

ThreatQuotient



Recorded Future CDF

Version 2.10.1

November 11, 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	4
Support	5
Integration Details.....	6
Introduction	7
Prerequisites	8
Installation.....	9
Configuration	10
Recorded Future Domain Risk List Parameters.....	10
Recorded Future Vulnerability Risk List Parameters	15
Recorded Future Hash Risk List Parameters	18
Recorded Future IP Risk List Parameters	21
Recorded Future URL Risk List Parameters	25
Recorded Future Analyst Note Parameters	28
Recorded Future Alerts Parameters.....	31
Recorded Future Playbook Alerts Parameters	33
Recorded Future Fusion Files Parameters	35
ThreatQ Mapping.....	37
Recorded Future Domain Risk List	37
Recorded Future IP Risk List.....	39
Recorded Future URL Risk List	40
Recorded Future Vulnerability Risk List	41
Recorded Future Hash Risk List	42
Recorded Future Analyst Note	44
Entities Mapping	46
Recorded Future Alerts	48
Related Indicator Type Mapping	53
Event Attributes Mapping.....	54
Recorded Future Playbook Alerts.....	56
Recorded Future - Get Playbook Alerts by Category (Supplemental)	60
Domain Abuse	60
Third Party Risk.....	64
Cyber Vulnerability.....	66
Code Repo Leakage	68
Recorded Future Fusion Files.....	71
Command and Control IPs	71
Known TOR IPs.....	73
Active RAT C2 IPs	74
Fast Flux IPs.....	75
Dynamic DNS IPs	76
Potentially Undetectable Malware.....	77
Weaponized Domains.....	78
Exploits in the Wild Hashes.....	80

Average Feed Run.....	81
Recorded Future Domain Risk List	81
Recorded Future IP Risk List.....	81
Recorded Future URL Risk List	81
Recorded Future Vulnerability Risk	82
Recorded Future Hash Risk List	82
Recorded Future Analyst Note	83
Recorded Future Alerts	83
Recorded Future Playbook Alerts	84
Recorded Future Fusion Files	85
Known Issues / Limitations	86
Change Log	87

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.

Copyright © 2024 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

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	2.10.1
Compatible with ThreatQ Versions	>= 5.6.0
Support Tier	ThreatQ Supported

Introduction

The Recorded Future CDF ingests threat intelligence data from the following feeds published by the *Recorded Future* vendor:

- **Recorded Future Domain Risk List** - retrieves information in the form of a CSV list where the first token is risk data and the last token containing the supporting context.
- **Recorded Future IP Risk List** - retrieves IP Addresses from the provider.
- **Recorded Future URL Risk List** - retrieves URLs from the provider.
- **Recorded Future Vulnerability Risk List** - retrieves CVEs from the provider.
- **Recorded Future Hash Risk List** - retrieves Hashes from the provider.
- **Recorded Future Analyst Note** - retrieves Reports, Indicators, and Attack Patterns from the provider.
- **Recorded Future Alerts** - retrieves Alerts from the provider.
- **Recorded Future Alerts Details (Supplemental)** - retrieves related data for each of the ingested events retrieved from the Alert endpoint.
- **Recorded Future Playbook Alerts** - retrieves a list of alerts filtered by the values provided in the configuration section.
- **Recorded Future - Get Playbook Alerts (Supplemental)** - retrieves related data for each of the ingested events retrieved from the Alert endpoint.
- **Recorded Future Fusion Files** - ingests threat intelligence information from the user selected Fusion feeds.

The integration ingests the following system objects:

- Adversaries
- Assets
- Attack Patterns
- Events
- Identities
- Indicators
- Malware
- Reports
- Vulnerabilities

Prerequisites

The following is required to install and run the integration:

- MITRE ATT&CK attack patterns must have already been ingested by a previous run of the MITRE ATT&CK feeds in order for MITRE ATT&CK attack patterns ingested by the Analyst Note feed to be created. MITRE ATT&CK attack patterns are ingested from the following feeds:
 - MITRE Enterprise ATT&CK
 - MITRE Mobile ATT&CK
 - MITRE PRE-ATT&CK

Installation

Perform the following steps to install the integration:



The same steps can be used to upgrade the integration to a new version.

1. Log into <https://marketplace.threatq.com/>.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration yaml file using one of the following methods:
 - Drag and drop the yaml file into the dialog box
 - Select **Click to Browse** to locate the yaml file on your local machine
6. Select the individual feeds to install, when prompted, and click **Install**. The feed will be added to the integrations page.



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

You will still need to [configure and then enable](#) the feed.

Configuration



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

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).



If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:



All Recorded Future feeds require the Recorded Future API Key. The tables below provide any additional parameters required for specific feeds included with this integration.

Recorded Future Domain Risk List Parameters

PARAMETER	DESCRIPTION
API Key	Your API Key to be used in HTTP headers for accessing feed data.
List to be Retrieved	Use the checkboxes provided to select specific Recorded Future lists to be retrieved.  It is highly recommended to use the All option as it will ingest the latest information from Recorded Future. If you are using the All option, confirm that you have unselected the other options. Running the feed with the All option selected along with other individual list options, will cause the feed to fail. This is a known issue and will be addressed in a future release of the integration. You should schedule feed runs hourly or longer when using the All option.

PARAMETER

DESCRIPTION

Options include:

- All (default)
- Historically Reported by Insikt Group
- Historically Reported Botnet Domain
- Newly Registered Certificate With Potential for Abuse - DNS Sandwich
- Newly Registered Certificate With Potential for Abuse - Typo or Homograph
- C&C Nameserver
- Historical C&C DNS Name
- Historical COVID-19-Related Domain Lure
- Recently Resolved to Host of Many DDNS Names
- Historically Reported as a Defanged DNS Name
- Historically Reported by DHS AIS
- Recent Fast Flux DNS Name
- Historically Reported Fraudulent Content
- Frequently Abused Free DNS Provider
- Historically Reported in Threat List
- Historically Linked to Cyber Attack
- Historically Detected Malware Operation
- Historically Suspected Malware Operation
- Historically Detected Cryptocurrency Mining Techniques
- Blacklisted DNS Name
- No Risk Observed
- Observed in the Wild by Recorded Future Telemetry
- Historical Phishing Lure
- Historically Detected Phishing Techniques
- Historically Suspected Phishing Techniques
- Active Phishing URL
- Recorded Future Predictive Risk Model
- Recently Reported Fraudulent Content
- Recently Linked to Cyber Attack
- Recently Detected Malware Operation
- Recently Suspected Malware Operation
- Recent Cryptocurrency Mining Pool
- Recently Detected Cryptocurrency Mining Techniques
- Recent Phishing Lure: Malicious
- Recent Phishing Lure: Suspicious
- Recently Detected Phishing Techniques
- Recently Suspected Phishing Techniques
- Recent Web Filter Avoidance Proxy Domain
- Recent Punycode Domain
- Recently Referenced by Insikt Group
- Recently Reported Spam or Unwanted Content
- Recent Suspected C&C DNS Name
- Recent Threat Researcher
- Recent Typosquat Similarity - DNS Sandwich
- Recent Typosquat Similarity - Typo or Homograph
- Recent Ukraine-Related Domain Lure: Malicious
- Recent Ukraine-Related Domain Lure: Suspicious
- Recently Active Weaponized Domain

PARAMETER

DESCRIPTION

- | | |
|---|---|
| ○ Historically Detected Web Filter Avoidance Proxy Domain | ○ Recently Defaced Site |
| ○ Historical Punycode Domain | ○ Historically Referenced by Insikt Group |
| ○ Recently Reported by Insikt Group | ○ Recently Resolved to Malicious IP |
| ○ Recently Reported Botnet Domain | ○ Recently Resolved to Suspicious IP |
| ○ Recent C&C DNS Name | ○ Recently Resolved to Unusual IP |
| ○ Recent COVID-19-Related Domain Lure: Malicious | ○ Recently Resolved to Very Malicious IP |
| ○ Recent COVID-19-Related Domain Lure: Suspicious | ○ Trending in Recorded Future Analyst Community |
| ○ Recently Reported as a Defanged DNS Name | ○ Historically Reported Spam or Unwanted Content |
| ○ Recently Reported by DHS AIS | ○ Historical Suspected CANDC DNS Name |
| | ○ Historical Threat Researcher |
| | ○ Historical Typosquat Similarity - DNS Sandwich |
| | ○ Historical Typosquat Similarity - Typo or Homograph |
| | ○ Historical Ukraine-Related Domain Lure |
| | ○ Historically Active Weaponized Domain |

Minimum Risk Score Threshold

The numeric value representing the minimum risk score required to ingest an IOC. The default setting is 50.

