ThreatQuotient

A Securonix Company

Recorded Future Action Bundle

Version 1.5.0

April 21, 2026

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: tq-support@securonix.com
Web: https://ts.securonix.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: tq-support@securonix.com
Support Web: https://ts.securonix.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	1.5.0
Compatible with ThreatQ Versions	>= 5.19.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Recorded Future Action Bundle enables seamless enrichment of ThreatQ objects by leveraging Recorded Future's intelligence platform. By submitting supported object types from a Data Collection, the bundle retrieves risk scores, rule-based context, and related threat intelligence including indicators, malware, adversaries, and vulnerabilities, enhancing visibility and supporting more informed analysis and decision-making.

The integration provides the following actions:

- **Recorded Future** - retrieves the risk score of an Ip address, domain or URL, hash, vulnerability.
- **Recorded Future Vulnerabilities** - retrieves the rules and values of the provided IP address, domain, URL, hash, vulnerability which tells how critical the object is.
- **Recorded Future - GeoIP Lookup** - retrieves the geographical location and proxy information of the provided IP address.
- **Recorded Future - Find Entity Links** - resolves a Recorded Future entity and ingests related malware, adversaries.

The actions are compatible with the following object types:

- Adversaries
- Indicators
    - MD5
    - SHA-1
    - SHA-256
    - SHA-512
    - IP Address
    - Domain
    - CVE
    - URL
- Malware
- Vulnerabilities

The action returns the following enriched data:

- Adversaries
- Indicators

    - Indicator Attributes
    - Indicator Tags
- Malware
- Vulnerabilities

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.
- Recorded Future API key.
- A data collection containing at least one of the following object types:
  - Adversaries
  - Indicators
    - MD5
    - SHA-1
    - SHA-256
    - SHA-512
    - IP Address
    - Domain
    - CVE
    - URL
  - Malware
  - Vulnerabilities

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 action(s) to 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.

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:

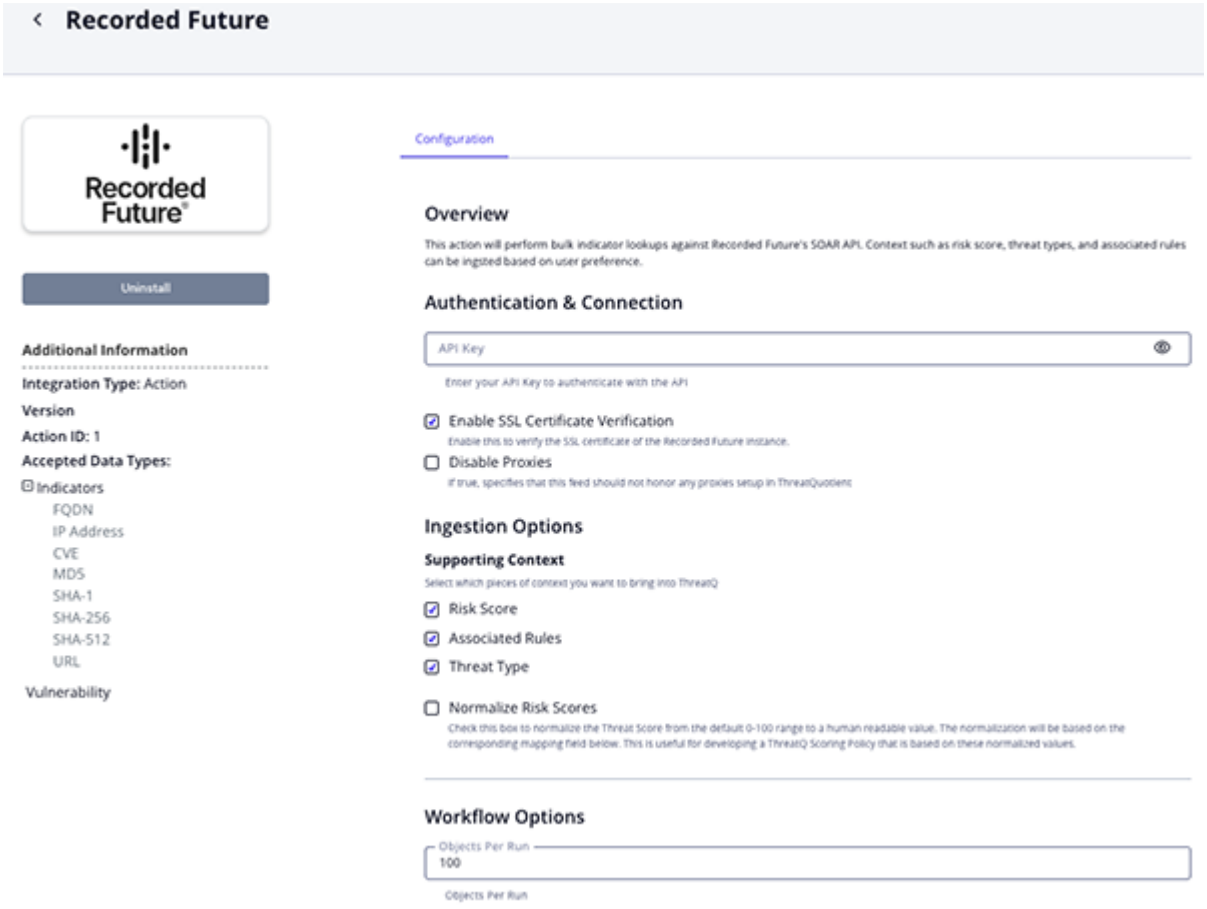
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

   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.

