ThreatQuotient

IBM QRadar SOAR Action

Version 1.0.0

January 28, 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 **3**
Support **4**
Integration Details **5**
Introduction **6**
Prerequisites **7**
Installation **8**
Configuration **9**
Actions **12**
IBM QRadar SOAR - Update Events 13
Get ORG ID 13
Get Incident ID 15
Get/Add/Update/Delete Comment 20
Get All Indicators, Add a New Indicator 21
Update Custom Attributes/Objects 23
Known Issues / Limitations **24**
Change Log **25**

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	>= 6.5.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The IBM QRadar SOAR action allows updating events from ThreatQ to your Resilient instance. It has the ability to push new indicators and comments from updated Resilient events in ThreatQ to Resilient as artifacts and comments, respectively.

The integration provides the following action:

- **IBM QRadar SOAR - Update Events** - pushes indicators and comments from updated Resilient events in ThreatQ to Resilient.

The action is compatible with event object types.

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

Prerequisites

- An IBM QRadar SOAR instance.
- A username and password for the IBM QRadar SOAR instance.
- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing the event object type.

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

> 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.

You will still need to configure the action.

Configuration

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

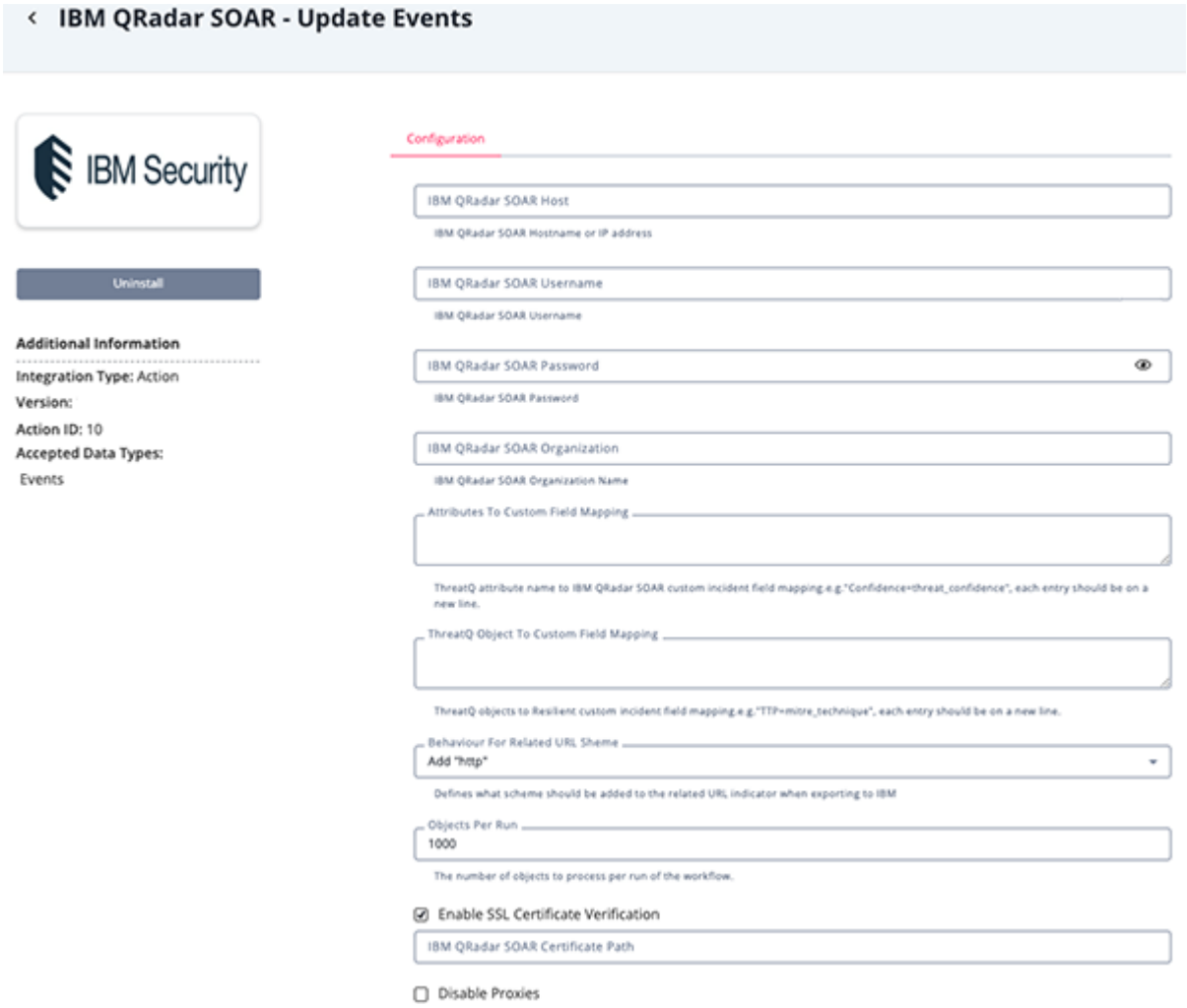
To configure the integration:

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.