Normalize Risk Score

Enable this parameter ingest a normalized risk score value as a scorable attribute.

Risk Score Normalization Mapping

Mapping used to normalize the numeric risk score values to the scorable attribute, `Normalized Risk`. The Risk Score itself will always be ingested. This mapping should contain a line-separated CSV formatted string with the following columns: **Minimum**, **Maximum**, and **Normalized Value**.

PARAMETER	DESCRIPTION
	Default Values 0,25,Low 26,50,Medium 51,75,High 76,100,Critical  This parameter is only accessible if you have enabled the Normalize Risk Score parameter.
Filter Out Entries with No New Evidence	Enabling this option will filter out entries that have no new evidence. A risk list is a rolling list of indicators. As a result, there are entries within the list that may be from days, months, or even years ago. Once the feed runs historically and ingests all the entries, subsequent runs do not need to re-ingest the same entries again if there is no new evidence. Disabling it will re-ingest all entries, with solely the old evidence being filtered out. This parameter is enabled by default.
Enable SSL Verification	Enable this for the feed to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.

< Recorded Future Domain Risk List



Disabled ☐ Enabled ☒

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration

Activity Log

API Key



List To Be Retrieved

Specific Recorded Future list to be retrieved

- ☒ All
- ☐ Historically Reported by Insikt Group
- ☐ Historically Reported Botnet Domain
- ☐ Newly Registered Certificate With Potential for Abuse - DNS Sandwich
- ☐ Newly Registered Certificate With Potential for Abuse - Typo or Homograph
- ☐ C&C Nameserver
- ☐ Historical C&C DNS Name
- ☐ Historical COVID-19-Related Domain Lure
- ☐ Recently Resolved to Host of Many DDNS Names
- ☐ Historically Reported as a Defanged DNS Name
- ☐ Historically Reported by DHS AIS
- ☐ Recent Fast Flux DNS Name
- ☐ Historically Reported Fraudulent Content
- ☐ Frequently Abused Free DNS Provider
- ☐ Historically Reported in Threat List

Recorded Future Vulnerability Risk List Parameters

PARAMETER	DESCRIPTION
API Key	Your API Key to be used in HTTP headers for accessing feed data.
List to be Retrieved	Use the checkboxes provided to select specific Recorded Future lists to be retrieved. Options include: ☐ Historically Reported by Insikt Group ☐ Web Reporting Prior to CVSS Score ☐ Cyber Exploit Signal: Critical ☐ Cyber Exploit Signal: Important ☐ Cyber Exploit Signal: Medium ☐ Historically Exploited in the Wild by Malware ☐ Likely Historical Exploit Development ☐ Linked to Historical Cyber Exploit ☐ Historically Linked to Exploit Kit ☐ Historically Linked to Malware ☐ Historically Linked to Remote Access Trojan ☐ Historically Linked to Ransomware ☐ Linked to Recent Cyber Exploit ☐ Recently Linked to Exploit Kit ☐ Recently Linked to Malware ☐ Recently Linked to Remote Access Trojan ☐ NIST Severity: Low ☐ NIST Severity: Medium ☐ Web Reporting Prior to NVD Disclosure ☐ Historical Unverified Proof of Concept Available ☐ Historical Verified Proof of Concept Available ☐ Historical Verified Proof of Concept Available Using Remote Execution ☐ Recently Reported by Insikt Group ☐ Exploit Likely in Active Development ☐ Exploited in the Wild by Recently Active Malware ☐ Recent Unverified Proof of Concept Available ☐ Recent Verified Proof of Concept Available ☐ Recent Verified Proof of Concept Available Using Remote Execution ☐ Recently Referenced by Insikt Group ☐ Recently Linked to Penetration Testing Tools ☐ Historically Referenced by Insikt Group ☐ Historically Linked to Penetration Testing Tools ☐ Vendor Severity: Critical ☐ Vendor Severity: High ☐ Vendor Severity: Low ☐ Vendor Severity: Medium

PARAMETER	DESCRIPTION
	☐ Recently Linked to Ransomware ☐ Exploited in the Wild by Malware ☐ NIST Severity: Critical ☐ NIST Severity: High
Save CVE Data As	Select whether to ingest CVEs as: Vulnerabilities, Indicators, or Both.  The default setting is to ingest Indicators objects.
Minimum Risk Score Threshold	The numeric value representing the minimum risk score required to ingest an IOC. The default setting is 50.
Normalize Risk Score	Enable this parameter ingest a normalized risk score value as a scorable attribute.
Risk Score Normalization Mapping	Mapping used to normalize the numeric risk score values to the scorable attribute, Normalized Risk. The Risk Score itself will always be ingested. This mapping should contain a line-separated CSV formatted string with the following columns: Minimum, Maximum, and Normalized Value. Default Values <pre>0,25,Low 26,50,Medium 51,75,High 76,100,Critical</pre>  This parameter is only accessible if you have enabled the Normalize Risk Score parameter.
Filter Out Entries with No New Evidence	Enabling this option will filter out entries that have no new evidence. A risk list is a rolling list of indicators. As a result, there are entries within the list that may be from days, months, or even years ago. Once the feed runs historically and ingests all the entries, subsequent runs do not need to re-ingest the same entries again if there is no

PARAMETER	DESCRIPTION
	new evidence. Disabling it will re-ingest all entries, with solely the old evidence being filtered out. This parameter is enabled by default.
Enable SSL Verification	Enable this for the feed to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.

< Recorded Future Vulnerability Risk List



Disabled ☐ Enabled ☒

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration Activity Log

API Key

List To Be Retrieved

Specific recorded future list to be retrieved

- ☐ Historically Reported by Insikt Group
- ☐ Web Reporting Prior to CVSS Score
- ☐ Cyber Exploit Signal: Critical
- ☐ Cyber Exploit Signal: Important
- ☐ Cyber Exploit Signal: Medium
- ☐ Historically Exploited in the Wild by Malware
- ☐ Likely Historical Exploit Development
- ☐ Linked to Historical Cyber Exploit
- ☐ Historically Linked to Exploit Kit
- ☐ Historically Linked to Malware
- ☐ Historically Linked to Remote Access Trojan
- ☐ Historically Linked to Ransomware
- ☐ Linked to Recent Cyber Exploit
- ☐ Recently Linked to Exploit Kit
- ☐ Recently Linked to Malware
- ☐ Recently Linked to Remote Access Trojan
- ☐ Recently Linked to Ransomware
- ☐ Exploited in the Wild by Malware
- ☐ NIST Severity: Critical
- ☐ NIST Severity: High