Recorded Future Parameters

PARAMETER	DESCRIPTION
API Key	Your Recorded Future API Key.
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.
Supporting Context	Select the context for the action to return. Options include: ◦ Risk Score ◦ Associated Rules

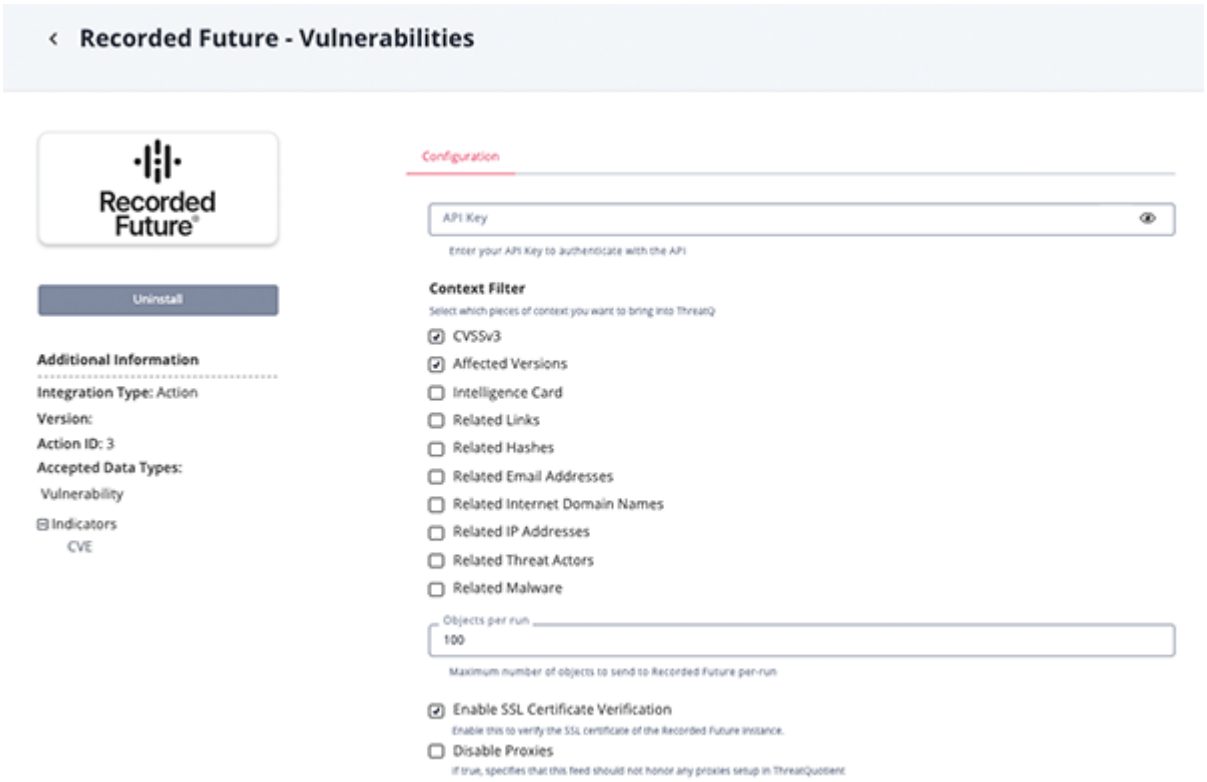
PARAMETER	DESCRIPTION
	◦ Threat Type
Normalize Risk Scores	Configure a mapping to normalize numeric threat score values to the scorable attribute, Normalized Threat Score. The raw Threat Score value will always be ingested. This mapping must be defined as a pipe-separated, CSV-formatted string with the following columns: Minimum, Maximum, and Normalized Value.
Objects Per Run	The number of object to return with each run.



Recorded Future - Vulnerabilities Parameters

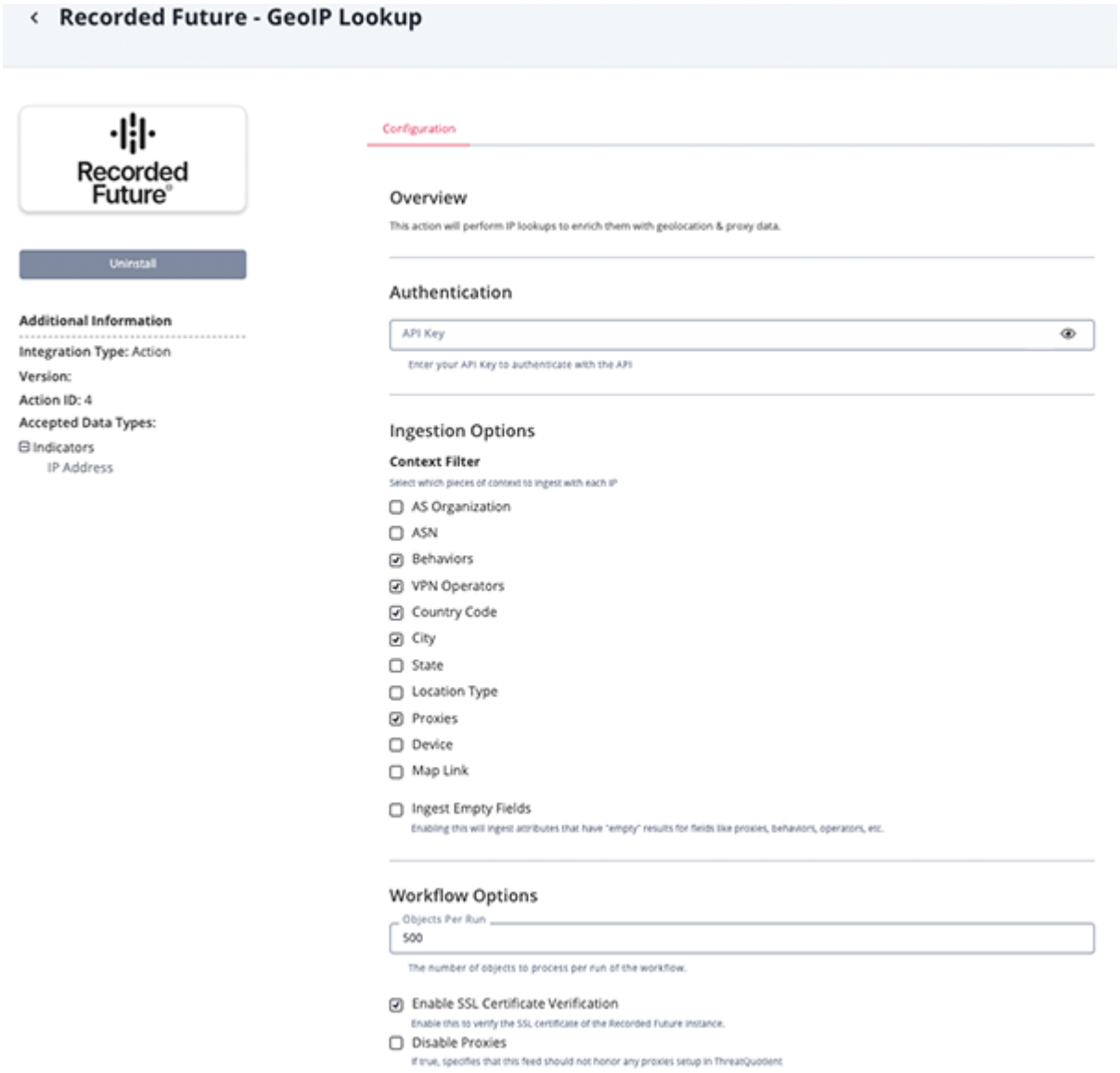
PARAMETER	DESCRIPTION
API Key	Your Recorded Future API Key.
Supporting Context	Select the context for the action to return. Options include: ◦ **CVSSv3 (default)** - ingests attributes related to CVSS ◦ **Affected Versions (default)** - ingests cpe22Uri information as one attribute ◦ **Intelligence Card** - ingests the attribute Intelligence Card ◦ **Related Links** - ingests the attribute Related Links ◦ **Related Hashes** - ingests hash values as related indicators ◦ **Related Email Addresses** - ingests email addresses as related indicators ◦ **Related Internet Domain Names** - ingests FQDNs as related indicators ◦ **Related IP Addresses** - ingests IP Addresses as related indicators ◦ **Related Threat Actors** - ingests threat actors as related adversaries ◦ **Related Malware** - ingests malware as related malware
Objects Per Run	The number of object to return with each run.
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.