PARAMETER	DESCRIPTION
IBM QRadar SOAR Host	Enter your IBM QRadar SOAR Hostname or IP Address.
IBM QRadar SOAR Username	Enter your IBM QRadar SOAR Username.
IBM QRadar SOAR Password	Enter your IBM QRadar SOAR Password.
IBM QRadar SOAR Organization	Enter your IBM QRadar SOAR Organization Name.
Attributes to Custom Field Mapping	Enter the ThreatQ attribute name to IBM QRadar SOAR custom incident field mapping. Each entry should be on its own line. **Example:** Confidence=threat_confidence

PARAMETER	DESCRIPTION
ThreatQ Object To Custom Field Mapping	Enter the ThreatQ objects to Resilient custom incident field mapping. Each entry should be on its own line. **Example:** TTP=mitre_technique Supported ThreatQ objects types are: ◦ Adversary ◦ Assets ◦ Attack Pattern ◦ Campaign ◦ Course of Action ◦ Events ◦ Exploit Target ◦ Files ◦ Identity ◦ Incident ◦ Indicators ◦ Intrusion Set ◦ Malware ◦ Notes ◦ Report ◦ Signatures ◦ Tasks ◦ Tool ◦ TTP ◦ Vulnerability
Behaviour for related URL scheme	Define what scheme should be added to the related URL indicator when exporting to IBM. Options include: ◦ Add "http" ◦ Add "https"
Enable SSL Certificate Verification	Enable this for the action to validate the host-provided SSL certificate.
IBM QRadar SOAR Certificate Path	Enter the path to your IBM QRadar SOAR certificate.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.



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

Actions

The following action is available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
IBM QRadar SOAR - Update Events	Pushes indicators and comments from updated Resilient events in ThreatQ to Resilient	Events	Incidents

IBM QRadar SOAR - Update Events

The IBM QRadar SOAR - Update Events action pushes indicators and comments from updated Resilient events in ThreatQ to Resilient

Get ORG ID

The Get ORG ID retrieves the ORG ID in order to fetch the incidents.

`POST https://{host}/rest/session`

Sample Response:


```
{
    "orgs": [
        {
            "id": 201,
            "name": "Organization_X",
            "addr": null,
            "addr2": null,
            "city": null,
            "state": null,
            "zip": null,
            "attachments_enabled": true,
            "final_phase_required": false,
            "tasks_private": false,
            "has_saml": false,
            "require_saml": false,
            "twofactor_auth_domain": null,
            "has_available_twofactor": false,
            "authorized_ldap_group": null,
            "supports_ldap": false,
            "incident_deletion_allowed": true,
            "configuration_type": "standard",
            "parent_org": null,
            "session_timeout": 1200,
            "last_modified_by": {
                "id": 1,
                "type": "user",
                "name": "test@threatq.com",
                "display_name": "User Test"
            },
            "last_modified_time": 1726070182493,
            "uuid": "692649b6-f8e6-449e-ad93-8dbecae7bd4f",
            "timezone": null,
            "cloud_account": null,
            "perms": {
                "master_administrator": true,
                "administrator": true,
                "observer": false,
```

```
            "create_incs": true,
            "create_shared_layout": true
        },
        "effective_permissions": [
            139,
            140
        ],
        "role_handles": [
            1003,
            1002,
            1001
        ],
        "instance_roles": [
            {
                "role_handles": [
                    1003,
                    1002,
                    1001
                ],
                "effective_permissions": [
                    105,
                    104
                ],
                "typed_object": {
                    "parent": null,
                    "object_id": 201,
                    "object_name": "Organization_X",
                    "type_id": 7,
                    "type_name": "organization"
                }
            }
        ],
        "enabled": true,
        "twofactor_cookie_lifetime_secs": 0
    }
],
"password_expiration_date": 1743425721904,
"user_id": 1,
"user_fname": "User",
"user_lname": "Test",
"user_displayname": "User Test",
"user_email": "test@threatq.com",
"saml_alias": null,
"csrf_token": "60d3165ae17cad9a97401dff12ce5b50",
"session_ip": "10.10.10.10",
"next_nps_survey_date": null,
"preferred_org_id": null,
"effective_system_permissions": [],
"is_saml": false,
```

```
    "is_ldap": false
}
```

Get Incident ID

The Get Incident ID uses the ID from the ThreatQ Event Title to get the specific Incident from IBM.

