ThreatQuotient

VMware Carbon Black EDR On Premise Action Bundle

Version 1.0.0

October 29, 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	>= 5.25.0
ThreatQ TQO License Required	Yes
Third-Party Deployment Method	On Premise
Support Tier	ThreatQ Supported

Introduction

The VMware Carbon Black EDR On Premise action bundle enriches indicators and assets in a data collection with information found in VMWare Carbon Black EDR On Premise instances.

WMWare Carbon Black EDR is used to record and save endpoint activity data. Security analysts can use this data to find in real time potential threats.

The integration provides the following actions:

- **VMware Carbon Black EDR On Premise - Process Enrichment** - queries data regarding processes.
- **VMware Carbon Black EDR On Premise - Binary Enrichment** - queries data regarding binaries.
- **VMware Carbon Black EDR On Premise - Alert Enrichment** - queries data regarding alerts.

The integration is compatible with the following object types:

- Assets
- Indicators

The integration returns the following enriched system objects:

- Assets
- Indicators

This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

- An VMware Carbon Black EDR On Premise instance.
- An VMware Carbon Black EDR API Token - see https://developer.carbonblack.com/reference/enterprise-response/authentication/ for more information.
- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing at least one of the following object types:
  - Asset
  - Indicator

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 action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
   - Drag and drop the zip file into the dialog box
   - Select **Click to Browse** to locate the zip file on your local machine
6. Select the actions to install, when prompted, and then click on **Install**.

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

The action(s) have now been installed on your ThreatQ instance. You will still need to configure the action(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:

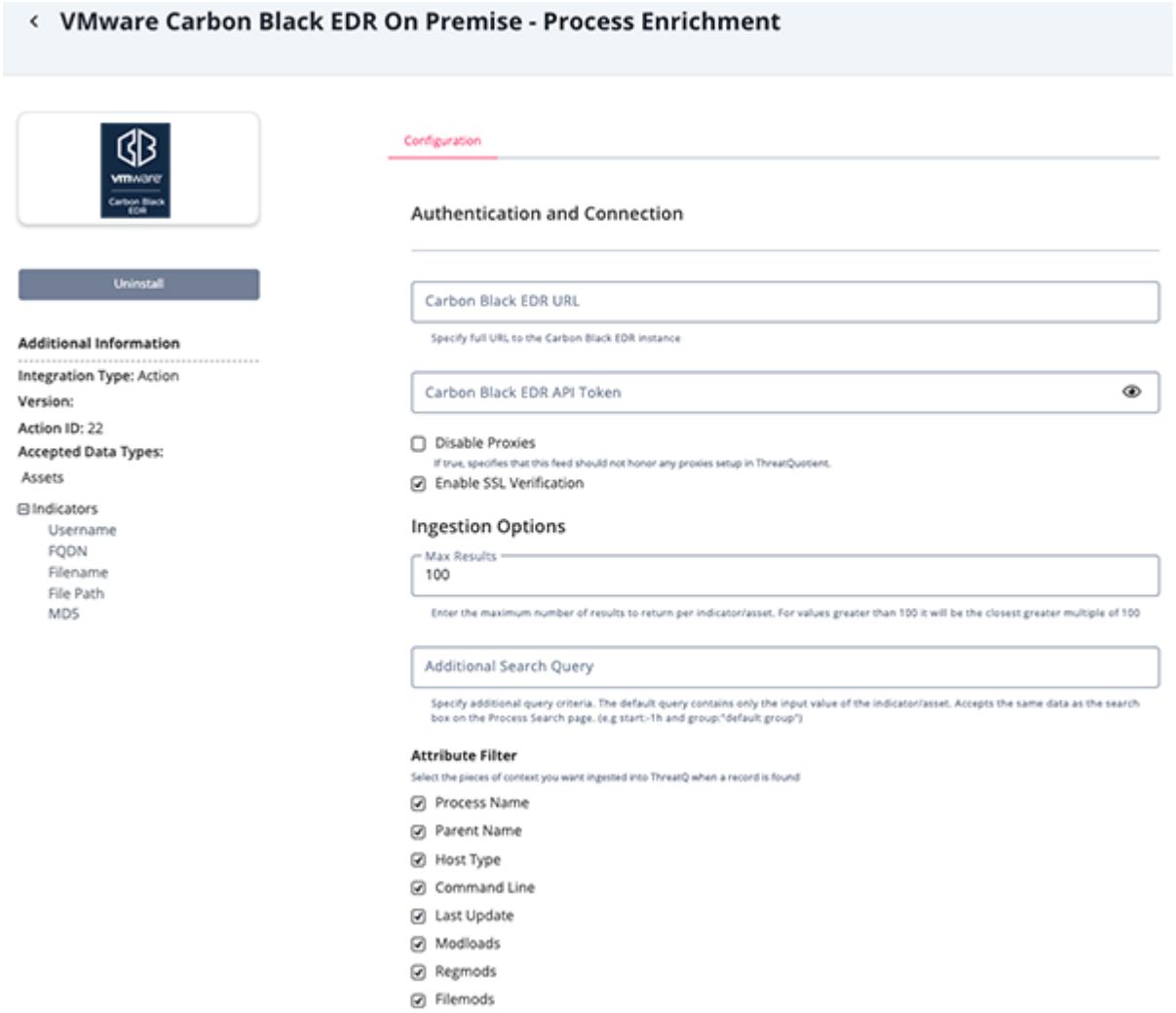
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