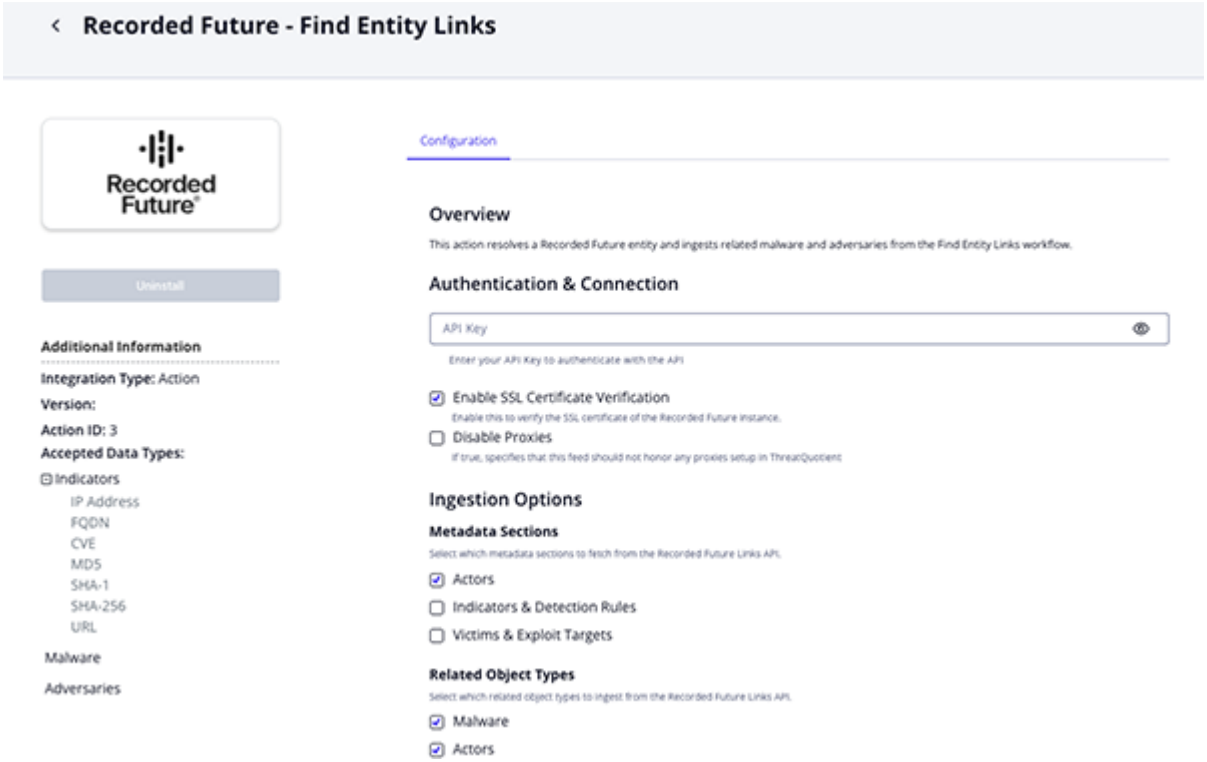
Recorded Future - GeoIP Lookup Parameters

PARAMETER	DESCRIPTION
API Key	Your Recorded Future API Key.
Context Filter	Select which pieces of context to ingest with each IP. Options include: ◦ AS Organization ◦ ASN ◦ Behaviors (default) ◦ VPN Operators (default) ◦ Country Code (default) ◦ City (default) ◦ State ◦ Location Type ◦ Proxies *(default)* ◦ Device ◦ Map Link
Ingest Empty Fields	Enable this parameter to ingest attributes that have empty results for fields such as proxies, behaviors, and operators. This parameter is disabled by default.
Objects Per Run	The number of object to return with each run.
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.


