    "name": "nrt-dlp-malware"
                },
                "matched_policies": {
                    "type": "matched_policies",
                    "matched_policies_unique_identifier": "98226976-d3c1-404d-acb2-b6ab1f1ce995",
                    "matched_policy_names": [
                        "NRT- Malware scan for AWS S3",
                        "Workload Malware Scan"
                    ]
                },
                "policy_source": "McAfee Skyhigh DLP",
                "malware": {
                    "type": "malware",
                    "name": "Artemis!6ce6f415d847",
                    "category": "Trojan",
                    "confidence": "Very High",
                    "checksums": [
                        {
                            "checksum": "6ce6f415d8475545be5ba114f208b0ff",
                            "algorithm": "MD5"
                        },
                        {
                            "checksum": "da39a3ee5e6b4b0d3255bfef95601890afd80709",
                            "algorithm": "SHA1"
                        },
                        {
                            "checksum": "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855",
                            "algorithm": "SHA256"
                        }
                    ],
                    "detection_source": "GTI",
                    "descriptive_name": "Trojan:Artemis!6ce6f415d847"
                },
                "resource": {
                    "type": "resource",
                    "id": "nrt-dlp-malware",
                    "iaas_resource_id": "e82d8c7ac5eff9d80d3d9a35a8a9450cfe340804fd7aa090bd9e9dd725658399",
                    "entity_type_id": 2048
                },
                "scan": {
```

```
                    "type": "scan",
                    "id": 1768282,
                    "name": "AWS-VM-VA-Scan",
                    "instance": "2021-12-22T17:17:17.645Z"
                },
                "activities": [
                    {
                        "type": "activity",
                        "name": "On Demand Scan"
                    }
                ]
            },
            "last_modified_date": "2022-02-01T10:46:02.369Z",
            "user_attributes": {},
            "significantly_updated_at": "2022-02-01T10:46:02.369Z"
        },
        {
            "incident_id":
"8:73130:2049:940035197275:858784:8fe11441c68999bca246956a4112879771525498:93932:VERSION_2",
            "tenant_id": 73130,
            "type": "vulnerability_violation",
            "severity": 2,
            "created_on_date": "2021-12-23T17:16:28.089Z",
            "inserted_on_date": "2021-12-23T17:16:29.382Z",
            "workflow": {
                "type": "workflow",
                "id": "139",
                "status": "archived",
                "status_id": "2006",
                "last_executed_response_label": "Violation Detected"
            },
            "incident_detail": {
                "type": "vulnerability_violation_detail",
                "response": {
                    "type": "response",
                    "actions": [
                        {
                            "type": "audit_violation_response_action",
                            "response_label": "Violation Detected",
                            "remediation_label": "Violation Detected",
                            "weight": 2,
                            "name": "VIOLATION_DETECTED"
                        }
                    ]
                },
                "account_id": "940035197275",
                "account_name": "MVC-AWS",
                "audit_item": "eksworkshop-eksctl",
                "cves": [
                    "- - 2 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8561 Medium 2021-09-20T17:15Z
kubeapiserver:1.19.13 -",
                    "- - 2 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25735 Medium 2021-09-06T12:15Z
kubeapiserver:1.19.13 -"
                ],
                "scan": {
                    "type": "scan",
                    "id": 1770686,
                    "name": "AWS-VM-VA-Scan",
                    "instance": "2021-12-23T17:16:28.089Z"
                },
                "resource": {
```

```
            "type": "resource",
            "id": "arn:aws:eks:us-west-2:940035197275:cluster/eksworkshop-eksctl",
            "iaas_resource_id": "f72340b775882d2c3adacde049c8513b417bcf7bb9c07ba62548a29f1c26b4d2",
            "entity_type_id": 2039
        },
        "scan_history": [
            {
                "type": "scan",
                "id": 1801487,
                "name": "AWS-VM-VA-Scan",
                "instance": "2022-01-05T17:18:03.895Z"
            },
            {
                "type": "scan",
                "id": 1798966,
                "name": "AWS-VM-VA-Scan",
                "instance": "2022-01-04T17:16:03.999Z"
            },
            {
                "type": "scan",
                "id": 1796547,
                "name": "AWS-VM-VA-Scan",
                "instance": "2022-01-03T17:13:52.292Z"
            },
            {
                "type": "scan",
                "id": 1794199,
                "name": "AWS-VM-VA-Scan",
                "instance": "2022-01-02T17:11:46.307Z"
            },
            {
                "type": "scan",
                "id": 1791878,
                "name": "AWS-VM-VA-Scan",
                "instance": "2022-01-01T17:14:31.680Z"
            }
        ],
        "service": {
            "type": "service",
            "name": "Amazon Web Services",
            "id": 2049,
            "instance": {
                "type": "instance",
                "instance_id": 6291,
                "instance_name": "AWS-Cloud Sec"
            },
            "accountIds": null
        },
        "user": {
            "type": "user",
            "name": "N/A"
        },
        "content": {
            "type": "content",
            "item": {
                "type": "item",
                "id": "arn:aws:eks:us-west-2:940035197275:cluster/eksworkshop-eksctl",
                "name": "eksworkshop-eksctl",
                "item_type": "eks",
                "created_on_date": "2022-01-05T17:18:03.895Z",
                "modified_on_date": "2022-01-05T17:18:03.895Z"
```

