ThreatQuotient

VMware Carbon Black EDR Action Bundle

Version 1.1.0

March 04, 2025

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	1.1.0
Compatible with ThreatQ Versions	>= 5.12.1
ThreatQ TQO License Required	Yes
Third-Party Deployment Method	Online
Support Tier	ThreatQ Supported

Introduction

VMware Carbon Black EDR is an incident response and threat hunting solution designed for Security Operations Center teams with offline environment requirements. VMware Carbon Black EDR continuously records and stores endpoint activity data so security professionals can hunt threats in real time and visualize the complete attack kill chain, using the VMware Carbon Black Cloud's aggregated threat intelligence.

The VMware Carbon Black EDR Action Bundle installs the following actions:

- **VMware Carbon Black EDR - File Hash Enrichment** - submits indicators to VMware Carbon Black EDR to be enriched with related threat intelligence.
- **VMware Carbon Black EDR - Export Indicators** - exports indicators to the VMware Carbon Black EDR platform.
- **VMware Carbon Black EDR - Override Reputation** - overrides the reputation for banned applications using a SHA-256 hash or path to a known IT tool application.

The actions are compatible with following indicator types:

- MD5 (File Hash Enrichment and Export Indicators actions)
- SHA-256 (Override Reputation action)
- Filename (Override Reputation action)
- File Path (Override Reputation action)

The File Hash Enrichment action returns the following enriched system objects:

- Indicators
- Exploit Target
  - Exploit Target Attributes
- Events
  - Event Attributes

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

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing the following indicator types:
  - MD5 (File Hash Enrichment and Export Indicators actions)
  - SHA-256 (Override Reputation action)
  - Filename (Override Reputation action)
  - File Path (Override Reputation action)
- The **Override Reputation** action requires CREATE, READ, and DELETE `org.reputation` permissions. You will need to create a "Custom" access level that includes each category.

  > ⚠ This should be done prior to creating a VMware Carbon Black EDR API ID and Secret Key.

  See the following for additional information - https://developer.carbonblack.com/reference/carbon-black-cloud/platform/latest/reputation-override-api/#configure-reputation-override.
- A VMware Carbon Black Organization Key.
- A VMWare Carbon Black EDR API ID.
- A VMWare Carbon Black EDR API Secret Key.

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 bundle zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the 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 individual actions to install, when prompted, and then click **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.

7. The action(s) will be added to the integrations page. 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:

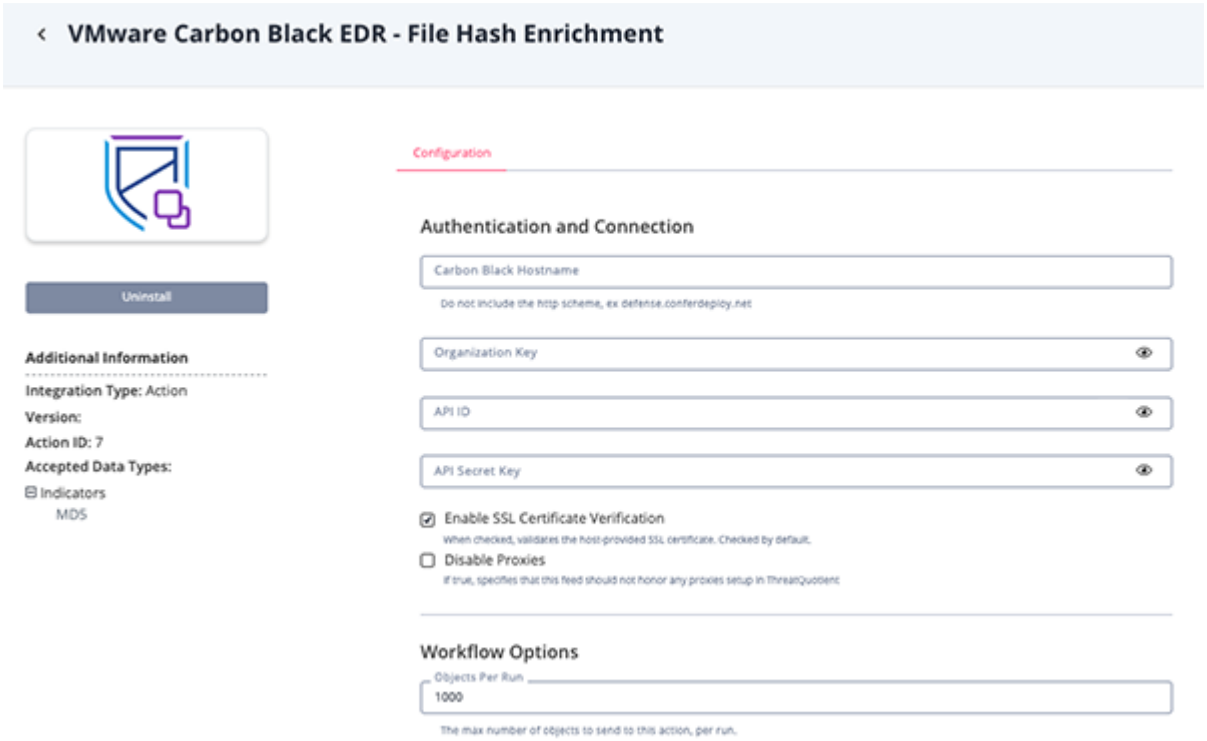
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> 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.