Process Enrichment Parameters

PARAMETER	DESCRIPTION
Carbon Black EDR URL	Specify full URL to the Carbon Black EDR instance. The format is `https://<hostname>:<port>`.
Carbon Black EDR API Token	The API Token used to connect to Carbon Black EDR instance.
Disable Proxies	Enable this parameter if the action should not honor the proxies set in ThreatQ.
Enable SSL Verification	When enabled, the action validates the host-provided SSL certificate. This option is enabled by default.
Max Results	Enter the maximum number of results to return per indicator/asset. The value you enter will round to the nearest 100. Example: if you enter 180, the integration will ingest 200.

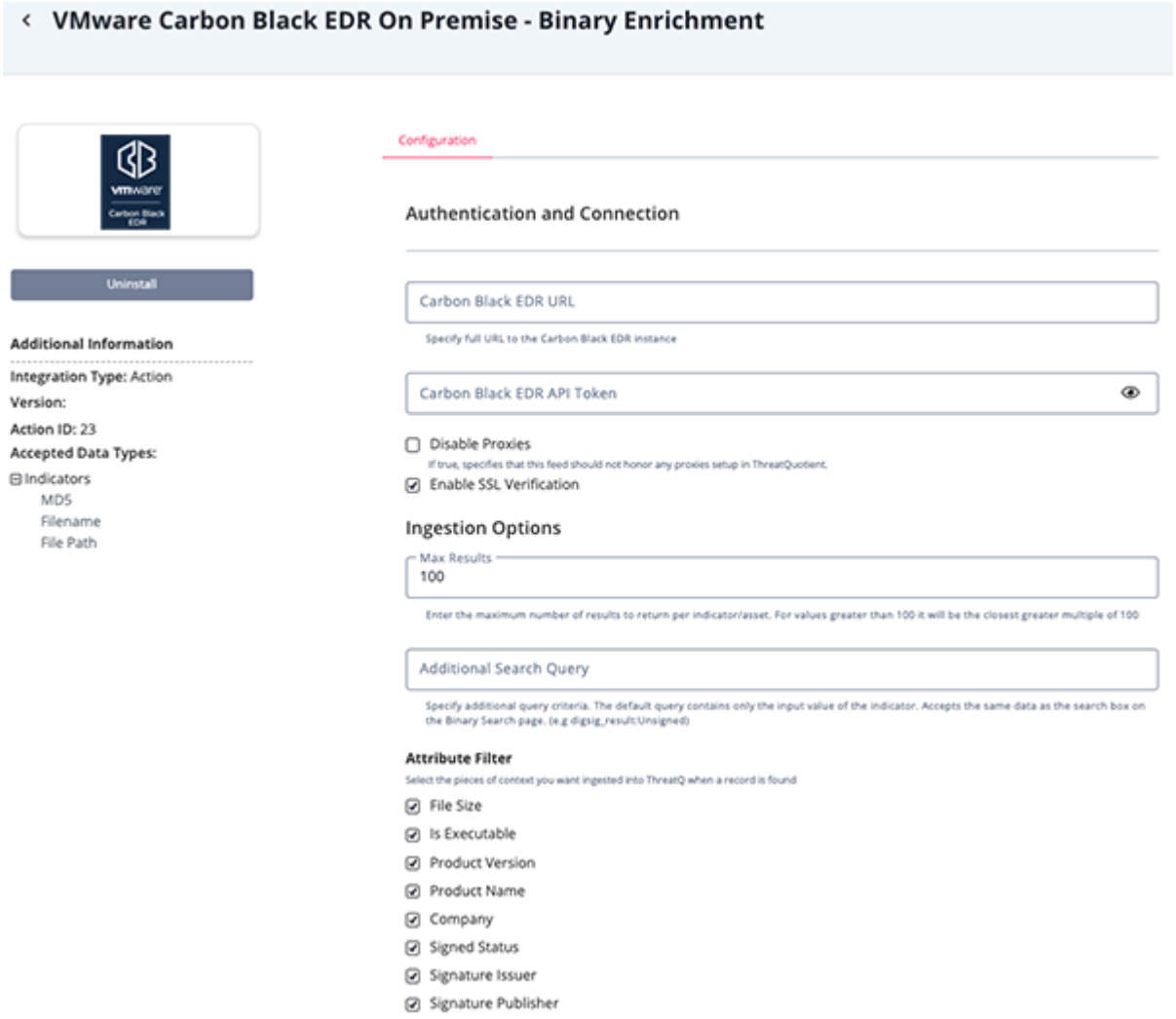
PARAMETER	DESCRIPTION
Additional Search Query	Specify additional query criteria. The default query contains only the input value of the indicator/asset. Accepts the same data as the search box on the Process Search page. (e.g start:-1h and group:"default group")
Attribute Filter	Select the pieces of context to ingest into the ThreatQ platform when a record is found. Options include: ◦ Process Name ◦ Parent Name ◦ Host Type ◦ Command Line ◦ Last Update ◦ Modloads ◦ Regmods ◦ Filemods ◦ Netconns ◦ Fileless Scriptloads ◦ Children ◦ Carbon Black EDR Group ◦ Operating System
Related Objects Filter	Select the related objects to ingest into ThreatQ when a record is found. Options include: ◦ Process MD5 (Indicator) ◦ Process Path (Indicator) ◦ Username (Indicator) ◦ Hostname (Asset)
Objects Per Run	The number of objects to process per run of the workflow.