```
                    },
                    "policy_result": {
                        "type": "policy_result",
                        "policy_id": 858784,
                        "policy_name": "VM- Vulnerability scan"
                    }
                },
                "name": "VM Vulnerability",
                "updated_at": "2021-12-23T17:16:28.089Z",
                "created_on_date": "2021-12-23T17:16:28.089Z",
                "policy_category": {
                    "type": "policy_category"
                },
                "scan_config_id": "93932"
            },
            "last_modified_date": "2022-04-10T03:59:43.346Z",
            "user_attributes": {},
            "significantly_updated_at": "2022-04-10T03:59:43.346Z"
        }
    ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
results[].incident_detail.content.item.name	Event.Title	MVISION Cloud	results[].created_on_date	MVISION Cloud Malware Incident - eicar_com.zip	Depending on the value present on `results[].type` the title of the Event will be adjusted
results[].incident_detail.content.item.name	Event.Title	MVISION Cloud	results[].created_on_date	MVISION Cloud Vulnerability Incident - eksworkshop-eksctl	Depending on the value present on `results[].type` the title of the Event will be adjusted
results[].type	Event.Attribute	Incident Type	results[].created_on_date	malware_policy_violation	N/A
results[].severity	Event.Attribute	Severity	results[].created_on_date	2	N/A
results[].inserted_on_date	Event.Attribute	Inserted On	results[].created_on_date	2022-02-01T10:46:02.389Z	N/A
results[].incident_detail.response.type	Event.Attribute	Response Type	results[].created_on_date	response	N/A
results[].incident_detail.response.actions[].response_label	Event.Attribute	Response Label	results[].created_on_date	Quarantined	N/A
results[].incident_detail.response.actions[].remediation_label	Event.Attribute	Remediation Label	results[].created_on_date	Quarantine	N/A
results[].incident_detail.scan.name	Event.Attribute	Scan Name	results[].created_on_date	AWS-VM-VA-Scan	N/A
results[].incident_detail.scan.instance	Event.Attribute	Scan Instance	results[].created_on_date	2021-12-22T17:17:17.645Z	N/A
results[].incident_detail.scan.instance	Event.Attribute	Scan Instance Name	results[].created_on_date	AWS-Cloud Sec	N/A
results[].incident_detail.content.policy_result.policy_name	Event.Attribute	Policy Name	results[].created_on_date	Workload Malware Scan	N/A
results[].incident_detail.policy_source	Event.Attribute	Policy Source	results[].created_on_date	McAfee Skyhigh DLP	Only for Events where `results[].type == malware_policy_violation`
results[].incident_detail.malware.type	Event.Attribute	Malware Type	results[].created_on_date	malware	Only for Events where `results[].type == malware_policy_violation`
results[].incident_detail.malware.name	Event.Attribute	Malware Name	results[].created_on_date	Artemis!6ce6f415d847	Only for Events where `results[].type == malware_policy_violation`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
results[].incident_detail.malware.category	Event.Attribute	Malware Category	results[].created_on_date	Trojan	Only for Events where `results[].type == malware_policy_violation`
results[].incident_detail.malware.confidence	Event.Attribute	Malware Confidence	results[].created_on_date	Very High	Only for Events where `results[].type == malware_policy_violation`
results[].incident_detail.malware.detection_source	Event.Attribute	Malware Detection Source	results[].created_on_date	GTI	Only for Events where `results[].type == malware_policy_violation`
results[].incident_detail.activities[]	Event.Attribute	Activity Type	results[].created_on_date	On Demand Scan	Only for Events where `results[].type == malware_policy_violation`
results[].incident_detail.malware.checksums[].checksum	Related Indicator.Value	MD5	results[].created_on_date	6ce6f415d8475545be5ba114f208b0ff	Only for Events where `results[].type == malware_policy_violation`
results[].incident_detail.malware.checksums[].checksum	Related Indicator.Value	SHA-1	results[].created_on_date	da39a3ee5e6b4b0d3255bfef95601890afd80709	Only for Events where `results[].type == malware_policy_violation`
results[].incident_detail.malware.checksums[].checksum	Related Indicator.Value	SHA-256	results[].created_on_date	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	Only for Events where `results[].type == malware_policy_violation`
results[].incident_detail.content.item.name	Related Indicator.Value	Filename	results[].created_on_date	eicar_com.zip	Only for Events where `results[].type == malware_policy_violation`
results[].incident_detail.cves	Related Indicator.Value	CVE	results[].created_on_date	CVE-2020-8561	Only for Events where `results[].type == vulnerability_violation`

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.

McAfee MVISION Cloud

METRIC	RESULT
Run Time	2 minutes
Events	12
Event Attributes	176
Indicators	41

Change Log

- **Version 1.0.0**
  - Initial release