Recorded Future - GeoIP Lookup
Recorded Future
Uninstall
Additional Information
Integration Type: Action
Version:
Action ID: 4
Accepted Data Types:
Indicators
IP Address
Configuration
Overview
This action will perform IP lookups to enrich them with geolocation & proxy data.
Authentication
API Key
Enter your API Key to authenticate with the API
Ingestion Options
Context Filter
Select which pieces of context to ingest with each IP
AS Organization
ASN
Behaviors
VPN Operators
Country Code
City
State
Location Type
Proxies
Device
Map Link
Ingest Empty Fields
Enabling this will ingest attributes that have "empty" results for fields like proxies, behaviors, operators, etc.
Workflow Options
Objects Per Run
500
The number of objects to process per run of the workflow.
Enable SSL Certificate Verification
Enable this to verify the SSL certificate of the Recorded Future instance.
Disable Proxies
If true, specifies that this feed should not honor any proxies setup in ThreatQuotient

Recorded Future - Find Entity Links Parameters

PARAMETER	DESCRIPTION
API Key	Your Recorded Future API Key.
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.
Metadata Sections	Select which Recorded Future metadata sections to search for related links. Options include: ◦ Actors *(default)* ◦ Indicators & Detection Rules ◦ Victims & Exploit Targets
Related Object Types	Select which related object types to ingest from the Recorded Future Links API. Options include: ◦ Malware *(default)* ◦ Actors *(default)*
Sources	Select which Recorded Future source types to use when searching entity links. Options include: ◦ Technical *(default)* ◦ Insikt Group *(default)*
Objects Per Run	The number of object to return with each run.



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

Actions Functions

The following actions are available with the integration:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Recorded Future	Submits the data to the SOAR Enrichment API and gets the IOC related data	Indicator	MD5, SHA-1, SHA-256, SHA-512, IP Address, Domain, URL, CVE
Recorded Future - Vulnerabilities	Submits the data to the Vulnerability API and gets more information and related IOCs	Indicator, Vulnerability	Indicator Type: CVE
Recorded Future - GeoIP Lookup	Retrieves the geographical location and proxy information of the provided IP address.	Indicator	IP Address
Recorded Future - Find Entity Links	Resolves a Recorded Future entity and ingests related malware, adversaries	Indicator, Malware, Adversary	Indicator Type: IP Address, FQDN, CVE, MD5, SHA-1, SHA-256, URL

Recorded Future

The Recorded Future action collects the user data fields and submits it to the Recorded Future API via POST call. The API analyzes the IP Address or url or domain which we have passed as run_params, sends the risk score, rule associated to it and even the threat type of the object.

```
POST https://api.recordedfuture.com/v3/soar/enrichment
```

Sample Response:


```
[
    {
        "Recorded_Future_action": {
            "results": [
                {
                    "entity": {
                        "id": "ip:5.39.93.43",
                        "name": "5.39.93.43",
                        "type": "IpAddress"
                    },
                    "risk": {
                        "context": {
                            "c2": {
                                "rule": {
                                    "count": 0,
                                    "maxCount": 2
                                },
                                "score": 0.0
                            },
                            "phishing": {
                                "rule": {
                                    "count": 0,
                                    "maxCount": 3
                                },
                                "score": 0.0
                            },
                            "public": {
                                "mostCriticalRule": "Historical
Positive Malware Verdict",
                                "rule": {
                                    "maxCount": 63
                                },
```

```
                                "score": 24.0,
                                "summary": [
                                    {
                                        "count": 6.0,
                                        "level": 1.0
                                    }
                                ]
                            }
                        },
                        "level": 1.0,
                        "rule": {
                            "count": 6,
                            "evidence": {
                                "analystNote": {
                                    "count": 1,
                                    "description": "1 sighting on 1
source: <e id=VKz42X>Insikt Group</e>. 1 report: Recorded Future-
analyzed sample communicates with <e
id=ip:5.39.93.43>5[.]39[.]93[.]43</e>, historical <e id=LPc838>C&C
server</e>. Most recent link (Jul 30, 2018): https://
app.recordedfuture.com/live/sc/5UVpLbAD91Ga",
                                    "level": 1,
                                    "mitigation": "",
                                    "rule": "Historically Reported by
Insikt Group",
                                    "sightings": 1,
                                    "timestamp":
"2018-07-30T00:00:00.000Z"
                                },
                                "cncServer": {
                                    "count": 2,
                                    "description": "3 sightings on 2
sources: <e id=RqhhKn>BroadAnalysis</e>, <e id=VKz42X>Insikt Group</
e>.",
                                    "level": 1,
                                    "mitigation": "",
                                    "rule": "Historical C&C Server",
                                    "sightings": 3,
                                    "timestamp":
"2022-09-08T07:45:46.296Z"
                                },
                                "historicalThreatListMembership": {
```

```
                                    "count": 1,
                                    "description": "Previous
sightings on 1 source: <e id=report:Tluf00>Recorded Future Analyst
Community Trending Indicators</e>. Observed between Aug 13, 2018, and
Aug 21, 2018.",
                                    "level": 1,
                                    "mitigation": "",
                                    "rule": "Historically Reported in
Threat List",
                                    "sightings": -1,
                                    "timestamp":
"2022-09-08T07:45:46.296Z"
                                },
                                "linkedIntrusion": {
                                    "count": 2,
                                    "description": "3 sightings on 2
sources: <e id=LErKlJ>Malware-Traffic-Analysis.net - Blog Entries</
e>, <e id=TbciDE>ReversingLabs</e>. 5 related intrusion methods: <e
id=JVTS__>Exploit Kit</e>, <e id=QhiNin>CryptMix</e>, <e
id=LFGSHZ>RIG Exploit Kit</e>, <e id=J0Nl-p>Ransomware</e>, <e
id=ctmpMt>Trojan.Hydracrypt</e>. Most recent link (Oct 19, 2016):
https://a1000.reversinglabs.com/accounts/login/?next=/
%3Fq%3D573c68bd0951e81e24d4fc5ca8fb9756866e53aefa8ea085a0d5aa31f28dbf
08",
                                    "level": 1,
                                    "mitigation": "",
                                    "rule": "Historically Linked to
Intrusion Method",
                                    "sightings": 3,
                                    "timestamp":
"2016-10-19T12:26:00.000Z"
                                },
                                "positiveMalwareVerdict": {
                                    "count": 2,
                                    "description": "3 sightings on 2
sources: <e id=LErKlJ>Malware-Traffic-Analysis.net - Blog Entries</
e>, <e id=TbciDE>ReversingLabs</e>. Most recent link (Oct 17, 2016):
http://malware-traffic-analysis.net/2016/10/17/index.html",
                                    "level": 1,
                                    "mitigation": "",
                                    "rule": "Historical Positive
Malware Verdict",
```

```
                                    "sightings": 3,
                                    "timestamp":
"2016-10-19T00:00:00.000Z"
                                },
                                "threatResearcher": {
                                    "count": 1,
                                    "description": "2 sightings on 1
source: <e id=RqhhKn>BroadAnalysis</e>. Most recent link (Oct 17,
2016): http://www.broadanalysis.com/2016/10/17/rig-exploit-kit-via-
eitest-delivers-crypt2-ransomware-c2-5-39-93-43/",
                                    "level": 1,
                                    "mitigation": "",
                                    "rule": "Historical Threat
Researcher",
                                    "sightings": 2,
                                    "timestamp":
"2016-10-17T18:27:32.000Z"
                                }
                            },
                            "maxCount": 64,
                            "mostCritical": "Historical Positive
Malware Verdict",
                            "summary": [
                                {
                                    "count": 6.0,
                                    "level": 1.0
                                }
                            ]
                        },
                        "score": 24
                    }
                }
            ]
        }
    }
]
```


ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.risk.score	Indicator.Attribute	Risk Score	N/A	24	User-configurable. Updatable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.risk.score	Indicator.Attribute	Normalized Risk Score	N/A	Low	User-configurable. Updatable. Derived from user-defined normalization mapping as per risk score value
.risk.context.c2.score	Indicator.Attribute	Threat Type	N/A	C2	User-configurable. C2 if .risk.context.c2.score is grater than 0
.risk.context.phishing.score	Indicator.Attribute	Threat Type	N/A	Phishing	User-configurable Phishing if .risk.context.phishing.score is grater than 0
.risk.context.malware.score	Indicator.Attribute	Threat Type	N/A	Malware	User-configurable Malware if .risk.context.malware.score is grater than 0
.risk.rule.evidence.rule	Indicator.Attribute	Associated Rule	N/A	Historically Reported by Insikt Group	User-configurable
.md5_hash	Indicator.Value	MD5	N/A	N/A	N/A
.sha1_hash	Indicator.Value	SHA-1	N/A	N/A	N/A
.sha256_hash	Indicator.Value	SHA-256	N/A	N/A	N/A
.sha512_hash	Indicator.Value	SHA-512	N/A	N/A	N/A
.c2	Indicator.Value	IP ADDRESS	N/A	5.39.93.43	N/A
.c2	Indicator.Value	URL	N/A	https://www.gmail.com/malware.php	N/A
.c2	Indicator.Value	Domain	N/A	google.com	N/A

Recorded Future - Vulnerabilities

The Recorded Future - Vulnerabilities action submits CVE type indicators or vulnerabilities to Recorded Future Vulnerability API. The API returns more information about the vulnerability and related IOCs. Depending on user data fields the selected pieces of information are ingested to the ThreatQ platform.

```
GET https://api.recordedfuture.com/v2/vulnerability/CVE-2021-21033
```

Sample Query Request:

```
{
  "fields":
"nvdDescription,entity,timestamps,relatedEntities,cvssv3,cpe22uri,intelCard,relatedLinks"
}
```