`GET https://{host}/rest/orgs/{org_id}/incidents/{incident_id}`

Sample Response:

```
{
    "dtm": {},
    "cm": {
        "unassigneds": [],
        "total": 0,
        "geo_counts": {}
    },
    "regulators": {
        "ids": [
            149
        ]
    },
    "hipaa": {
        "hipaa_adverse": null,
        "hipaa_misused": null,
        "hipaa_acquired": null,
        "hipaa_additional_misuse": null,
        "hipaa_breach": null,
        "hipaa_adverse_comment": "",
        "hipaa_misused_comment": "",
        "hipaa_acquired_comment": "",
        "hipaa_additional_misuse_comment": "",
        "hipaa_breach_comment": ""
    },
    "tasks": null,
    "artifacts": null,
    "name": "TestAction",
    "description": "<div class=\"soar-rte-content\"><p>Incident Test</p></
div>",
    "phase_id": 1004,
    "inc_training": false,
    "vers": 3,
    "addr": null,
    "city": null,
    "creator": {
        "id": 1,
        "fname": "Valentin",
        "lname": "Todorov",
        "display_name": "Valentin Todorov",
        "status": "A",
```

```
        "email": "valentin@threatq.com",
        "locked": false,
        "password_changed": false,
        "is_external": false,
        "ui_theme": "verydarkmode",
        "is_ldap": false,
        "is_saml": false
    },
    "creator_principal": {
        "id": 1,
        "type": "user",
        "name": "valentin@threatq.com",
        "display_name": "Valentin Todorov"
    },
    "exposure_type_id": 1,
    "incident_type_ids": [
        16
    ],
    "reporter": null,
    "state": null,
    "country": null,
    "zip": null,
    "workspace": 1,
    "exposure": 0,
    "org_handle": 201,
    "members": [],
    "negative_pr_likely": null,
    "perms": {
        "read": true,
        "write": true,
        "comment": true,
        "assign": true,
        "close": true,
        "change_members": true,
        "attach_file": true,
        "read_attachments": true,
        "delete_attachments": true,
        "create_milestones": true,
        "list_milestones": true,
        "create_artifacts": true,
        "list_artifacts": true,
        "delete": true,
        "change_workspace": true
    },
    "confirmed": true,
    "task_changes": {
        "added": [],
        "removed": []
    },
    "assessment": "<?xml version=\"1.0\" encoding=\"UTF-8\" standalone=\"yes\"?
```

```
>\n<assessment>\n    <rollups/>\n    <optional>There are 1 required and 0
optional tasks from 1 regulators.</optional>\n</assessment>\n",
    "data_compromised": null,
    "draft": false,
    "properties": {
        "sn_snow_record_link": null,
        "sn_snow_table_name": null,
        "threatq_link": null,
        "sn_snow_record_id": null,
        "internal_customizations_field": null
    },
    "resolution_id": null,
    "resolution_summary": null,
    "pii": {
        "data_compromised": null,
        "determined_date": 1736842753000,
        "harmstatus_id": 2,
        "data_encrypted": null,
        "data_contained": null,
        "impact_likely": null,
        "ny_impact_likely": null,
        "or_impact_likely": null,
        "wa_impact_likely": null,
        "dc_impact_likely": null,
        "data_source_ids": [],
        "data_format": null,
        "assessment": "<?xml version=\"1.0\" encoding=\"UTF-8\"
standalone=\"yes\"?>\n<assessment>\n    <rollups/>\n    <optional>There are 1
required and 0 optional tasks from 1 regulators.</optional>\n</assessment>\n",
        "exposure": 0,
        "gdpr_harm_risk": null,
        "gdpr_lawful_data_processing_categories": [],