Recorded Future Hash Risk List Parameters

PARAMETER	DESCRIPTION
API Key	Your API Key to be used in HTTP headers for accessing feed data.
List to be Retrieved	Use the checkboxes provided to select specific Recorded Future lists to be retrieved.  It is highly recommended to use the All option as it will ingest the latest information from Recorded Future. If you are using the All option, confirm that you have unselected the other options. Running the feed with the All option selected along with other individual list options, will cause the feed to fail. This is a known issue and will be addressed in a future release of the integration. You should schedule feed runs hourly or longer when using the All option. Options include: ☐ All (default) ☐ Reported by Insikt Group ☐ Reported by DHS AIS ☐ Historically Reported in Threat List ☐ Linked to Cyber Attack ☐ Linked to Malware ☐ Linked to Attack Vector ☐ Linked to Vulnerability ☐ Malware SSL Certificate Fingerprint ☐ Positive Sandbox Detection on File ☐ No Risk Observed ☐ Observed in Underground Virus Testing Sites ☐ Observed in the Wild by Recorded Future Telemetry ☐ Positive Malware Verdict ☐ Recently Active Targeting Vulnerabilities in the Wild ☐ Referenced by Insikt Group ☐ Trending in Recorded Future Analyst Community ☐ Suspicious Behavior Detected ☐ Threat Researcher
Ingested Hash Types	Select the type of hashes to be ingested into ThreatQ. Options include ☐ MD5 ☐ SHA-1 ☐ SHA-256

PARAMETER	DESCRIPTION
Minimum Risk Score Threshold	The numeric value representing the minimum risk score required to ingest an IOC. The default setting is 50.
Normalize Risk Score	Enable this parameter ingest a normalized risk score value as a scorable attribute.
Risk Score Normalization Mapping	Mapping used to normalize the numeric risk score values to the scorable attribute, <code>Normalized Risk</code>. The Risk Score itself will always be ingested. This mapping should contain a line-separated CSV formatted string with the following columns: Minimum, Maximum, and Normalized Value. Default Values <pre>0,25,Low 26,50,Medium 51,75,High 76,100,Critical</pre>  This parameter is only accessible if you have enabled the Normalize Risk Score parameter.
Filter Out Entries with No New Evidence	Enabling this option will filter out entries that have no new evidence. A risk list is a rolling list of indicators. As a result, there are entries within the list that may be from days, months, or even years ago. Once the feed runs historically and ingests all the entries, subsequent runs do not need to re-ingest the same entries again if there is no new evidence. Disabling it will re-ingest all entries, with solely the old evidence being filtered out. This parameter is enabled by default.
Enable SSL Verification	Enable this for the feed to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.

< Recorded Future Hash Risk List



Disabled ☒ Enabled

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration

Activity Log

API Key



List To Be Retrieved

Specific recorded future list to be retrieved

- ☒ All
- ☐ Reported by Insikt Group
- ☐ Reported by DHS AIS
- ☐ Historically Reported in Threat List
- ☐ Linked to Cyber Attack
- ☐ Linked to Malware
- ☐ Linked to Attack Vector
- ☐ Linked to Vulnerability
- ☐ Malware SSL Certificate Fingerprint
- ☐ Positive Sandbox Detection on File From Underground Virus Testing Sites
- ☐ No Risk Observed
- ☐ Observed in Underground Virus Testing Sites
- ☐ Observed in the Wild by Recorded Future Telemetry
- ☐ Positive Malware Verdict
- ☐ Recently Active Targeting Vulnerabilities in the Wild
- ☐ Referenced by Insikt Group
- ☐ Trending in Recorded Future Analyst Community
- ☐ Suspicious Behavior Detected
- ☐ Threat Researcher

Ingested Hash Types

The hash types to be ingested into ThreatQ.

- ☒ MD5
- ☒ SHA-1
- ☒ SHA-256

Recorded Future IP Risk List Parameters

PARAMETER	DESCRIPTION
API Key	Your API Key to be used in HTTP headers for accessing feed data.
List to be Retrieved	Use the checkboxes provided to select specific Recorded Future lists to be retrieved.  It is highly recommended to use the All option as it will ingest the latest information from Recorded Future. If you are using the All option, confirm that you have unselected the other options. Running the feed with the All option selected along with other individual list options, will cause the feed to fail. This is a known issue and will be addressed in a future release of the integration. You should schedule feed runs hourly or longer when using the All option. Options include: ☐ All (default) ☐ Threat Actor Used Infrastructure ☐ Historically Reported by Insikt Group ☐ Inside Possible Bogus BGP Route ☐ Historical Botnet Traffic ☐ Historical Brute Force ☐ Nameserver for C&C Server ☐ Cyber Exploit Signal: Critical ☐ Cyber Exploit Signal: Important ☐ Cyber Exploit Signal: Medium ☐ Recent Host of Many DDNS Names ☐ Historical DDoS ☐ Historically Reported as a Defanged IP ☐ Historically Reported by DHS AIS ☐ Historical DNS Abuse ☐ Recent DNS Abuse ☐ Recent Honeypot Sighting ☐ Recently Linked to Intrusion Method ☐ Recently Linked to APT ☐ Recently Linked to Cyber Attack ☐ Recent Malicious Infrastructure Admin Server ☐ Recent Malware Delivery ☐ Recent Multicategory Blocklist ☐ Recent Open Proxies ☐ Recent Phishing Host ☐ Recent Positive Malware Verdict ☐ Recently Referenced by Insikt Group ☐ Recently Reported C&C Server ☐ Recently Communicating With Reported C&C Server ☐ Recent Spam Source

PARAMETER

DESCRIPTION

- | | |
|---|--|
| ☐ Resolution of Fast Flux DNS Name | ☐ Recent SSH/Dictionary Attacker |
| ☐ Historically Reported in Threat List | ☐ Recent Bad SSL Association |
| ☐ Historical Honeypot Sighting | ☐ Recent Suspected C&C Server |
| ☐ Honeypot Host | ☐ Recent Threat Researcher |
| ☐ Recently Communicating Validated C&C Server | ☐ Recent Tor Node |
| ☐ Historically Linked to Intrusion Method | ☐ Recent Unusual IP |
| ☐ Historically Linked to APT | ☐ Validated C&C Server |
| ☐ Historically Linked to Cyber Attack | ☐ Recently Communicating With Validated C&C Server |
| ☐ Historical Malicious Infrastructure Admin Server | ☐ Recently Defaced Site |
| ☐ Suspected Malicious Packet Source | ☐ Historically Referenced by Insikt Group |
| ☐ Historical Malware Delivery | ☐ Historically Reported C&C Server |
| ☐ Historical Multicategory Blocklist | ☐ Trending in Recorded Future Analyst Community |
| ☐ Observed in the Wild by Recorded Future Telemetry | ☐ Historical Spam Source |
| ☐ Historical Open Proxies | ☐ Historical SSH/Dictionary Attacker |
| ☐ Historical Phishing Host | ☐ Historical Bad SSL Association |
| ☐ Historical Positive Malware Verdict | ☐ Historical Suspected C&C Server |
| ☐ Recorded Future Predictive Risk Model | ☐ Suspected Phishing Host |
| ☐ Actively Communicating Validated C&C Server | ☐ Historical Threat Researcher |
| ☐ Recently Reported by Insikt Group | ☐ Tor Node |
| ☐ Recent Botnet Traffic | ☐ Unusual IP |
| ☐ Recent Brute Force | ☐ Previously Validated C&C Server |
| ☐ Recent DDoS | ☐ Vulnerable Host |
| ☐ Recently Reported as a Defanged IP | ☐ Observed High-Impact Vulnerability |
| ☐ Recently Reported by DHS AIS | |

Save CVE Data
As

Select whether to ingest CVEs as: Vulnerabilities, Indicators, or Both.



The default setting is to ingest Indicators objects.