Sample Response:


```
{
  "data": {
    "relatedLinks": [
      "https://github.com/zldww2011/CVE-2018-0802_POC",
      "http://www.securityfocus.com/bid/102347"
    ],
    "timestamps": {
      "lastSeen": "2023-10-02T21:36:50.949Z",
      "firstSeen": "2018-01-09T18:54:06.320Z"
    },
    "cvssv3": {
      "scope": "UNCHANGED",
      "exploitabilityScore": 1.8,
      "modified": "2020-08-24T17:37:00.000Z",
      "baseSeverity": "HIGH",
      "baseScore": 7.8,
      "privilegesRequired": "NONE",
      "userInteraction": "REQUIRED",
      "impactScore": 5.9,
      "attackVector": "LOCAL",
      "integrityImpact": "HIGH",
      "confidentialityImpact": "HIGH",
      "vectorString": "CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H",
      "version": "3.0",
      "attackComplexity": "LOW",
      "created": "2018-01-10T01:29:00.000Z",
      "availabilityImpact": "HIGH"
    },
    "intelCard": "https://app.recordedfuture.com/live/sc/entity/U_3qAY",
    "cpe22uri": [
      "cpe:/a:microsoft:word:2016",
      "cpe:/a:microsoft:office:2013:sp1:~~~rt~~"
    ],
```

```
    "entity": {
      "id": "U_3qAY",
      "name": "CVE-2018-0802",
      "type": "CyberVulnerability",
      "description": "Equation Editor in Microsoft Office 2007, Microsoft Office
2010, Microsoft Office 2013, and Microsoft Office 2016 allow a remote code execution
vulnerability due to the way objects are handled in memory, aka \"Microsoft Office
Memory Corruption Vulnerability\". This CVE is unique from CVE-2018-0797 and
CVE-2018-0812."
    },
    "relatedEntities": [
      {
        "entities": [
          {
            "count": 6,
            "entity": {
              "id": "hash:4195192b66a50fd0641019f634d2c86c",
              "name": "4195192b66a50fd0641019f634d2c86c",
              "type": "Hash"
            }
          }
        ],
        "type": "RelatedHash"
      },
      {
        "entities": [
          {
            "count": 2,
            "entity": {
              "id": "email:kevin.beaumont@gmail.com",
              "name": "kevin.beaumont@gmail.com",
              "type": "EmailAddress"
            }
          }
        ],
        "type": "RelatedEmailAddress"
      },
      {
        "entities": [
          {
            "count": 13,
            "entity": {
              "id": "idn:cracking.to",
              "name": "cracking.to",
              "type": "InternetDomainName"
            }
          }
        ],
        "type": "RelatedInternetDomainName"
      },
      {
        "entities": [
```

```
        {
          "count": 1501,
          "entity": {
            "id": "B56PMu",
            "name": "SHA-256",
            "type": "Technology"
          }
        }
      ],
      "type": "RelatedTechnology"
    },
    {
      "entities": [
        {
          "count": 7,
          "entity": {
            "id": "ip:118.189.81.19",
            "name": "118.189.81.19",
            "type": "IpAddress"
          }
        }
      ],
      "type": "RelatedIpAddress"
    },
    {
      "entities": [
        {
          "count": 1,
          "entity": {
            "id": "izUZWO",
            "name": "RedFoxtrot",
            "type": "Organization"
          }
        }
      ],
      "type": "RelatedAttacker"
    },
    {
      "entities": [
        {
          "count": 637,
          "entity": {
            "id": "QIfsz2",
            "name": "Trillium Security MultiSploit Tool",
            "type": "Malware"
          }
        }
      ],
      "type": "RelatedMalware"
    },
    {
      "entities": [
```

```
        {
          "count": 446,
          "entity": {
            "id": "0efpT",
            "name": "Trojan",
            "type": "MalwareCategory"
          }
        }
      ],
      "type": "RelatedMalwareCategory"
    },
    {
      "entities": [
        {
          "count": 13063,
          "entity": {
            "id": "ROY7kq",
            "name": "CWE-787",
            "type": "CyberVulnerability"
          }
        }
      ],
      "type": "RelatedCyberVulnerability"
    },
    {
      "entities": [
        {
          "count": 582,
          "entity": {
            "id": "UUJs-s",
            "name": "Trillium",
            "type": "Person"
          }
        }
      ],
      "type": "RelatedThreatActor"
    },
    {
      "entities": [
        {
          "count": 2,
          "entity": {
            "id": "Ee0a8",
            "name": "People's Liberation Army (China)",
            "type": "Organization"
          }
        }
      ],
      "type": "RelatedTarget"
    },
    {
      "entities": [
```

```
          {
            "count": 709,
            "entity": {
              "id": "0fsV7",
              "name": "Zero Day Exploit",
              "type": "AttackVector"
            }
          }
        ],
        "type": "RelatedAttackVector"
      }
    ],
    "nvdDescription": "Equation Editor in Microsoft Office 2007, Microsoft Office
2010, Microsoft Office 2013, and Microsoft Office 2016 allow a remote code execution
vulnerability due to the way objects are handled in memory, aka \"Microsoft Office
Memory Corruption Vulnerability\". This CVE is unique from CVE-2018-0797 and
CVE-2018-0812."
  }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data.entity.name	Indicator.Value/ Vulnerability.Value	CVE/N/A	.data.timestamps.firstSeen	CVE-2018-0802	The object has the same type as the input value from the ThreatQ collection.
.data.nvdDescription	Indicator.Description/ Vulnerability.Description	N/A	N/A	Equation Editor in Microsoft Office 2007, Microsoft Office 2010...	N/A
.data.cpe22uri[]	Indicator.Attribute/ Vulnerability.Attribute	Affected Versions	.data.timestamps.firstSeen	cpe:/a:microsoft:word:2016, cpe:/a:microsoft2013:sp1:~~rt~~	User-configurable. Values are concatenated
.data.cvssv3.created	Indicator.Attribute/ Vulnerability.Attribute	CVSS3 Created Date	.data.timestamps.firstSeen	2018-01-10T01:29:00.000Z	User-configurable. Updatable
.data.cvssv3.baseSeverity	Indicator.Attribute/ Vulnerability.Attribute	CVSSv3 Base Severity	.data.timestamps.firstSeen	HIGH	User-configurable. Updatable
.data.cvssv3.baseScore	Indicator.Attribute/ Vulnerability.Attribute	CVSSv3 Base Score	.data.timestamps.firstSeen	7.8	User-configurable. Updatable
.data.cvssv3.exploitabilityScore	Indicator.Attribute/ Vulnerability.Attribute	CVSSv3 Exploitability Score	.data.timestamps.firstSeen	1.8	User-configurable. Updatable
.data.cvssv3.impactScore	Indicator.Attribute/ Vulnerability.Attribute	CVSSv3 Impact Score	.data.timestamps.firstSeen	5.9	User-configurable. Updatable
.data.cvssv3.version	Indicator.Attribute/ Vulnerability.Attribute	CVSSv3 Version	.data.timestamps.firstSeen	3.0	User-configurable. Updatable
.data.cvssv3.vectorString	Indicator.Attribute/ Vulnerability.Attribute	CVSSv3 Vector String	.data.timestamps.firstSeen	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	User-configurable. Updatable
.data.cvssv3.attackVector	Indicator.Attribute/ Vulnerability.Attribute	CVSSv3 Attack Vector	.data.timestamps.firstSeen	LOCAL	User-configurable. Updatable
.data.cvssv3.attackComplexity	Indicator.Attribute/ Vulnerability.Attribute	CVSSv3 Attack Complexity	.data.timestamps.firstSeen	LOW	User-configurable. Updatable
.data.cvssv3.privilegesRequired	Indicator.Attribute/	CVSSv3 Privileges Required	.data.timestamps.firstSeen	NONE	User-configurable. Updatable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
	Vulnerability.Attribute				
.data.cvssv3.userInteraction	Indicator.Attribute/ Vulnerability.Attribute	CVSSv3 User Interaction	.data.timestamps.firstSeen	REQUIRED	User-configurable. Updatable
.data.cvssv3.scope	Indicator.Attribute/ Vulnerability.Attribute	CVSSv3 Scope	.data.timestamps.firstSeen	UNCHANGED	User-configurable. Updatable
.data.cvssv3.confidentialityImpact	Indicator.Attribute/ Vulnerability.Attribute	CVSSv3 Confidentiality Impact	.data.timestamps.firstSeen	HIGH	User-configurable. Updatable
.data.cvssv3.integrityImpact	Indicator.Attribute/ Vulnerability.Attribute	CVSSv3 Integrity Impact	.data.timestamps.firstSeen	HIGH	User-configurable. Updatable
.data.cvssv3.availabilityImpact	Indicator.Attribute/ Vulnerability.Attribute	CVSSv3 Availability Impact	.data.timestamps.firstSeen	HIGH	User-configurable. Updatable
.data.cvssv3.intelCard	Indicator.Attribute/ Vulnerability.Attribute	Intelligence Card	.data.timestamps.firstSeen	https://app.recordedfuture.com/live/sc/entity/U_3qAY	User-configurable. Updatable
.data.cvssv3.relatedLinks[]	Indicator.Attribute/ Vulnerability.Attribute	Related Link	.data.timestamps.firstSeen	https://github.com/zldww2011/CVE-2018-0802_POC	User-configurable.
.data.cvssv3.relatedEntities[].entities[].entity.name	Related Indicator.Value	MD5/ SHA-1/ SHA-256/ SHA-512	.data.timestamps.firstSeen	4195192b66a50fd0641019f634d2c86c	User-configurable. If .data.cvssv3.relatedEntities[].type is Hash.
.data.cvssv3.relatedEntities[].entities[].entity.name	Related Indicator.Value	Email Address	.data.timestamps.firstSeen	kevin.beaumont@gmail.com	User-configurable. If .data.cvssv3.relatedEntities[].type is RelatedEmailAddress.
.data.cvssv3.relatedEntities[].entities[].entity.name	Related Indicator.Value	FQDN	.data.timestamps.firstSeen	cracking.to	User-configurable. If .data.cvssv3.relatedEntities[].type is RelatedInternetDomainName.
.data.cvssv3.relatedEntities[].entities[].entity.name	Related Indicator.Value	IP Address	.data.timestamps.firstSeen	118.189.81.19	User-configurable. If .data.cvssv3.relatedEntities[].type is RelatedIpAddress.
.data.cvssv3.relatedEntities[].entities[].entity.name	Related Adversary.Name	N/A	.data.timestamps.firstSeen	Trillium	User-configurable. If .data.cvssv3.relatedEntities[].type is RelatedThreatActor.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data.cvssv3.relatedEntities[].entities[].entity.name	Related Malware.Name	N/A	.data.timestamps.firstSeen	Trillium Security MultiSploit Tool	User-configurable. If .data.cvssv3.relatedEntities[].type is RelatedMalware.

Recorded Future - GeoIP Lookup

The Recorded Future - GeoIP Lookup action takes a data collection of IP addresses and performs a lookup to fetch geolocation and proxy information. You can find out information such as the location data, behaviors, VPN operators, and more.