File Hash Enrichment

PARAMETER	DESCRIPTION
Carbon Black Hostname	Your VMWare Carbon Black EDR hostname.
Organization key	Your Organization key which can be found in the API Access section of Account Settings on your EDR instance.
API ID	Your API ID which can be found in the API Access section of Account Settings on your EDR instance.
API Secret Key	Your API Secret which can be found in the API Access section of Account Settings on your EDR instance.
Enable SSL Certificate Verification	Enable this for the action to validate the host-provided SSL certificate.

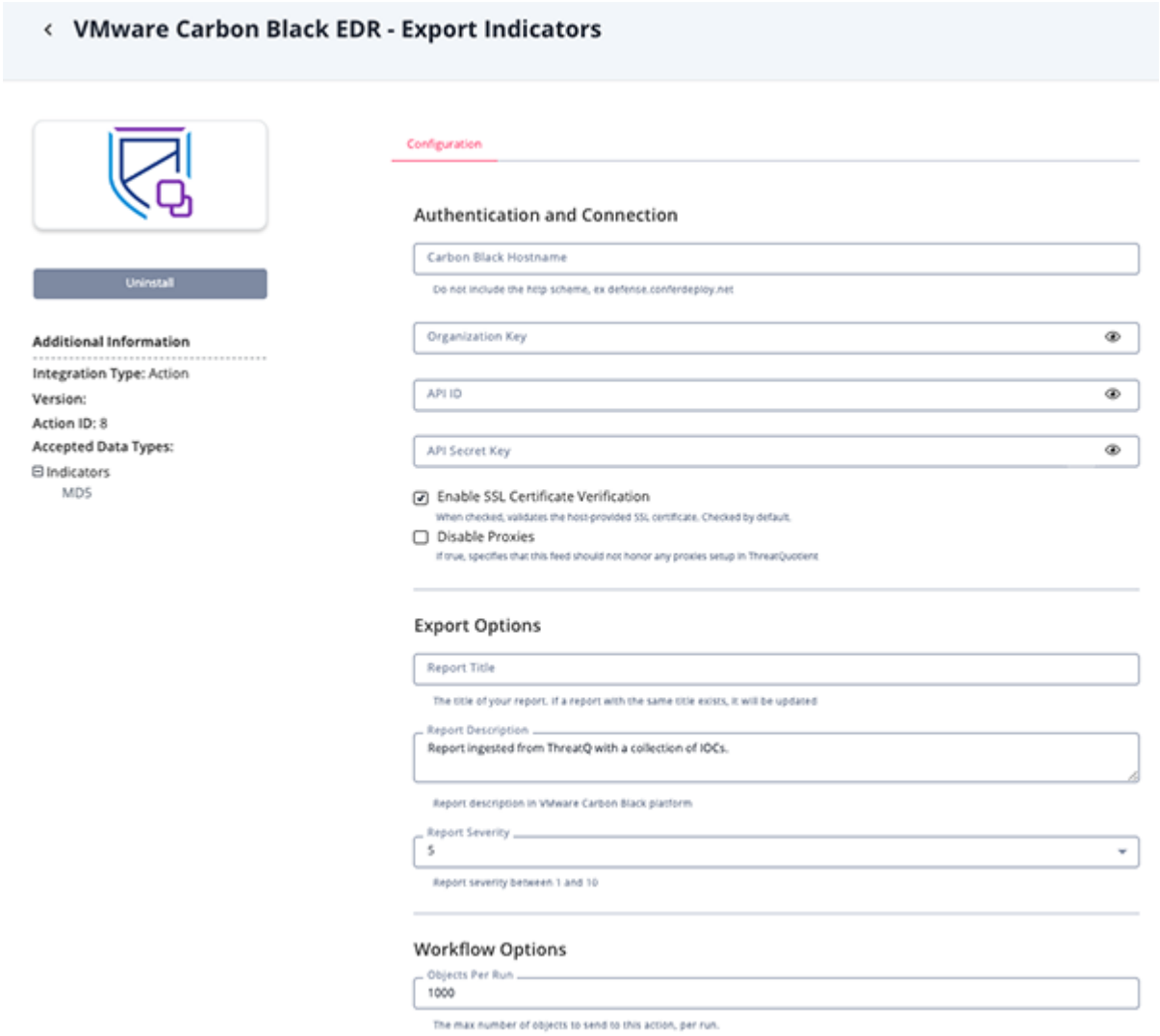
PARAMETER	DESCRIPTION
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Objects Per Run	The max number of objects per run.