Binary Enrichment Parameters

PARAMETER	DESCRIPTION
Carbon Black EDR URL	Specify full URL to the Carbon Black EDR instance. The format is: `https://<hostname>:<port>`.
Carbon Black EDR API Token	The API Token used to connect to Carbon Black EDR instance.
Disable Proxies	Enable this parameter if the action should not honor the proxies set in ThreatQ.

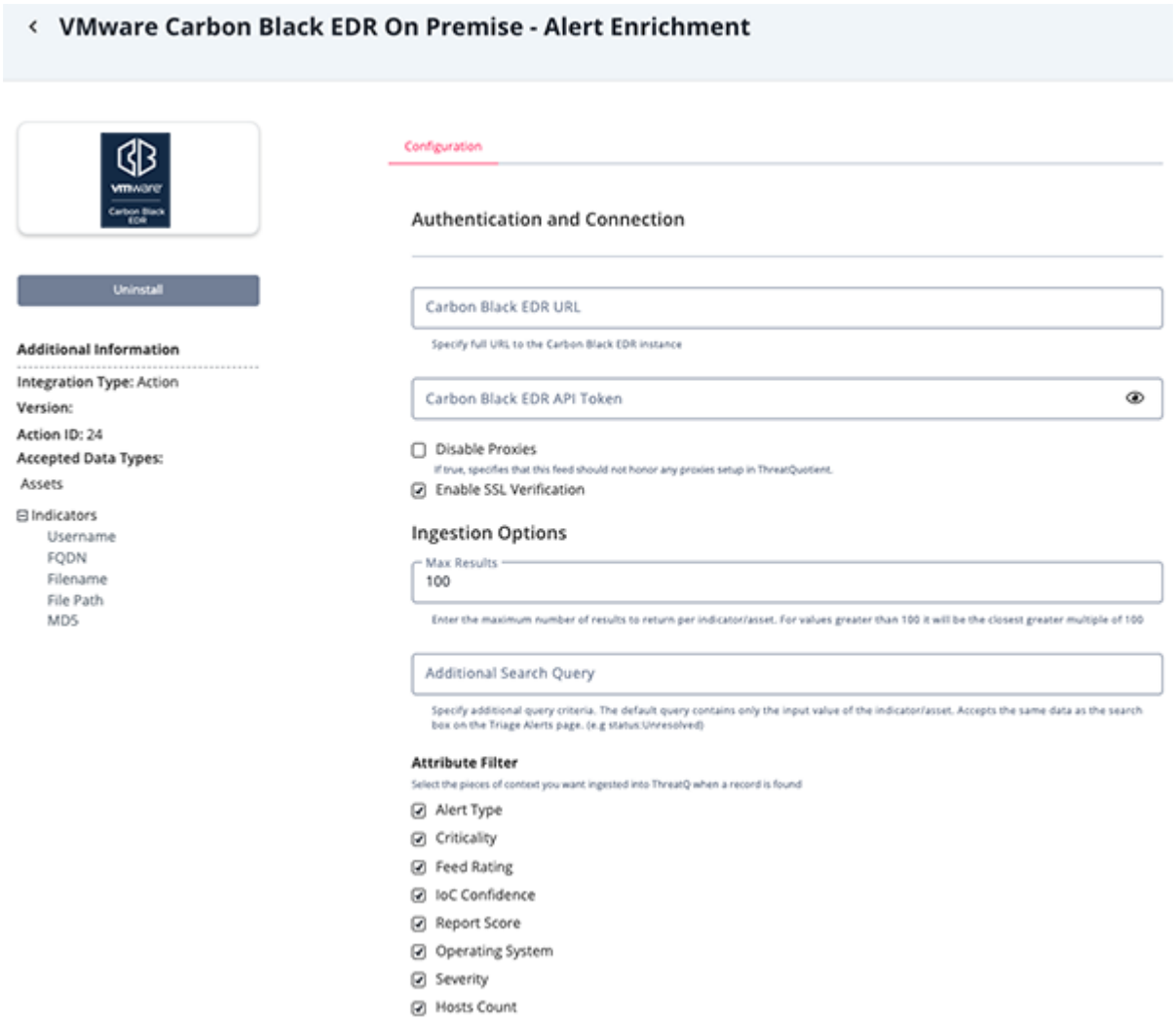
PARAMETER	DESCRIPTION
Enable SSL Verification	When enabled, the action validates the host-provided SSL certificate. This option is enabled by default.
Max Results	Enter the maximum number of results to return per indicator/asset. For values greater than 100 it will be the closest greater multiple of 100.
Additional Search Query	Specify additional query criteria. The default query contains only the input value of the indicator/asset. Accepts the same data as the search box on the Process Search page. (e.g start:-1h and group:"default group")
Attribute Filter	Select the pieces of context to ingest into the ThreatQ platform when a record is found. Options include: ◦ File Size ◦ Is Executable ◦ Product Version ◦ Product Name ◦ Company ◦ Signed Status ◦ Signature Issuer ◦ Signature Publisher ◦ Virustotal Score ◦ Operating System ◦ Hosts Count
Objects Per Run	The number of objects to process per run of the workflow



Alert Enrichment Parameters

PARAMETER	DESCRIPTION
Carbon Black EDR URL	Specify full URL to the Carbon Black EDR instance. The format is: `https://<hostname>:<port>`.
Carbon Black EDR API Token	The API Token used to connect to Carbon Black EDR instance.
Disable Proxies	If true, specifies that this feed should not honor any proxies setup in ThreatQuotient

PARAMETER	DESCRIPTION
Enable SSL Verification	When checked, validates the host-provided SSL certificate. Checked by default
Max Results	Enter the maximum number of results to return per indicator/asset. For values greater than 100 it will be the closest greater multiple of 100
Additional Search Query	Specify additional query criteria. The default query contains only the input value of the indicator/asset. Accepts the same data as the search box on the Process Search page. (e.g start:-1h and group:"default group")
Attribute Filter	Select the pieces of context to ingest into the ThreatQ platform when a record is found. Options include: ◦ Alert Type ◦ Criticality ◦ Feed Rating ◦ IoC Confidence ◦ Report Score ◦ Operating System ◦ Severity ◦ Hosts Count ◦ Modloads ◦ Regmods ◦ Filemods ◦ Netconns ◦ Fileless Scriptloads ◦ Children ◦ Signed Status ◦ Process Name
Related Objects Filter	Select the related objects to ingest into the ThreatQ platform when a record is found. Options include: ◦ MD5 ◦ Filename ◦ File Path ◦ Username ◦ Hostname (Asset)
Objects Per Run	The number of objects to process per run of the workflow



5. Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The following actions are available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
VMware Carbon Black EDR On Premise - Process Enrichment	Queries data regarding processes.	Indicator/ Asset	Username, FQDN, File Path, Filename, MD5
VMware Carbon Black EDR On Premise - Binary Enrichment	Queries data regarding binaries.	Indicator	File Path, Filename, MD5
VMware Carbon Black EDR On Premise - Alert Enrichment	Queries data regarding alerts.	Indicator/ Asset	Username, FQDN, File Path, Filename, MD5

Process Enrichment

The Process Enrichment action queries data regarding process saved in VMWare Carbon Black EDR. This search is the same as the one performed in UI on the Process Search page. The default query contains only the input value of the indicator/asset. The user field `Additional Search Query` allows additional query criteria. It accepts the same data as the search box on the Process Search page (e.g start:-1h and group:"default group"). More information can be found at: https://developer.carbonblack.com/resources/query_overview.pdf.

`GET "{{CARBON_BLACK_EDR_INSTANCE}}/api/v1/process"`

Query Parameters:

```
{
   "q": "f34217144e41c2a0ea56df7056f0b4d7 and (start:-1h and group:\"default
group\")"
}
```

Sample Response:

```
{
  "results": [
    {
      "unique_id": "00000005-0015-ab5c-01db-2386a75d5e87-0192ade246f5",
      "parent_unique_id": "00000005-ffff-ffff-0000-000000000000-000000000001",
      "id": "00000005-0015-ab5c-01db-2386a75d5e87",
      "parent_id": "00000005-ffff-ffff-0000-000000000000",
      "path": "/usr/sbin/xtables-nft-multi",
      "process_name": "xtables-nft-multi",
      "process_md5": "6efe836697311c356a7db2f39e1ac6a2",
      "parent_name": "runc",
      "parent_md5": "00000000000000000000000000000000",
      "hostname": "workstation1",
      "host_type": "workstation",
      "os_type": "linux",
      "start": "2024-10-21T06:58:37.806Z",
      "last_update": "2024-10-21T06:58:37.806Z",
      "last_server_update": "2024-10-21T07:02:20.780Z",
      "sensor_id": 5,
      "group": "int_7535",
      "segment_id": 1729494140661,
      "username": "root",
      "cmdline": "/usr/sbin/iptables -t filter -S FLANNEL-FWD 1 --wait",
      "process_pid": 1420124,
      "parent_pid": -1,
      "comms_ip": 175178466,
      "interface_ip": 175178466,
      "emet_config": "",
      "terminated": false,
      "filtering_known_dlls": false,
      "logon_type": -1,
```

```
      "tampered": false,
      "regmod_count": 1,
      "netconn_count": 2,
      "filemod_count": 3,
      "modload_count": 4,
      "childproc_count": 5,
      "crossproc_count": 0,
      "emet_count": 0,
      "processblock_count": 0,
      "fileless_scriptload_count": 6
    }
  ],
  "elapsed": 0.043074607849121094,
  "all_segments": true,
  "comprehensive_search": true,
  "start": 0,
  "total_results": 6066,
  "terms": [
    "username:root",
    "start:-1h",
    "group:\"int_7535\""
  ],
  "tagged_pids": {},
  "incomplete_results": false
}
```

ThreatQuotient provides the following default mapping for this action:

> Mappings are based on each of the items within the `.results[]` JSON path.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.process_md5	Related Indicator	MD5	.start	6efe836697311c356a7db2f39e1ac6a2	User-configurable
.path	Related Indicator	File Path	.start	/usr/sbin/xtables-nft-multi	User-configurable
.username	Related Indicator	Username	.start	root	User-configurable
.hostname	Related Asset	N/A	.start	workstation1	User-configurable
.process_na me	Related Indicator Attribute	Process Name	.start	xtables-nft-multi	User-configurable
.parent_name	Related Indicator Attribute	Parent Name	.start	runc	User-configurable
.cmdline	Related Indicator Attribute	Command Line	.start	/usr/sbin/iptables -t filter -S FLANNEL-FWD 1 --wait	User-configurable
.last_update	Related Indicator Attribute	Last Update	.start	2024-10-21T06:58:37.806Z	User-configurable. Updatable
.modload_count	Related Indicator Attribute	Modloads	.start	4	User-configurable. Updatable
.regmod_count	Related Indicator Attribute	Regmods	.start	1	User-configurable. Updatable
.filemod_count	Related Indicator Attribute	Filemods	.start	3	User-configurable. Updatable
.netconn_count	Related Indicator Attribute	Netconns	.start	2	User-configurable. Updatable
.childproc_count	Related Indicator Attribute	Children	.start	5	User-configurable. Updatable
.fileless_scriptload_count	Related Indicator Attribute	Fileless Scriptloads	.start	6	User-configurable. Updatable
.group	Related Indicator Attribute	Carbon Black EDR Group	.start	int_7535	User-configurable.
.os_type	Related Indicator Attribute	Operating System	.start	Linux	User-configurable. Title cased

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.host_type	Related Asset Attribute	Host Type	.start	Workstation	User-configurable. Title cased

Binary Enrichment

The Binary Enrichment action queries data regarding binary files saved in VMWare Carbon Black EDR. This search is the same as the one performed in UI on the Binary Search page. The default query contains only the input value of the indicator. The user field `Additional Search Query` allows additional query criteria. It accepts the same data as the search box on the Binary Search page (e.g digsig_result:Unsigned).

More information can be found at: https://developer.carbonblack.com/resources/query_overview.pdf.

`GET "{{CARBON_BLACK_EDR_INSTANCE}}/api/v1/binary"`

Query Parameters:

```
{
   "q": "f34217144e41c2a0ea56df7056f0b4d7 and (digsig_result:Unsigned)"
}
```

Sample Response:

```
{
  "results": [
    {
      "md5": "A92ACA8CE49D71D26B5853D0442A7473",
      "sha256":
"1ff597e8bd590896c17d856188d1f0950a5a4cf4e7d2c0b40a6c1eb95c9586b3",
      "signed": "Unsigned",
      "timestamp": "2024-10-17T10:22:17.771Z",
      "company_name": "Windows",
      "product_name": "Microsoft Office Word",
      "original_filename": "(unknown)",
      "observed_filename": [
        "/usr/lib/x86_64-linux-gnu/ld-linux-x86-64.so.2"
      ],
      "internal_name": "(unknown)",
      "product_version": "6.3.9200",
      "file_version": "(unknown)",
      "file_desc": "Documents editor",
      "server_added_timestamp": "2024-10-17T10:22:17.771Z",
      "copied_mod_len": 122480,