```
GET https://api.recordedfuture.com/v2/ip/{{ value }}/extension/
active_ip_geo
```

Sample Response:


```
{
  "data": {
    "organization": "PT. SUITEN INOVASI SUKSES",
    "proxies": ["No proxied traffic detected on this IP."],
    "ip": {
      "id": "ip:103.120.66.51",
      "name": "103.120.66.51",
      "type": "IpAddress"
    },
    "map": {
      "url": "https://www.google.com/maps/search/?api=1&query=ID
country",
      "name": "Google Maps (precision: country)"
    },
    "geo": {
      "country": "ID",
      "type": "Hosting Location"
    },
    "support_link": {
      "url": "https://support.recordedfuture.com/hc/en-us/articles/
1500011643082",
      "name": "External Link"
    },
    "asn": {
      "id": "asn:AS137373",
      "name": "AS137373",
      "type": "ASNumber"
    },
    "behaviors": ["Behavioral analysis not available for this IP."],
    "operators": ["No VPN operations detected on this IP."],
    "devices": "estimate unavailable"
```

```
    }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.organization	Indicator.Attribute	AS Organization	N/A	PT. SUITEN INOVASI SUKSES	User-configurable.
.proxies[]	Indicator.Attribute	Proxy	N/A	N/A	User-configurable.
.map.url	Indicator.Attribute	Map Link	N/A	N/A	User-configurable.
.geo.country	Indicator.Attribute	Country Code	N/A	US	User-configurable.
.geo.city	Indicator.Attribute	City	N/A	San Francisco	User-configurable.
.geo.state	Indicator.Attribute	State	N/A	California	User-configurable.
.geo.type	Indicator.Attribute	Location Type	N/A	Hosting Location	User-configurable.
.asn.name	Indicator.Attribute	ASN	N/A	AS137373	User-configurable.
.behaviors[]	Indicator.Attribute	Behavior	N/A	N/A	User-configurable.
.operators[]	Indicator.Attribute	VPN Operator	N/A	N/A	User-configurable.
.devices	Indicator.Attribute	Device	N/A	N/A	User-configurable.

Recorded Future - Find Entity Links

The Recorded Future – Find Entity Links action resolves the provided indicator, malware, or adversary into corresponding Recorded Future entities, then leverages link analysis to identify and ingest related malware, adversaries, and victim context into ThreatQ.