PARAMETER	DESCRIPTION
Minimum Risk Score Threshold	The numeric value representing the minimum risk score required to ingest an IOC. The default setting is 50.
Normalize Risk Score	Enable this parameter ingest a normalized risk score value as a scorable attribute.
Risk Score Normalization Mapping	Mapping used to normalize the numeric risk score values to the scorable attribute, <code>Normalized Risk</code>. The Risk Score itself will always be ingested. This mapping should contain a line-separated CSV formatted string with the following columns: Minimum, Maximum, and Normalized Value. Default Values <pre>0,25,Low 26,50,Medium 51,75,High 76,100,Critical</pre>  This parameter is only accessible if you have enabled the Normalize Risk Score parameter.
Filter Out Entries with No New Evidence	Enabling this option will filter out entries that have no new evidence. A risk list is a rolling list of indicators. As a result, there are entries within the list that may be from days, months, or even years ago. Once the feed runs historically and ingests all the entries, subsequent runs do not need to re-ingest the same entries again if there is no new evidence. Disabling it will re-ingest all entries, with solely the old evidence being filtered out. This parameter is enabled by default.
Enable SSL Verification	Enable this for the feed to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.

< Recorded Future IP Risk List



Disabled ☒ Enabled

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration

Activity Log

API Key



List To Be Retrieved

Specific recorded future list to be retrieved

- ☒ All
- ☐ Threat Actor Used Infrastructure
- ☐ Historically Reported by Insikt Group
- ☐ Inside Possible Bogus BGP Route
- ☐ Historical Botnet Traffic
- ☐ Historical Brute Force
- ☐ Nameserver for C&C Server
- ☐ Cyber Exploit Signal: Critical
- ☐ Cyber Exploit Signal: Important
- ☐ Cyber Exploit Signal: Medium
- ☐ Recent Host of Many DDNS Names
- ☐ Historical DDoS

Recorded Future URL Risk List Parameters

PARAMETER	DESCRIPTION
API Key	Your API Key to be used in HTTP headers for accessing feed data.
List to be Retrieved	Use the checkboxes provided to select specific Recorded Future lists to be retrieved.  It is highly recommended to use the All option as it will ingest the latest information from Recorded Future. If you are using the All option, confirm that you have unselected the other options. Running the feed with the All option selected along with other individual list options, will cause the feed to fail. This is a known issue and will be addressed in a future release of the integration. You should schedule feed runs hourly or longer when using the All option. Options include: ☐ All (default) ☐ Historically Reported by Insikt Group ☐ Historically Reported Botnet URL ☐ Historical C&C URL ☐ Historically Reported as a Defanged URL ☐ Historically Reported by DHS AIS ☐ Historically Reported Fraudulent Content ☐ Historically Reported in Threat List ☐ Historically Detected Malware Distribution ☐ Historically Suspected Malware Distribution ☐ Historically Detected Cryptocurrency Mining Techniques ☐ Recently Reported as a Defanged URL ☐ Recently Reported by DHS AIS ☐ Recently Reported Fraudulent Content ☐ Recently Detected Malware Distribution ☐ Recently Suspected Malware Distribution ☐ Recently Detected Cryptocurrency Mining Techniques ☐ Recently Detected Phishing Techniques ☐ Recently Suspected Phishing Techniques ☐ Recent Web Filter Avoidance Proxy URL

PARAMETER	DESCRIPTION
	○ No Risk Observed ○ Observed in the Wild by Recorded Future Telemetry ○ Historically Detected Phishing Techniques ○ Historically Suspected Phishing Techniques ○ Historically Detected Web Filter Avoidance Proxy URL ○ Recently Reported by Insikt Group ○ Recently Reported Botnet URL ○ Recent C&C URL ○ Recently Referenced by Insikt Group ○ Recent Reported C&C URL ○ Recently Reported Spam or Unwanted Content ○ Recent Suspected C&C URL ○ Recently Active URL on Weaponized Domain ○ Historically Referenced by Insikt Group ○ Historical Reported C&C URL ○ Historically Reported Spam or Unwanted Content ○ Historical Suspected C&C URL
Save CVE Data As	Select whether to ingest CVEs as: Vulnerabilities, Indicators, or Both.  The default setting is to ingest Indicators objects.
Minimum Risk Score Threshold	The numeric value representing the minimum risk score required to ingest an IOC. The default setting is 50.
Normalize Risk Score	Enable this parameter ingest a normalized risk score value as a scorable attribute.
Risk Score Normalization Mapping	Mapping used to normalize the numeric risk score values to the scorable attribute, Normalized Risk. The Risk Score itself will always be ingested. This mapping should contain a line-separated CSV formatted string with the following columns: Minimum, Maximum, and Normalized Value. Default Values <pre>0,25,Low 26,50,Medium 51,75,High 76,100,Critical</pre>

PARAMETER

DESCRIPTION



This parameter is only accessible if you have enabled the **Normalize Risk Score** parameter.

Filter Out Entries with No New Evidence

Enabling this option will filter out entries that have no new evidence. A risk list is a rolling list of indicators. As a result, there are entries within the list that may be from days, months, or even years ago. Once the feed runs historically and ingests all the entries, subsequent runs do not need to re-ingest the same entries again if there is no new evidence. Disabling it will re-ingest all entries, with solely the old evidence being filtered out. This parameter is enabled by default.

Enable SSL Verification

Enable this for the feed to validate the host-provided SSL certificate.

Disable Proxies

Enable this option if the feed should not honor proxies set in the ThreatQ UI.

< Recorded Future URL Risk List



Disabled ☐ Enabled ☒

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration

Activity Log

API Key



List To Be Retrieved

Specific recorded future list to be retrieved

- ☒ All
- ☐ Historically Reported by Insikt Group
- ☐ Historically Reported Botnet URL
- ☐ Historical C&C URL
- ☐ Historically Reported as a Defanged URL
- ☐ Historically Reported by DHS AIS
- ☐ Historically Reported Fraudulent Content
- ☐ Historically Reported in Threat List
- ☐ Historically Detected Malware Distribution
- ☐ Historically Suspected Malware Distribution
- ☐ Historically Detected Cryptocurrency Mining Techniques
- ☐ No Risk Observed
- ☐ Observed in the Wild by Recorded Future Telemetry
- ☐ Historically Detected Phishing Techniques

Recorded Future Analyst Note Parameters

PARAMETER	DESCRIPTION
API Key	Your API Key to be used in HTTP headers for accessing feed data.
Entity	A string to search for notes by entity ID.
Author	A string to search for notes by author ID.
Title	A string to search for notes by title.
Topic	A string to search for notes by topic ID. The options for this user field are: • Actor Profile • Analyst On-Demand Report • Cyber Threat Analysis • Flash Report • Geopolitical Intelligence Summary • Geopolitical Flash Event • Geopolitical Threat Forecast • Geopolitical Validated Event • Hunting Package • Indicator • Insikt Research Lead • Informational • Malware/Tool Profile • Regular Vendor Vulnerability Disclosures • Sigma Rule • SNORT Rule • Source Profile • The Record by Recorded Future • Threat Lead • TTP Instance • Validated Intelligence Event • Weekly Threat Landscape • YARA Rule
Label	A string that helps searching for notes by label, by name.
Source	A string that helps sorting by the source of note. The options for this user field will be: ○ Insikt Group ○ ThreatQuotient - Partner Notes

PARAMETER	DESCRIPTION
Tagged Text	Select whether the text should contain tags or not. Possible values are: ○ True ○ False
Ingest CVEs As	Select which ThreatQ entity type to ingest CVE values as. Options include Vulnerabilities (default) and Indicators .
Ingest Selected Primary Entities as Indicators	Select which entity types to ingest as indicators of compromise into ThreatQ. Options include: ○ URLs (default) ○ Internet Domain Names (default) ○ IP Addresses (default) ○ Hashes (default) ○ Email Addresses (default) ○ Usernames ○ Filenames  This will only ingest the selected types from the "primary" entities (note_entities), and not the "supporting" entities (context_entities). This is so we can reduce the amount of false positives being ingested into the platform. Even if you do not select any of these, they will still be included in the description of the note.
Ingest Selected Supporting Entities as Indicators	Select which entity types to ingest as indicators of compromise into ThreatQ. Options include: ○ Internet Domain Names ○ IP Addresses ○ Hashes ○ Email Addresses ○ Usernames ○ Filenames  This will only enable the ingestion of the selected types from the "supporting" entities (context_entities), and not the "primary" entities (note_entities). ThreatQuotient does not recommend enabling option due to the high likelihood of false positives. Even if you do not select any of these, they will still be included in the description of the note.