        "alberta_health_risk_assessment": null,
        "california_health_risk_assessment": null,
        "new_zealand_risk_assessment": null,
        "singapore_risk_assessment": null
    },
    "gdpr": {
        "gdpr_breach_circumstances": [],
        "gdpr_breach_type": null,
        "gdpr_personal_data": null,
        "gdpr_identification": null,
        "gdpr_consequences": null,
        "gdpr_final_assessment": null,
        "gdpr_breach_type_comment": null,
        "gdpr_personal_data_comment": null,
        "gdpr_identification_comment": null,
        "gdpr_consequences_comment": null,
        "gdpr_final_assessment_comment": null,
        "gdpr_subsequent_notification": null
    },
```

```
    "regulator_risk": {},
    "score": null,
    "inc_last_modified_date": 1736930054495,
    "comments": null,
    "actions": [],
    "playbooks": [
        {
            "playbook_handle": 90,
            "display_name": "Qualys VM: Manage Restricted IPs"
        },
        {
            "playbook_handle": 81,
            "display_name": "Qualys VM: Asset Group Add"
        },
        {
            "playbook_handle": 82,
            "display_name": "Qualys VM: Asset Group Delete"
        },
        {
            "playbook_handle": 83,
            "display_name": "Qualys VM: Asset Group List"
        },
        {
            "playbook_handle": 84,
            "display_name": "Qualys VM: Asset Tracked Address Add"
        },
        {
            "playbook_handle": 85,
            "display_name": "Qualys VM: Host - List"
        },
        {
            "playbook_handle": 86,
            "display_name": "Qualys VM: IP - List"
        },
        {
            "playbook_handle": 88,
            "display_name": "Qualys VM: List Vulnerabilities"
        },
        {
            "playbook_handle": 89,
            "display_name": "Qualys VM: List Vulnerabilities of Host"
        },
        {
            "playbook_handle": 87,
            "display_name": "Qualys VM: List Hosts With Vulnerabilities"
        },
        {
            "playbook_handle": 91,
            "display_name": "Qualys VM: Report List"
        },
```

```
        {
            "playbook_handle": 92,
            "display_name": "Qualys VM: Scan Launch"
        },
        {
            "playbook_handle": 93,
            "display_name": "Qualys VM: Scan List"
        },
        {
            "playbook_handle": 94,
            "display_name": "Qualys VM: Scan Manage"
        },
        {
            "playbook_handle": 100,
            "display_name": "SNOW: Create New Incident (PB)"
        },
        {
            "playbook_handle": 102,
            "display_name": "SNOW: Create New Security Incident (PB)"
        },
        {
            "playbook_handle": 54,
            "display_name": "ThreatQ: Export Incident"
        }
    ],
    "timer_field_summarized_incident_data": [],
    "admin_id": null,
    "creator_id": 1,
    "crimestatus_id": 5,
    "employee_involved": null,
    "end_date": null,
    "exposure_dept_id": null,
    "exposure_individual_name": null,
    "exposure_vendor_id": null,
    "jurisdiction_name": null,
    "jurisdiction_reg_id": null,
    "start_date": null,
    "inc_start": null,
    "org_id": 201,
    "is_scenario": false,
    "hard_liability": 0,
    "nist_attack_vectors": [],
    "id": 2120,
    "sequence_code": null,
    "discovered_date": 1736842753000,
    "due_date": null,
    "create_date": 1736929251055,
    "owner_id": 1,
    "severity_code": 4,
```

```
    "plan_status": "A"
}
```