Resolving Object

This action first resolves the ThreatQ object to a Recorded Future entity.

```
POST https://api.recordedfuture.com/entity-match/match
```

Sample Request:

```
{
    "name": "1.1.1.1",
    "type": ["type:IpAddress"],
    "limit": 5
}
```

Sample Response:

```
[
    {
        "id": "ip:1.1.1.1",
        "name": "1.1.1.1",
        "type": "IpAddress"
    }
]
```

Searching Links

The action then searches the Recorded Future links graph for the matched entity IDs.

```
POST https://api.recordedfuture.com/links/search
```

Sample Request:

```
{
    "entities": ["ip:1.1.1.1"],
    "filters": {
        "sections": ["iU_ZsE", "iU_ZsI"],
        "entity_types": ["type:Malware", "type:Person",
"type:Organization"],
        "sources": ["technical", "insikt"]
    },
```

```
    "limits": {
        "search_scope": "medium",
        "per_entity_type": 100
    }
}
```

Sample Response:

```
{
    "data": [
        {
            "entity": {
                "type": "type:IpAddress",
                "id": "ip:1.1.1.1",
                "name": "1.1.1.1"
            },
            "links": [
                {
                    "type": "type:Malware",
                    "id": "VtMwd9",
                    "name": "BRICKSTORM",
                    "source": "technical",
                    "section": "iU_ZsE",
                    "attributes": [
                        {
                            "id": "criticality",
                            "value": "Malicious"
                        },
                        {
                            "id": "risk_score",
                            "value": 70
                        },
                        {
                            "id": "risk_level",
                            "value": 3
                        }
                    ]
                },
                {
                    "type": "type:Organization",
                    "id": "M6NPJ7",
                    "name": "Martinique Government",
                    "source": "insikt",
```

```
                    "section": "iU_ZsI",
                    "attributes": [
                        {
                            "id": "threat_actor",
                            "value": false
                        }
                    ]
                }
            ]
        }
    ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.links[].name	Related Malware.Value	N/A	N/A	WARZONE RAT	If .links[].type is type:Malware.
.links[].attributes[].value	Related Malware.Attribute	Criticality	N/A	Malicious	If .links[].attributes[].id is criticality.
.links[].attributes[].value	Related Malware.Attribute	Risk Score	N/A	70	If .links[].attributes[].id is risk_score.
.links[].attributes[].value	Related Malware.Attribute	Risk Level	N/A	3	If .links[].attributes[].id is risk_level.
.links[].name	Related Adversary.Name	N/A	N/A	WARP Panda	If .links[].type is type:Person or type:Organization and .links[].attributes[].id is threat_actor with value true.
.links[].attributes[].value	Related Adversary.Attribute	Criticality	N/A	Malicious	If present on the adversary link and .links[].attributes[].id is criticality.
.links[].attributes[].value	Related Adversary.Attribute	Risk Score	N/A	70	If present on the adversary link and .links[].attributes[].id is risk_score.
.links[].attributes[].value	Related Adversary.Attribute	Risk Level	N/A	3	If present on the adversary link and .links[].attributes[].id is risk_level.
.links[].name	Indicator.Attribute / Malware.Attribute / Adversary.Attribute	Victim	N/A	Martinique Government	If .links[].type is type:Person or type:Organization and threat_actor is false or not present. Added to the original source object.

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.

Recorded Future

METRIC	RESULT
Run Time	2 minutes
Indicators	100
Indicator Attributes	300

Recorded Future - Vulnerabilities

METRIC	RESULT
Run Time	2 minutes
Indicators	781
Indicator Attributes	16
Vulnerability	3
Vulnerability Attributes	67

Recorded Future - GeoIP Lookup

METRIC	RESULT
Run Time	1 minute
Indicators	3
Indicator Attributes	343

Recorded Future - Find Entity Links

METRIC	RESULT
Run Time	1 minute
Adversaries	10
Indicators	100
Indicator Attributes	100
Malware	25

Use Case Example

Recorded Future Action

1. A user submits IP Address `5.39.93.43` data using the Recorded Future action to the Recorded Future Enrichment SOAR API.
2. The Recorded Future API queries to submitted data for IP Address type data.
3. The action returns a list of dictionary type data from the provider which contains details like Risk score, Associated Rule, Threat Type etc.

Recorded Future Vulnerabilities Action

1. A user submits CVE `CVE-2018-0802` data using the Recorded Future - Vulnerabilities action to the Recorded Future Vulnerability API.
2. The Recorded Future API queries its database to retrieve all the information about the submitted data.
3. The action returns a dictionary type data from the provider which contains all the available information.

Recorded Future Find Entity Links

1. A user submits a collection of indicators, malware, or adversaries to `Recorded Future - Find Entity Links`.
2. The action resolves each object to Recorded Future entity IDs using the entity match API.
3. The action searches Recorded Future relationship data and ingests related malware, threat actors, and victims back into ThreatQ.

Known Issues / Limitations

- This enrichment action utilizes Recorded Future's "SOAR Enrichment" API, which only returns a subset of everything Recorded Future knows about a given IOC.
- Long runs with data collections larger than 500 objects may cause the Recorded Future API to timeout.

Change Log

- **Version 1.5.0**
  - Added a new action, **Recorded Future - Find Entity Links**. This action adds support for ingesting related malware, adversaries from Recorded Future entity links. The action also adds support for ingesting victims as a `Victim` attribute when a linked person or organization is not a threat actor.
- **Version 1.4.0**
  - Enhanced performance by updating SOAR Enrichment API queries to execute in bulk rather than per indicator.
  - Added support for enriching Vulnerability (CVE ID) objects.
  - Introduced risk score normalization to convert numeric values into human-readable formats, aligned with Recorded Future feeds.
  - Added support for the Threat Type: Malware attribute when applicable.
  - Added a new configuration parameter to the Recorded Future action:
    - **Normalize Risk Scores** - configure a mapping to normalize numeric threat score values to the scorable attribute, Normalized Threat Score.
- **Version 1.3.0**
  - The `Risk Score` attribute for the **Recorded Future** action is now updatable.
  - Added the following configuration parameters to all actions:
    - **Enable SSL Certificate Verification** - enable or disable verification of the server's SSL certificate.
    - **Disable Proxies** - determines if the action should honor proxy settings set in the ThreatQ UI.
- **Version 1.2.0**
  - Added a new action: **Recorded Future - GeoIP Lookup**. This action retrieves the geographical location and proxy information for submitted IP addresses.
  - Added a new known issue where long runs with data collections larger than 1,000 objects may cause the Recorded Future API to timeout.
- **Version 1.1.0**
  - Added new action: **Recorded Future - Vulnerabilities**.
  - Updated minimum ThreatQ version to 5.19.0.
  - Updated user guide name to Recorded Future Action Bundle.

- **Version 1.0.0**
  - Initial release