Export Indicators

PARAMETER	DESCRIPTION
Carbon Black Hostname	Your VMWare Carbon Black EDR hostname.
Organization key	Your Organization key which can be found in the API Access section of Account Settings on your EDR instance.
API ID	Your API ID which can be found in the API Access section of Account Settings on your EDR instance.

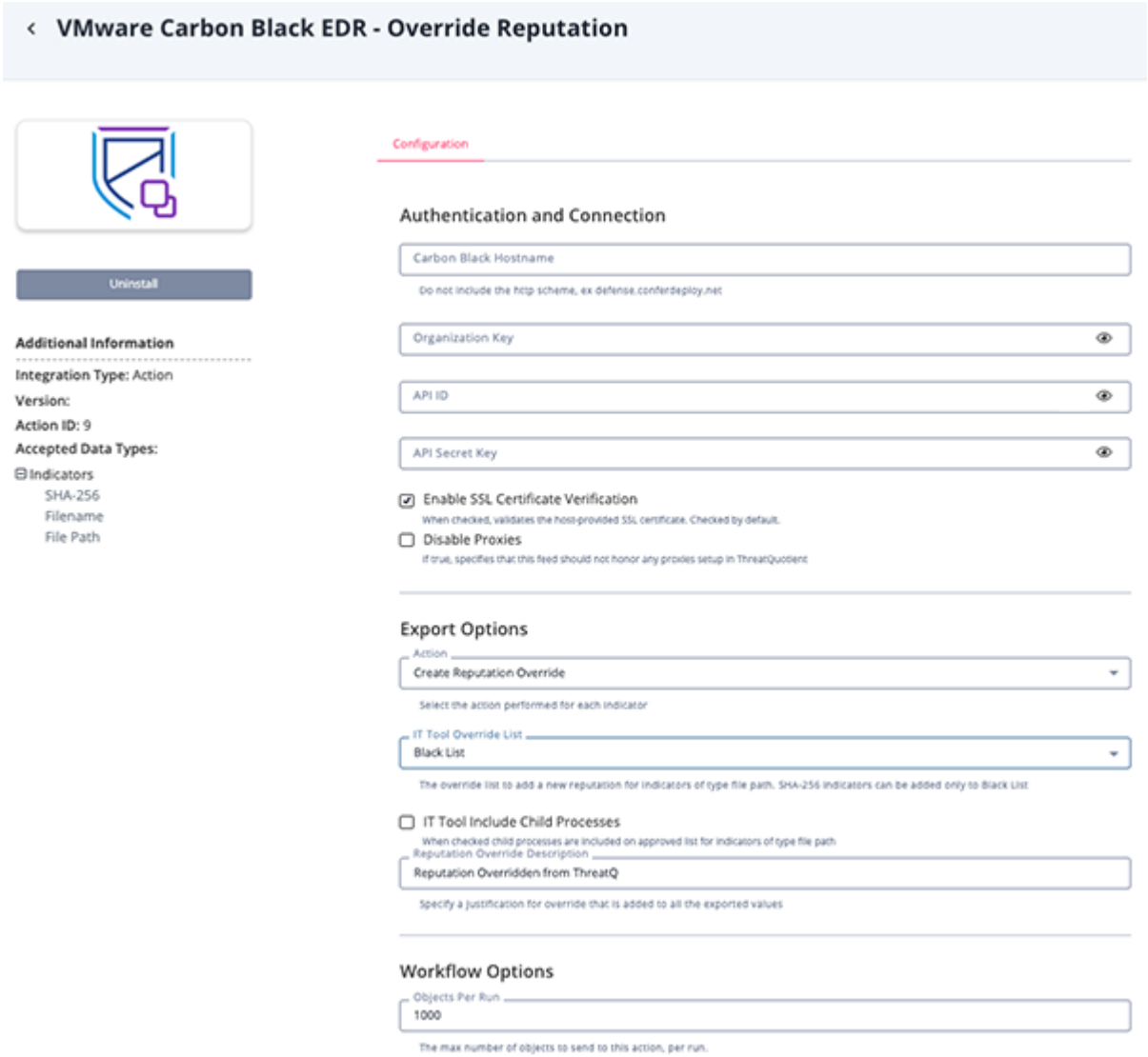
PARAMETER	DESCRIPTION
API Secret Key	Your API Secret which can be found in the API Access section of Account Settings on your EDR instance.
Enable SSL Certificate Verification	Enable this for the action to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Report Title	Enter a report title.
Report Description	Enter a report description.
Report Severity	Enter the report severity ranging from 1 to 10. The default selection is 5.
Objects Per Run	The max number of objects per run. The Export Indicators action can only send 1,000 objects per run.