      "orig_mod_len": 122480,
      "digsig_result": "Unsigned",
      "is_executable_image": false,
      "is_64bit": true,
      "facet_id": 708717,
      "endpoint": [
        "int-7535|5"
      ],
      "group": [
        "int_7535"
      ],
```

```
      "os_type": "Linux",
      "cb_version": 780,
      "host_count": 1,
      "last_seen": "2024-10-17T10:30:04.587Z",
      "digsig_issuer": "DigiCert",
      "digsig_publisher": "Digi",
      "alliance_score_virustotal": 20,
      "watchlists": [
        {
          "wid": "5",
          "value": "2024-10-17T10:30:04.482Z"
        }
      ]
    }
  ],
  "facets": {},
  "highlights": [
    {
      "name": "PREPREPREA92ACA8CE49D71D26B5853D0442A7473POSTPOSTPOST",
      "ids": [
        "A92ACA8CE49D71D26B5853D0442A7473"
      ]
    }
  ],
  "elapsed": 0.01130533218383789,
  "start": 0,
  "total_results": 1,
  "terms": [
    "A92ACA8CE49D71D26B5853D0442A7473"
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

> Mappings are based on each of the items within the `.results[]` JSON path.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.md5	Related Indicator	MD5	.server_added_timestamp	A92ACA8CE49D71D26B5853D0442A7473	N/A
.observed_filename	Related Indicator	File Path	.server_added_timestamp	/usr/lib/x86_64-linux-gnu/ld-linux-x86-64.so.2	N/A
.sha256	Related Indicator	SHA-256	.server_added_timestamp	1ff597e8bd590896c17d856188d1f0950a5a4cf4e7d2c0b40a6c1eb95c9586b3	N/A
.os_type	Indicator Attribute	Operating System	.server_added_timestamp	Linux	User-configurable
.host_count	Indicator Attribute	Hosts Count	.server_added_timestamp	1	User-configurable. Updatable
.alliance_score_virustotal	Indicator Attribute	Virustotal Score	.server_added_timestamp	20	User-configurable. Updatable
.digsig_publisher	Indicator Attribute	Signature Publisher	.server_added_timestamp	Digi	User-configurable
.digsig_issuer	Indicator Attribute	Signature Issuer	.server_added_timestamp	DigiCert	User-configurable
.digsig_result	Indicator Attribute	Signed Status	.server_added_timestamp	Unsigned	User-configurable
.company_name	Indicator Attribute	Company	.server_added_timestamp	Windows	User-configurable
.product_name	Indicator Attribute	Product Name	.server_added_timestamp	Microsoft Office Word	User-configurable
.product_version	Indicator Attribute	Product Version	.server_added_timestamp	6.3.9200	User-configurable
.is_executable_image	Indicator Attribute	Is Executable	.server_added_timestamp	True	User-configurable. Updatable
.orig_mod_len	Indicator Attribute	File Size	.server_added_timestamp	122480	User-configurable. Updatable

Alert Enrichment

The Alert Enrichment action queries data regarding alerts saved in VMWare Carbon Black EDR. This search is the same as the one performed in UI on the Triage Alerts page. The default query contains only the input value of the indicator/asset. The user field `Additional Search Query` allows additional query criteria. It accepts the same data as the search box on the Triage Alerts page (e.g status:Unresolved).

More information can be found at: https://developer.carbonblack.com/resources/query_overview.pdf.

`GET "{{CARBON_BLACK_EDR_INSTANCE}}/api/v2/alert"`

Query Parameters:

```
{
   "q": "f34217144e41c2a0ea56df7056f0b4d7 and (status:Unresolved)"
}
```

Sample Response:


```
{
  "results": [
    {
      "unique_id": "665d5e3c-08e2-4d3e-b39e-332939235ba5",
      "created_time": "2024-10-17T13:20:05.650Z",
      "alert_type": "watchlist.hit.query.process",
      "status": "Unresolved",
      "sensor_criticality": 3.0,
      "feed_rating": 3.0,
      "ioc_confidence": 0.5,
      "report_score": 75,
      "os_type": "linux",
      "username": "root",
      "process_name": "php",
      "process_path": "/usr/local/bin/php",
      "modload_count": 0,
      "filemod_count": 5,
      "regmod_count": 0,
      "netconn_count": 4,
      "childproc_count": 10,
      "crossproc_count": 0,
      "fileless_scriptload_count": 0,
      "md5": "73A444BE513D5FB25D9A78F2C8B5A9CB",
      "sha256": "(unknown)",
      "process_unique_id": "00000005-001d-8bc0-01db-207fa9066037-01929a084d71",
      "feed_name": "My Watchlists",
      "feed_id": -1,
      "watchlist_name": "PHP",
      "watchlist_id": "10",
      "ioc_type": "query",
      "ioc_attr": "{\"highlights\":[\"/usr/local/binPREPREPRE/
```