Get/Add/Update/Delete Comment

Get All Comments - `GET https://{host}/rest/orgs/{org_id}/incidents/{incident_id}/comments`

Add a New Comment - `PUT https://{host}/rest/orgs/{org_id}/incidents/{incident_id}/comments`

Update a Comment - `POST https://{host}/rest/orgs/{org_id}/incidents/{incident_id}/comments/{comment_id}`

Delete a Comment - `https://{host}/rest/orgs/{org_id}/incidents/{incident_id}/comments/{comment_id}`

Sample Response:

```
{
    "type": "incident",
    "id": 134,
    "parent_id": null,
    "user_id": 1,
    "user_fname": "Valentin",
    "user_lname": "Todorov",
    "text": "<div class=\"rte\"><div>[TQ4]</div><div><p>Test comment ThreatQ</
p></div></div>",
    "create_date": 1737025949996,
    "modify_date": 1737025949996,
    "children": [],
    "mentioned_users": [],
    "is_deleted": false,
    "modify_user": {
        "id": 1,
        "first_name": "Valentin",
        "last_name": "Todorov"
    },
    "actions": [],
    "playbooks": [
        {
            "playbook_handle": 104,
            "display_name": "SNOW: Send as Additional Comment (PB)"
        },
        {
            "playbook_handle": 105,
            "display_name": "SNOW: Send as Work Note (PB)"
        }
    ],
    "inc_id": 2120,
    "inc_name": "TestAction",
    "task_id": null,
```

```
    "task_name": null,
    "task_custom": null,
    "task_members": null,
    "task_at_id": null,
    "inc_owner": 1,
    "user_name": "Valentin Todorov",
    "modify_principal": {
        "id": 1,
        "type": "user",
        "name": "valentin@threatq.com",
        "display_name": "Valentin Todorov"
    },
    "comment_perms": {
        "update": true,
        "delete": true
    }
}
```


Get All Indicators, Add a New Indicator

Get All Indicators - `GET https://{host}/rest/orgs/{org_id}/incidents/{incident_id}/artifacts`

Add a New Indicator - `POST https://{host}/rest/orgs/{org_id}/incidents/{incident_id}/artifacts`

Sample Response:


```
{
        "id": 195,
        "type": 2,
        "value": "iploc.ru",
        "description": "Added by ThreatQ in Postman",
        "attachment": null,
        "parent_id": null,
        "creator": {
            "id": 1,
            "fname": "Valentin",
            "lname": "Todorov",
            "display_name": "Valentin Todorov",
            "status": "A",
            "email": "valentin@threatq.com",
            "locked": false,
            "password_changed": false,
            "is_external": false,
            "ui_theme": "verydarkmode",
            "is_ldap": false,
            "is_saml": false
        },
        "inc_id": 2123,
        "inc_name": "ACT_TQ_Test",
```

```
        "inc_owner": 1,
        "hits": [],
        "created": 1737451402072,
        "last_modified_time": 1737451402080,
        "last_modified_by": {
            "id": 1,
            "type": "user",
            "name": "valentin@threatq.com",
            "display_name": "Valentin Todorov"
        },
        "pending_sources": [],
        "perms": {
            "read": true,
            "write": true,
            "delete": true
        },
        "properties": null,
        "actions": [],
        "playbooks": [
            {
                "playbook_handle": 71,
                "display_name": "ThreatQ: Add Tags to Artifact"
            },
            {
                "playbook_handle": 79,
                "display_name": "ThreatQ: Find Related Malware (Example)"
            },
            {
                "playbook_handle": 75,
                "display_name": "ThreatQ: Export Artifact"
            },
            {
                "playbook_handle": 70,
                "display_name": "ThreatQ: Add Attribute to Artifact"
            },
            {
                "playbook_handle": 77,
                "display_name": "ThreatQ: Find Artifact Hits"
            },
            {
                "playbook_handle": 78,
                "display_name": "ThreatQ: Find Related Artifacts"
            },
            {
                "playbook_handle": 80,
                "display_name": "ThreatQ: Set Artifact Status"
            }
        ],
        "hash":
"e7231d43f070a6ca63fb6ca99be71ac10eebdb849f13ba1504be7921ebb10570",
```

```
        "relating": true,
        "creator_principal": {
            "id": 1,
            "type": "user",
            "name": "valentin@threatq.com",
            "display_name": "Valentin Todorov"
        },
        "related_incident_count": null,
        "pending_scan_result": false,
        "global_info": null,
        "ip": {
            "source": null,
            "destination": null
        },
        "global_artifact": []
    }
```


Update Custom Attributes/Objects

`PATCH https://{host}/rest/orgs/{org_id}/incidents/{incident_id}`

Sample Request:

```
{
    "changes":[
        {
            "field": {"name":"threatq_link"},
            "old_value": {},
            "new_value": {
                        "text": "new_val"
                    }
        }
    ]
}
```

Sample Response:

```
{
    "success": true,
    "title": null,
    "message": null,
    "hints": []
}
```

Known Issues / Limitations

- The **ThreatQ Object to Custom Field Mapping** configuration field supports the following ThreatQ object types:
  - Adversary
  - Assets
  - Attack Pattern
  - Campaign
  - Course of Action
  - Events
  - Exploit Target
  - Files
  - Identity
  - Incident
  - Indicators
  - Intrusion Set
  - Malware
  - Notes
  - Report
  - Signatures
  - Tasks
  - Tool
  - TTP
  - Vulnerability

Change Log

- **Version 1.0.0**
  - Initial release