Override Reputation

PARAMETER	DESCRIPTION
Carbon Black Hostname	Your VMWare Carbon Black EDR hostname.
Organization key	Your Organization key which can be found in the API Access section of Account Settings on your EDR instance.
API ID	Your API ID which can be found in the API Access section of Account Settings on your EDR instance.

PARAMETER	DESCRIPTION
API Secret Key	Your API Secret which can be found in the API Access section of Account Settings on your EDR instance.
Action	Select the action to perform for each indicator. Options include: ◦ Create Reputation Override *(default)* ◦ Delete Reputation Override
IT Tool Override List	Select the list to add a new reputation for File Path type indicators. Options include: ◦ Black List *(default)* ◦ White List SHA-256 type indicators can only be added to Black List.
IT Tool Include Child Processes	Enable this parameter child to include child processes on approved list for File Path type indicators.
Reputation Override Description	Enter a justification for that override that will be added to all the exported values.
Enable SSL Certificate Verification	Enable this for the action to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Objects Per Run	The max number of objects per run.



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

Actions

The bundle provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
VMware Carbon Black EDR - File Hash Enrichment	Submits indicators to VMware Carbon Black EDR to be enriched with related threat intelligence	Indicator	MD5
VMware Carbon Black EDR - Export Indicators	Exports indicators to VMware Carbon Black EDR platform.	Indicator	MD5
VMware Carbon Black EDR - Override Reputation	Override the reputation for banned applications using a SHA-256 hash or path to a known IT tool application.	Indicator	SHA-256, File Path, Filename

VMware Carbon Black EDR - File Hash Enrichment

The File Hash Enrichment action enriches the selected collection of indicators.