```
phPOSTPOSTPOSTp\",\"PREPREPREphpPOSTPOSTPOST /var/www/api/artisan.php
threatq:delete-cascade\",\"PREPREPREphpPOSTPOSTPOST\"]}",
      "process_id": "00000005-001d-8bc0-01db-207fa9066037",
      "segment_id": 1729161088369,
      "hostname": "int-7535",
      "group": "int_7535",
      "sensor_id": 5,
      "comms_ip": "10.113.2.226",
      "interface_ip": "10.113.2.226",
      "alert_severity": 50.625,
      "_version_": 1813167426300280832,
      "total_hosts": 1
    }
  ],
  "facets": {},
  "filtered": {},
  "highlights": [],
  "elapsed": 0.011178016662597656,
  "start": 0,
  "total_results": 1,
  "terms": [
    "int-7535",
    "73A444BE513D5FB25D9A78F2C8B5A9CB"
  ],
  "all_segments": true,
  "comprehensive_search": true,
  "incomplete_results": false
}
```

ThreatQuotient provides the following default mapping for this action:

> Mappings are based on each of the items within the `.results[]` JSON path.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.md5	Related Indicator	MD5	.created_time	73A444BE513D5FB25D9A78F2C8B5A9CB	User-configurable
.process_path	Related Indicator	File Path	.created_time	/usr/local/bin/php	User-configurable
.username	Related Indicator	Username	.created_time	root	User-configurable
.observed_filename	Related Indicator	File Path	.created_time	N/A	User-configurable
.hostname	Related Asset	N/A	.created_time	int-7535	User-configurable
.process_name .md5	Event Title	Alert	.created_time	Carbon Black EDR: php	`.md5` is used if `process_name` is missing
.process_name	Event Attribute	Process Name	.created_time	php	User-configurable
.modload_count	Event Attribute	Modloads	.created_time	4	User-configurable. Updatable
.regmod_count	Event Attribute	Regmods	.created_time	1	User-configurable. Updatable
.filemod_count	Event Attribute	Filemods	.created_time	3	User-configurable. Updatable
.netconn_count	Event Attribute	Netconns	.created_time	2	User-configurable. Updatable
.childproc_count	Event Attribute	Children	.created_time	5	User-configurable. Updatable
.fileless_scriptload_count	Event Attribute	Fileless Scriptloads	.created_time	6	User-configurable. Updatable
.os_type	Event Attribute	Operating System	.created_time	Linux	User-configurable
.alert_type	Event Attribute	Alert Type	.created_time	Watchlist hit query process	User-configurable. Title cased and `.` is replace with
.sensor_criticality	Event Attribute	Criticality	.created_time	3.0	User-configurable. Updatable
.feed_rating	Event Attribute	Feed Rating	.created_time	3.0	User-configurable. Updatable
.ioc_confidence	Event Attribute	IoC Confidence	.created_time	0.5	User-configurable. Updatable
.report_score	Event Attribute	Report Score	.created_time	75	User-configurable. Updatable
.alert_severity	Event Attribute	Severity	.created_time	50.625	User-configurable. Updatable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.total_hosts	Event Attribute	Hosts Count	.created_time	1	User-configurable. Updatable
.status	Event Attribute	Status	.created_time	Unresolved	Updatable
.digsig_result	Event Attribute	Signed Status	.created_time	N/A	User-configurable

Use Case Example

- **Process Enrichment**
  1. A Threat Analyst identifies a collection of indicators of type MD5 they would like to search in VMWare Carbon Black EDR.
  2. The Threat Analyst adds the VMware Carbon Black EDR On Premise - Process Enrichment Action to a Workflow.
  3. The Threat Analyst configures the action with the desired parameters, and enables the Workflow.
  4. The Workflow executes all Actions in the graph, including VMware Carbon Black EDR On Premise - Process Enrichment.
  5. The action returns the indicators enriched with information found in VMware Carbon Black EDR.
- **Binary Enrichment**
  1. A Threat Analyst identifies a collection of indicators of type MD5 they would like to search in VMWare Carbon Black EDR.
  2. The Threat Analyst adds the VMware Carbon Black EDR On Premise - Binary Enrichment Action to a Workflow.
  3. The Threat Analyst configures the action with the desired parameters, and enables the Workflow.
  4. The Workflow executes all Actions in the graph, including VMware Carbon Black EDR On Premise - Binary Enrichment.
  5. The action returns the indicators enriched with information found in VMware Carbon Black EDR.
- **Alert Enrichment**
  1. A Threat Analyst identifies a collection of indicators of type MD5 they would like to search in VMWare Carbon Black EDR.
  2. The Threat Analyst adds the VMware Carbon Black EDR On Premise - Alert Enrichment Action to a Workflow.
  3. The Threat Analyst configures the action with the desired parameters, and enables the Workflow.
  4. The Workflow executes all Actions in the graph, including VMware Carbon Black EDR On Premise - Alert Enrichment.
  5. The action returns the alerts where the indicators appear within VMware Carbon Black EDR.

Change Log

- **Version 1.0.0**
  - Initial release