PARAMETER

DESCRIPTION

Ingested Hash Types

Select the type of hashes to be ingested into ThreatQ. Options include

- MD5
- SHA-1
- SHA-256

Limit

The maximum number of records per request. This will be used in the pagination.

Enable SSL Verification

Enable this for the feed to validate the host-provided SSL certificate.

Disable Proxies

Enable this option if the feed should not honor proxies set in the ThreatQ UI.

< Recorded Future Analyst Note



Disabled ☒ Enabled

Run Integration

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration

Activity Log

API Key



Entity (Optional)

Filter by Report Entity ID

Author (Optional)

Filter by Report Author ID

Title (Optional)

Filter by Report Title

Topic (Optional)

Notes by Report Topic ID

Label (Optional)

Filter by Report Label Name

Source (Optional)

Filter by Report Source

☐ Tagged Text (Optional)

Select whether the text should contain tags or not.

Ingest CVEs As

Vulnerabilities

Select which ThreatQ entity type to ingest CVE values as.

Recorded Future Alerts Parameters

PARAMETER	DESCRIPTION
API Key	Your API Key to be used in HTTP headers for accessing feed data.
Triggered	A string to search for events from a specific date (YYYY-MM-DD or YYYY-MM or YYYY).
Review Status	A string to search for events by status (Unassigned, Assigned, No Action and Tuning). If no specific status is selected, all event statuses are returned by the provider.
Freetext Search	A string to search for events by any value.
Save CVE Data as	Select whether to ingest CVEs as: Vulnerabilities or Indicators.
Ingested Hash Types	Select the type of hashes to be ingested into ThreatQ. Options include ○ MD5 ○ SHA-1 ○ SHA-256
Enable SSL Verification	Enable this for the feed to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.

< Recorded Future Alerts



Disabled ☒ Enabled

Run Integration

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration Activity Log

API Key

.....



Triggered

Get events from a specific date (YYYY-MM-DD or YYYY-MM or YYYY) (Optional)

Review Status

Review Status (Optional)

Fretext Search

Fretext search for events by any value (Optional)

Save CVE Data As

ThreatQuotient maps CVE data as CVE indicators by default.

- ☒ Indicators
- ☐ Vulnerabilities

Ingested Hash Types

The hash types to be ingested into ThreatQ.

- ☒ MD5
- ☒ SHA-1
- ☒ SHA-256

Recorded Future Playbook Alerts Parameters

PARAMETER	DESCRIPTION
API Key	Your API Key to be used in HTTP headers for accessing feed data.
Filter By	The date that will be used for filtering the alerts: Creation or Update time of the Playbook Alert.
Statuses	The Status of the Playbook Alert. Options include: ○ New ○ In Progress ○ Dismissed ○ Resolved
Priority	The Priority of the Playbook Alert. Options include: ○ High Priority ○ Moderate Priority ○ Priority Informational
Normalize Risk Score	Enable this parameter ingest a normalized risk score value as a scorable attribute.
Risk Score Normalization Mapping	Mapping used to normalize the numeric risk score values to the scorable attribute, <code>Normalized Risk</code>. The Risk Score itself will always be ingested. This mapping should contain a line-separated CSV formatted string with the following columns: Minimum, Maximum, and Normalized Value. Default Values <pre>0,25,Low 26,50,Medium 51,75,High 76,100,Critical</pre>  This parameter is only accessible if you have enabled the Normalize Risk Score parameter.

PARAMETER	DESCRIPTION
Enable SSL Verification	Enable this for the feed to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.

< Recorded Future Playbook Alerts



Disabled ☒ Enabled

Run Integration

Uninstall

Additional Information
Integration Type: Feed
Version:

Configuration
Activity Log

API Key

Filter By
Creation time of the Playbook Alert

Statuses
The Status of the Playbook Alert
☒ New
☒ In Progress
☒ Dismissed
☒ Resolved

Priority
The Priority of the Playbook Alert
☒ High priority
☒ Moderate priority
☒ Priority Informational

Recorded Future Fusion Files Parameters

PARAMETER	DESCRIPTION
API Key	Your API Key to be used in HTTP headers for accessing feed data.
Selected Fusion Feeds	Select the Fusion Files to be retrieved. Options include: ○ Command and Control IPs ○ Known TOR IPs ○ Active RAT C2 IPs ○ Fast Flux IPs ○ Dynamic DNS IPs ○ Potentially Undetectable Malware ○ Weaponized Domains ○ Exploits in the Wild Hashes
Ingest Related Malware	Enabling this will ingest Malware related to indicators in the feeds.  It is important to note that over time, this may create a large number of relationships between indicators and malware.
Ingest Related CVEs	Optional - Enabling this will ingest CVEs related to indicators in the feeds.  This parameter only applies to the <code>Exploits in the Wild</code> feed and is disabled by default due to the large number of CVE relationships that may be created when enabled. Exercise caution when enabled this parameter.
Ingest CVEs As	Select whether to ingest CVEs as Vulnerabilities (default) or Indicators.
Enable SSL Verification	Enable this for the feed to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.

Recorded Future Fusion Files



Disabled ☒ Enabled

Run Integration

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration Activity Log

API Key

Selected Fusion Feeds

- ☐ Command and Control IPs
- ☐ Known TOR IPs
- ☐ Active RAT C2 IPs
- ☒ Fast Flux IPs
- ☐ Dynamic DNS IPs
- ☐ Potentially Undetectable Malware
- ☐ Weaponized Domains
- ☐ Exploits in the Wild Hashes

- ☒ **Ingest Related Malware**
Enabling this will ingest Malware related to indicators in the feeds. Keep in mind that over time, this may create a large number of relationships between indicators and malware.
- ☒ **Ingest Related CVEs**
Enabling this will ingest CVEs related to indicators in the feeds. This only applies to the "Exploits in the Wild" feed. It is optional and off by default due to the large number of CVL relationships that may be created when enabled. Use with caution.

- Ingest CVEs As - Vulnerabilities

Select which ThreatQ entity type to ingest CVE values as.

5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

Recorded Future Domain Risk List

The data on this feed comes in form of a CSV list. The first token is the actual risk data (domain), and the last token (EvidenceDetails) contains supporting context. This token is a JSON-formatted string of an array of dictionaries.

GET <https://api.recordedfuture.com/v2/domain/risklist>

Sample Response:

```
'ns513726.ip-192-99-148.net', '92', '3/32',
'{"EvidenceDetails":
  [
    {
      "CriticalityLabel": "Unusual",
      "Rule": "Historical Malware Analysis DNS Name",
      "EvidenceString": "6 sightings on 1 source: VirusTotal...",
      "Timestamp": "2015-04-04T00:00:00.000Z",
      "Criticality": 1
    },
    {
      "CriticalityLabel": "Suspicious",
      "Rule": "Blacklisted DNS Name",
      "EvidenceString": "1 sighting on 1 source: DShield: Suspicious
Domain List.",
      "Timestamp": "2018-12-26T07:12:00.936Z",
      "Criticality": 2
    },
    {
      "CriticalityLabel": "Very Malicious",
      "Rule": "C&C DNS Name",
      "EvidenceString": "1 sighting on 1 source: Abuse.ch: Zeus Domain
Blocklist (Standard).",
      "Timestamp": "2018-12-26T07:12:00.936Z",
      "Criticality": 4
    }
  ]
}'
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
0 (first token)	Indicator.Value	FQDN	N/A	ns513726.ip-192-99-148.net	N/A
1 (second token)	Indicator.Attribute	Risk Score	N/A	66	Updatable
1 (second token)	Indicator.Attribute	Normalized Risk	N/A	High	Mapped using Risk Score Normalization Mapping user field; Updatable
2 (third token)	Indicator.Attribute	Risk String	N/A	2/32	Updatable
3 (fourth token) [].CriticalityLabel	Indicator.Attribute	Criticality	3 (fourth token) [].Timestamp	Suspicious	Updatable
3 (fourth token) [].Rule	Indicator.Attribute	Associated Rule	3 (fourth token) [].Timestamp	Blacklisted DNS Name	N/A
3 (fourth token) [].EvidenceString	Indicator.Attribute	Evidence	3 (fourth token) [].Timestamp	1 sighting on 1 source: Abuse.ch: Zeus Domain Blocklist (Standard).	N/A

Recorded Future IP Risk List

Similar to the above feed, this feed gets IP addresses as indicators.

GET <https://api.recordedfuture.com/v2/ip/risklist>

Sample Response:

```
'5.120.187.119', '65', '1/49',
{'EvidenceDetails':
  [
    {
      "CriticalityLabel": "Malicious",
      "Rule": "Recent Positive Malware Verdict",
      "EvidenceString": "1 sighting on 1 source: ReversingLabs....",
      "Timestamp": "2018-11-22T00:00:00.000Z",
      "Criticality": 3
    }
  ]
}'
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
0 (first token)	Indicator.Value	IP Address	N/A	5.120.187.119	N/A
1 (second token)	Indicator.Attribute	Risk Score	N/A	65	Updatable
1 (second token)	Indicator.Attribute	Normalized Risk	N/A	High	Mapped using Risk Score Normalization Mapping user field; Updatable
2 (third token)	Indicator.Attribute	Risk String	N/A	1/49	Updatable
3 (fourth token) [.CriticalityLabel]	Indicator.Attribute	Criticality	3 (fourth token) [.Timestamp]	Malicious	Updatable
3 (fourth token) [.Rule]	Indicator.Attribute	Associated Rule	3 (fourth token) [.Timestamp]	Recent Positive Malware Verdict	N/A
3 (fourth token) [.EvidenceString]	Indicator.Attribute	Evidence	3 (fourth token) [.Timestamp]	1 sighting on 1 source: ReversingLabs.	N/A

Recorded Future URL Risk List

Similar to the above feeds, this feed gets URLs as indicators.

GET <https://api.recordedfuture.com/v2/url/risklist>

Sample Response:

```
'http://handle.booktobi.com/css/index.html', '65', '1/7',
{'EvidenceDetails':
  [
    {
      "CriticalityLabel": "Malicious",
      "Rule": "Active Phishing URL",
      "EvidenceString": "1 sighting on 1 source: PhishTank: Phishing
Reports.",
      "Timestamp": "2018-12-26T16:15:44.750Z",
      "Criticality": 3
    }
  ]
}'
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
0 (first token)	Indicator.Value	URL	N/A	http://handle.booktobi.com/css/index.html	N/A
1 (second token)	Indicator.Attribute	Risk Score	N/A	65	Updatable
1 (second token)	Indicator.Attribute	Normalized Risk	N/A	High	Mapped using Risk Score Normalization Mapping user field; Updatable
2 (third token)	Indicator.Attribute	Risk String	N/A	1/7	Updatable
3 (fourth token) [].CriticalityLabel	Indicator.Attribute	Criticality	3 (fourth token) [].Timestamp	Malicious	Updatable
3 (fourth token) [].Rule	Indicator.Attribute	Associated Rule	3 (fourth token) [].Timestamp	Active Phishing URL	N/A
3 (fourth token) [].EvidenceString	Indicator.Attribute	Evidence	3 (fourth token) [].Timestamp	1 sighting on 1 source: PhishTank: Phishing Reports.	N/A

Recorded Future Vulnerability Risk List

Similar to the above feeds, this feed gets CVEs.

GET <https://api.recordedfuture.com/v2/vulnerability/risklist>

Sample Response:

```
'CVE-2018-0802', '89', '11/18',
{'EvidenceDetails':
  [
    {
      "CriticalityLabel": "Low",
      "Rule": "Linked to Historical Cyber Exploit",
      "EvidenceString": "4281 sightings on 351 sources including: ...",
      "Timestamp": "2018-11-14T22:31:30.000Z",
      "Criticality": 1
    },
    {
      "CriticalityLabel": "Low",
      "Rule": "Historically Linked to Penetration Testing Tools",
      "EvidenceString": "1 sighting on 1 source: @DTechCloud...",
      "Timestamp": "2018-05-07T20:31:29.000Z", "Criticality": 1
    }
  ]
}'
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
0 (first token)	Indicator.Value/ Vulnerability.Value	CVE/N/A	N/A	CVE-2018-0802	N/A
1 (second token)	Indicator.Attribute/ Vulnerability.Attribute	Risk Score	N/A	89	Updatable
1 (second token)	Indicator.Attribute	Normalized Risk	N/A	High	Mapped using Risk Score Normalization Mapping user field; Updatable
2 (third token)	Indicator.Attribute/ Vulnerability.Attribute	Risk String	N/A	11/18	Updatable
3 (fourth token) [].CriticalityLabel	Indicator.Attribute/ Vulnerability.Attribute	Criticality	3 (fourth token) [].Timestamp	Low	Updatable
3 (fourth token) [].Rule	Indicator.Attribute/ Vulnerability.Attribute	Associated Rule	3 (fourth token) [].TimeStamp	Linked to Historical Cyber Exploit	N/A
3 (fourth token) [].EvidenceString	Indicator.Attribute/ Vulnerability.Attribute	Evidence	3 (fourth token) [].Timestamp	1 sighting on 1 source: @DTechCloud...	N/A

Recorded Future Hash Risk List

Similar to the above feeds, this feed gets Hashes.

GET <https://api.recordedfuture.com/v2/hash/risklist>

Sample Response:

```
'ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa', 'SHA-256',
'89', '4/10',
{'EvidenceDetails':
  [
    {
      "CriticalityLabel": "Unusual",
      "Rule": "Threat Researcher",
      "EvidenceString": "21 sightings on 9 sources including: ...",
      "Timestamp": "2018-01-28T11:24:35.942Z",
      "Criticality": 1.0
    },
    {
      "CriticalityLabel": "Suspicious",
      "Rule": "Linked to Vulnerability",
      "EvidenceString": "5 sightings on 2 sources: ...",
      "Timestamp": "2017-08-08T14:10:11.410Z",
      "Criticality": 2
    },
    {
      "CriticalityLabel": "Suspicious",
      "Rule": "Linked to Malware",
      "EvidenceString": "Previous sightings on 36 sources
including: ...",
      "Timestamp": "2017-05-12T15:39:30.000Z",
      "Criticality": 2
    }
  ]
}'
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
0 (first token)	Indicator.Value	1 (second token)	N/A	00d48afbba5ef9ead b572730b2d0cafa	N/A
2 (third token)	Indicator.Attribute	Risk Score	N/A	89	Updatable
2 (third token)	Indicator.Attribute	Normalized Risk	N/A	High	Mapped using Risk Score Normalization Mapping user field; Updatable
3 (fourth token)	Indicator.Attribute	Risk String	N/A	4/10	Updatable
4 (fifth token) [].CriticalityLabel	Indicator.Attribute	Criticality	4 (fifth token) [].Timestamp	Suspicious	Updatable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
4 (fifth token) [].Rule	Indicator.Attribute	Associated Rule	4 (fifth token) [].Timestamp	Linked to Malware	N/A
4 (fifth token) [].EvidenceString	Indicator.Attribute	Evidence	4 (fifth token) [].Timestamp	Previous sightings on 36 sources including: ...	N/A

Recorded Future Analyst Note

This feed gets Reports, Indicators and Attack Patterns. The data sample and mapping are below:

GET <https://api.recordedfuture.com/v2/analystnote/search>

Sample Response:

```
{
  "data": {
    "results": [
      {
        "source": {
          "id": "VKz42X",
          "name": "Insikt Group",
          "type": "Source"
        },
        "attributes": {
          "validated_on": "2020-02-06T06:59:32.784Z",
          "published": "2020-02-06T06:59:32.784Z",
          "text": "some text",
          "topic": [
            {
              "id": "TXSFt0",
              "name": "Flash Report",
              "type": "Topic"
            }
          ],
          "title": "Mailto Ransomware Targets Enterprise Networks",
          "note_entities": [
            {
              "id": "bLfMiL",
              "name": "Mailto Ransomware",
              "type": "Malware"
            }
          ],
          "context_entities": [
            {
              "id": "J6Uzb0",
              "name": "Bleeping Computer",
              "type": "Source"
            }
          ],
          "validation_urls": [
            {
              "id": "url:url:https://www.bleepingcomputer.com/news/security/mailto-netwalker-ransomware-targets-enterprise-networks/",
              "name": "url:https://www.bleepingcomputer.com/news/security/mailto-netwalker-ransomware-targets-enterprise-networks/",
              "type": "URL"
            }
          ]
        }
      }
    ]
  }
}
```

```

    },
    {
      "id": "url:url:https://twitter.com/VK_Intel/status/
1225086186445733889?s=20",
      "name": "url:https://twitter.com/VK_Intel/status/
1225086186445733889?s=20",
      "type": "URL"
    }
  ]
},
{id": "cu1WGK"
}
]
},
"counts": {
  "returned": 10,
  "total": 19216
}
}

```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.data.results[].attributes.title	Report.Name	Report	"Mailto Ransomware Targets Enterprise Networks"	N/A
.data.results[].attributes.published	Report.Published_at	N/A	"2020-02-06T06:59:32.784Z"	This date will also be used for related indicators and attack patterns.
.data.results[].attributes.text	Report.Description	Description	"text"	N/A
.data.results[].source.name	Report.Attribute	Recorded Future Source	"Insikt Group"	N/A
.data.results[].attributes.topic[].name	Report.Attribute	Topic Name	"Flash Report"	N/A
.data.results[].attributes.validated_on	Report.Attribute	Validated On	"2020-02-06T06:59:32.784Z"	Attribute updated if already exists.
.data.results[].attributes.context_entities	N/A	N/A	N/A	*See entities mapping.
.data.results[].attributes.note_entities	N/A	N/A	N/A	*See entities mapping.

Entities Mapping

This mapping will be used to map both values from `context_entities` and `note_entities`. The data sample and mapping are below:

Sample Response:

```
{
  "context_entities": [
    {
      "id": "J6Uzb0",
      "name": "Bleeping Computer",
      "type": "Source",
      "description": "some description"
    }
  ]
}
```

```
indicator_type_map:
  InternetDomainName: FQDN
  URL: URL
  IpAddress: IP Address
  EmailAddress: Email Address
  FileName: Filename
  Username: Username
  Hash: MD5, SHA-1, SHA-256
  CyberVulnerability: CVE
```

The integration will filter based by type. If the value of the `type` key is contained in the `indicator_type_map` below or is equal to Hash, an indicator will be ingested (the `published_at` date will be the same as for the report object). If the `type` key is equal to Malware, an object of type Malware type will be ingested. If the `type` key is equal to MitreAttackIdentifier, an object of Attack Pattern type will be ingested. Else, attributes will be created for the main report object.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.name	Report.Attribute/ Indicator.Attribute	.type	N/A	*See the Event Attributes Mapping table . If type is Product and there are related vulnerabilities, change the Product attribute key to Affected Product
.text	Report.Attribute	.description	N/A	N/A
.name	Indicator.Value	.type	98.123.54.12	IOC is enabled Ingest Selected Primary Entities as Indicators or Ingest Selected Supporting Entities as Indicators
.type	Indicator.Type	.name	Ip Address	The value for this will be <code>indicator_type_map[.type]</code> if it exists there. If the value is Hash, the value length will be analyzed and based on it it will be either MD5, SHA-1, or SHA-256.
.name	Adversary.Value	N/A	N/A	If .type is Organization

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.name	Adversary.Attribute	Category	"Bleeping Computer"	If .type is CyberThreatActorCategory
.name	Identity.Value	N/A	john.doe@acme.com	We ingest the Email Address as a Identity from "supporting" entities
.name	Attack Pattern.Value	N/A	T1023 - MITRE Technique Name	If type is equal to MitreAttackIdentifier
.name	Malware.Value	N/A	Mailto Ransomware	If .type is equal to Malware
.name	Malware.Attribute	Category	N/A	If .type id equal to MalwareCategory
.name	Vulnerability.Value	N/A	N/A	If the .type is equal to CyberVulnerability
.name	Vulnerability.Attribute/Indicator.Attribute	Affected Product	Citrix	Object type is based on Ingest CVEs As selection



Context (i.e. Malware, Adversaries, Attributes, and Attack Patterns) from the "primary" entities list will now be applied to the indicators of compromise from the "primary" entities list.

Recorded Future Alerts

The Alerts feed retrieves Alerts from the provider.

GET <https://api.recordedfuture.com/v3/alert/>

Sample Response:

```
{
  "data": [
    {
      "review": {
        "note": null,
        "status_in_portal": "New",
        "assignee": null,
        "status": "no-action"
      },
      "owner_organisation_details": {
        "organisations": [
          {
            "organisation_id": "uhash:ER135KQ6oL",
            "organisation_name": "ThreatQ - Partner"
          }
        ],
        "enterprise_id": "uhash:DimzHe41vx",
        "enterprise_name": "ThreatQ - Partner"
      },
      "url": {
        "api": "https://api.recordedfuture.com/v3/alerts/rj540x",
        "portal": "https://app.recordedfuture.com/live/sc/notification/?id=rj540x"
      },
      "rule": {
        "name": "Cyber Espionage, Related Vulnerabilities",
        "id": "nt4XZZ",
        "url": {
          "portal": "https://app.recordedfuture.com/live/sc/ViewIdkobra_view_report_item_alert_editor?view_opts=%7B%22reportId%22%3A%22nt4XZZ%22%2C%22bTitle%22%3Atrue%2C%22title%22%3A%22Cyber+Espionage%2C+Related+Vulnerabilities%22%7D"
        }
      },
      "id": "rj540x",
      "hits": [
        {
          "entities": [
            {
              "id": "B_HE4",
              "name": "Google",
              "type": "Company"
            },
            {
              "id": "idn:reuters.com",
              "name": "reuters.com",
              "type": "InternetDomainName"
            },
            {
              "id": "Xw2PY",
              "name": "Frankfurt",
              "type": "Airport"
            },
            {
              "id": "rVnb7k",
```