`GET https://defense.conferdeploy.net/api/investigate/v2/orgs/{{org_key}}/enriched_events/search_jobs/{{job_id}}/results`

Sample Response:


```
{
    "results": [
        {
            "backend_timestamp": "2022-05-19T03:27:57.960Z",
            "device_group_id": 0,
            "device_id": 5528062,
            "device_name": "gruyere\\t561-w10ltsb",
            "device_policy_id": 6525,
            "device_timestamp": "2022-05-19T03:26:18.645Z",
            "enriched": true,
            "enriched_event_type": "SYSTEM_API_CALL",
            "event_description": "The application \"<share><link
hash=\"ba4038fd20e474c047be8aad5bfacdb1bfc1ddbe12f803f473b7918d8d819436\">c:\
\windows\\system32\\windowspowershell\\v1.0\\powershell.exe</link></share>\"
attempted to find \"c:\\windows\\system32\\Write-Host\"*\", by calling the
function \"FindFirstFile\". The operation failed.",
            "event_id": "9664fa89d72311ec8b4cb3a8fccf7da2",
            "event_type": "crossproc",
            "ingress_time": 1652930850877,
            "legacy": true,
            "org_id": "7DESJ9GN",
            "parent_guid":
"7DESJ9GN-005459fe-00001240-00000000-1d86b30222266b3",
            "parent_pid": 4672,
            "process_guid":
"7DESJ9GN-005459fe-00000c78-00000000-1d86b30313f2923",
            "process_hash": [
                "097ce5761c89434367598b34fe32893b",

"ba4038fd20e474c047be8aad5bfacdb1bfc1ddbe12f803f473b7918d8d819436"
            ],
            "process_name": "c:\\windows\\system32\\windowspowershell\\v1.0\
\powershell.exe",
            "process_pid": [
                3192
            ],
            "process_username": [
                "NT AUTHORITY\\SYSTEM"
            ]
        }
    ]
```

```
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.results[].device_name	Exploit_target.value	Exploit Target Value	N/A	gruyere\t561-w10ltsb	N/A
.results[].device_id	Exploit_target.attribute	Device Id	N/A	5528062	N/A
.results[].device_policy_id	Exploit_target.attribute	Device Policy Id	N/A	6525	N/A
.results[].process_name	Event.title	Event Title	N/A	c:\windows\system32\windows powershell\v1.0\powershell.exe	N/A
.results[].event_description	Event.description	Event Description	N/A	The application ...	N/A
.results[].event_id	Event.hash	Event Id	N/A	9664fa89d72311ec8b4cb3a8fccf7da2	N/A
.results[].event_type	Event.type	Event Type	N/A	crossproc	N/A
.results[].ingress_time	Event.happened_at	Event Happened At	N/A	1652930850877	N/A
.results[].enriched	Event.attribute	Enriched	N/A	true	N/A
.results[].enriched_event_type	Event.attribute	Enriched Event Type	N/A	SYSTEM_API_CALL	N/A
.results[].legacy	Event.attribute	Legacy	N/A	true	N/A
.results[].parent_pid	Event.attribute	Parent Pid	N/A	4672	N/A
.results[].process_pid	Event.attribute	Process Pid	N/A	3192	N/A
.results[].process_username	Event.attribute	Process Username	N/A	NT AUTHORITY\SYSTEM	N/A

VMware Carbon Black EDR - Export Indicators

The Export Indicators action exports a collection of indicators. It first searches for a report with the given name on the VMware Carbon Black platform. If a report is found, it then updates the report's information and IOCs with the collection. If no report is found, it will create a new report with the information provided and the threat collection.

> ⚠ Only 1,000 IOCs can be exported at a time.

- `GET https://{{user_fields.hostname}}/threathunter/feedsearch/v1/orgs/{{user_fields.org_key}}/search`
- `POST https://{{user_fields.hostname}}/threathunter/watchlistmgr/v3/orgs/{{user_fields.org_key}}/reports`
- `PUT https://{{user_fields.hostname}}/threathunter/watchlistmgr/v3/orgs/{{user_fields.org_key}}/reports/{{run_params.report_id}}`

VMware Carbon Black EDR - Override Reputation

The Override Reputation action creates a new reputation override for indicators of type SHA-256, Filename and File Path.

The indicators of type File Path and Filename must contain valid paths to applications. Filename is included because sometimes it is populated with valid paths. If an indicator already has a reputation override, then its properties are updated.

The action is also able to delete a reputation override if it already exists.

> The API allows adding SHA-256 only to Black List. File paths can be added to Black List or White List.

`POST https://{{user_fields.hostname}}/appservices/v6/orgs/{{user_fields.org_key}}/reputations/overrides`

Sample Request Body:

```
{
  "override_list": "BLACK_LIST",
  "override_type": "SHA256",
  "sha256_hash":
"4b322cd349f647ab5f84766cb2f2176bac77f0b8d64c2a59b91a6d30c4072315"
}
```

Sample Response:

```
{
  "id": "5391cdcff5d811efaf2eb11d241b9f6d",
  "created_by": "NG4IXXXXXX",
  "create_time": "2025-02-28T13:31:33.558Z",
  "override_list": "BLACK_LIST",
  "override_type": "SHA256",
  "description": "ThreatQ integration",
  "source": "APP",
  "source_ref": null,
  "sha256_hash":
"4b322cd349f647ab5f84766cb2f2176bac77f0b8d64c2a59b91a6d30c4072315",
  "filename": null
}
```

Request to Create/Update Filename/File Path Reputation

The following details a request to create or update the reputation of a Filename or File Path type indicator.

```
POST https://{{user_fields.hostname}}/appservices/v6/orgs/
{{user_fields.org_key}}/reputations/overrides
```

Sample Request Body:

```
{
  "override_list": "WHITE_LIST",
  "override_type": "IT_TOOL",
  "path": "/var/logtemo",
  "include_child_processes": false
}
```

Sample Response:

```
{
    "id": "35b9a9aef5cf11efb9b96f9c5168538a",
    "created_by": "NG4IXXXXXX",
    "create_time": "2025-02-28T12:26:18.017Z",
    "override_list": "WHITE_LIST",
    "override_type": "IT_TOOL",
    "description": "Threatq integration",
    "source": "APP",
    "source_ref": null,
    "path": "/var/logtemo",
    "include_child_processes": false
}
```

Request to Search for Existing Reputation

The following details a request to search for an existing reputation.

```
POST https://{{user_fields.hostname}}/appservices/v6/orgs/
{{user_fields.org_key}}/reputations/overrides/_search
```

Sample Request Body:

```
{
  "query": "4b322cd349f647ab5f84766cb2f2176bac77f0b8d64c2a59b91a6d30c4072315"
}
```

Sample Response:

```
{
  "results": [
    {
      "id": "5391cdcff5d811efaf2eb11d241b9f6d",
      "created_by": "NG4IXXXXXX",
      "create_time": "2025-02-28T13:31:33.558Z",
```

```
      "override_list": "BLACK_LIST",
      "override_type": "SHA256",
      "description": "ThreatQ integration",
      "source": "APP",
      "source_ref": null,
      "sha256_hash":
"4b322cd349f647ab5f84766cb2f2176bac77f0b8d64c2a59b91a6d30c4072315",
      "filename": null
    }
  ]
}
```

Request to Delete Existing Reputation

The following endpoint is used to delete an existing reputation.

```
DELETE https://{{user_fields.hostname}}/appservices/v6/orgs/
{{user_fields.org_key}}/reputations/overrides/{reputation_id}
```

Enriched Data

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

VMware Carbon Black EDR - File Hash Enrichment

METRIC	RESULT
Run Time	1 minute
Exploit Target	7
Exploit Target Attributes	15
Events	189
Event Attributes	1,344
Indicators	1

Known Issues / Limitations

- **VMware Carbon Black EDR - Export Indicators Action** - Only 1,000 IOCs can be exported at a time.

Change Log

- **Version 1.1.0**
  - Added the following configuration parameters to all actions:
    - **Enable SSL Certificate Verification** - enable or disable verification of the server's SSL certificate.
    - **Disable Proxies** - determine if the action should honor proxy settings set in the ThreatQ UI.
  - Added a new action:
    - **VMware Carbon Black EDR - Override Reputation** - override the reputation for banned applications using a SHA-256 hash or path to a known IT tool application.
- **Version 1.0.0 rev-a**
  - Guide Update - updated introduction chapter.
- **Version 1.0.0**
  - Initial release