```

        "name": "Rhysida",
        "type": "Malware"
    },
    {
        "id": "J0Nl-p",
        "name": "Ransomware",
        "type": "MalwareCategory"
    },
    {
        "id": "K_4o-y",
        "name": "Anonymous Sudan",
        "type": "Organization"
    },
    {
        "id": "I_7J4G",
        "name": "Hacktivist",
        "type": "CyberThreatActorCategory"
    },
    {
        "id": "mitre:T1048",
        "name": "T1048",
        "type": "MitreAttackIdentifier"
    },
    {
        "id": "email:mary.silverstein@delta.com",
        "name": "mary.silverstein@delta.com",
        "type": "EmailAddress"
    },
    {
        "id": "jc5TL-",
        "name": "ProxyShell",
        "type": "CyberVulnerability",
        "description": "ProxyShell and Log4J Vulnerabilities Were the Most Exploited Flaws in
2021."
    }
],
"document": {
    "source": {
        "id": "source:hPTFPY",
        "name": "RedAlert | Blog",
        "type": "Source"
    },
    "title": "2022 Activities Summary of SectorA groups (ENG)",
    "url": "https://redalert.nshc.net/2023/06/08/2022-activities-summary-of-sectora-groups-
eng/",
    "authors": []
},
"fragment": "In this operation, the group targeted engineering companies in the <e
id=0qjp>energy</e> and military sectors and damaged their systems by <i id=HE-xwAAZh-v>exploiting
the <e id=kvXvR5>Log4Shell</e></i> vulnerability with an initial infiltration method.",
    "id": "HE-xwAAZh-v",
    "language": "eng",
    "primary_entity": {
        "id": "kvXvR5",
        "name": "CVE-2021-44228",
        "type": "CyberVulnerability",
        "description": "Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases
2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not
protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can
control log messages or log message parameters can execute arbitrary code loaded from LDAP servers
when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by
default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been
completely removed. Note that this vulnerability is specific to log4j-core and does not affect
log4net, log4cxx, or other Apache Logging Services projects."
    }
}

```

```

    },
    "analyst_note": null
  }
],
"ai_insights": {
  "comment": "The Recorded Future AI requires more references in order to produce a summary.",
  "text": null
},
"log": {
  "note_author": null,
  "note_date": null,
  "status_date": null,
  "triggered": "2023-06-08T04:53:13.444Z",
  "status_change_by": null
},
"title": "Cyber Espionage, Related Vulnerabilities - Rise: CVE-2021-44228",
"type": "ENTITY"
}
],
"counts": {
  "returned": 10,
  "total": 2653
}
}

```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].title	Event.Title	N/A	.data[].log.note_date / .data[].log.triggered	Cyber Espionage, Related Vulnerabilities - Rise: CVE-2021-44228	If .data[].log.note _date is not present .data[].log.trig gered is used as Published Date
.data[].log. triggered	Event.Happened_ at	N/A	N/A	2023-06-08T04:53: 13.444Z	N/A
.data[].ai_ insights.text	Event.Description	N/A	N/A	N/A	N/A
.data[].ai_ insights. comment	Event.Description	N/A	N/A	The Recorded Future AI requires more references in order to produce a summary.	N/A
.data[].review. assignee	Event.Attribute	Assignee	.data[].log.note_date / .data[].log.triggered	N/A	If the attribute already exists, the value will be updated.
.data[].log.note_ author	Event.Attribute	Note Author	.data[].log.note_date / .data[].log.triggered	N/A	N/A
.data[].review.status_ in_portal	Event.Attribute	Alert Status	.data[].log.note_date / .data[].log.triggered	no-action	If the attribute already exists, the value will be updated.
.data[].rule.name	Event.Attribute	Triggered Rule Name	.data[].log.note_date / .data[].log.triggered	Cyber Espionage, Related Vulnerabilities	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].type	Event.Attribute	Alert Type	.data[].log.note_date / .data[].log.triggered	ENTITY	N/A
.data[].owner_organisation_details.enterprise_name	Event.Attribute	Organisation Enterprise name	.data[].log.note_date / .data[].log.triggered	ThreatQ - Partner	N/A
.data[].hits[].document.url	Event.Attribute	URL	N/A	https://www.virustotal.com/84387248326473645	Ingested as attribute if 'www.virustotal.com' in .url
.data[].hits[].entities[].name	Event.Tags	N/A	N/A	ddosattacks	If data.hits[].entities[].type is Hashtag, Character # is removed.
.data[].hits[].entities[].name	Indicator.Value	data.hits[].entities[].type	N/A	N/A	See Related Indicator Type Mapping table below.
.data[].hits[].entities[].name	Event.Attribute	data.hits[].entities[].type	N/A	N/A	See Event Attributes Mapping table below.
.data[].hits[].entities[].name	Related.Malware.Value	N/A	N/A	Rhysida	If data.hits[].entities[].type is Malware
.data[].hits[].entities[].name	Related.Malware.Attribute	Malware Category	N/A	Ransomware	If data.hits[].entities[].type is MalwareCategory
.data[].hits[].entities[].name	Event.Attribute	Malware Category	N/A	Ransomware	If data.hits[].entities[].type is MalwareCategory
.data[].hits[].entities[].name	Event.Attribute	Organization	N/A	Anonymous Sudan	If data.hits[].entities[].type is Organization and it is not an Adversary
.data[].hits[].entities[].name	Related.Adversary.Value	N/A	N/A	Anonymous Sudan	If data.hits[].entities[].type is Organization
.data[].hits[].entities[].type	Related.Adversary.Attribute	Type	N/A	Organization	If data.hits[].entities[].type is Organization
.data[].hits[].entities[].name	Related.Adversary.Tags	N/A	N/A	Hacktivist	If data.hits[].entities[].type is CyberThreatActor Category

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].hits[].entities[].name	Event.Attribute	Cyber Threat Actor Category	N/A	Hacktivist	If data.hits[].entities[].type is CyberThreatActor Category
.data[].hits[].entities[].name	Related.Attack Patten.Value	N/A	N/A	T1048	If data.hits[].entities[].type is MitreAttackIdentifier
.data[].hits[].entities[].name	Related.Vulnerability.Value	N/A	N/A	ProxyShell	If data.hits[].entities[].type is CyberVulnerability or user config Save CVE Data as contains Vulnerabilities
.data[].hits[].entities[].name	Related.Identity.Value	N/A	N/A	mary.silverstein@delta.com	If data.hits[].entities[].type is EmailAddress



In the previous table, there is a Related Indicator that is set dynamically. This is because the ThreatQ Object Type is extracted from the same path `.data.hits[].entities[].type` if the `.data.hits[].entities[].type` is one from the Related Indicator Type Mapping table listed below.

Related Indicator Type Mapping

RECORDED FUTURE INDICATOR TYPE	THREATQ INDICATOR TYPE	NOTES
Hash	MD5	If the length of the hash value is 32 characters
Hash	SHA-1	If the length of the hash value is 40 characters
Hash	SHA-256	If the length of the hash value is 64 characters
CyberVulnerability	CVE	If '.data.hits[].entities[].name' contains 'CVE' and user config Save CVE Data as contains Indicators

Event Attributes Mapping

In the previous table, **Related Indicator Type Mapping**, there is a **Related Indicator Attribute** that is set dynamically. We do this because the **Attribute Key** is extracted from the same path `.data.hits[].entities[].type` if the `.data.hits[].entities[].type` is one from the table listed below.

RECORDED FUTURE ATTRIBUTE TYPE	THREATQ ATTRIBUTE KEY
AttackVector	Attack Vector
Product	Affected Product
Company	Company
City	City
Country	Country
Facility	Facility
FileNameExtension	File Extension
FileType	File Type
GeoEntity	Geo Entity
Industry	Industry
IndustryTerm	Industry Term
Logotype	Logotype
Operation	Operation
OrgEntity	Organization Entity

RECORDED FUTURE ATTRIBUTE TYPE	THREATQ ATTRIBUTE KEY
PhoneNumber	Phone Number
ProvinceOrState	State
Region	Region
Technology	Technology
Topic	Topic

Recorded Future Playbook Alerts

The Recorded Future Playbook Alerts feed retrieves a list of alerts filtered by the values provided in the configuration section. For each of the alerts, the `playbook_alert_id` is used to call the Recorded Future - Get Playbook Alerts by Category supplemental feed, to fetch the full alert context.

POST <https://api.recordedfuture.com/playbook-alert/search>

Sample Response:

```
{
  "status": {
    "status_code": "Ok",
    "status_message": "Playbook alert search successful"
  },
  "data": [
    {
      "playbook_alert_id": "task:2803c5f5-aa32-41ce-98c1-41a7771cd9ad",
      "created": "2022-11-08T09:44:02.447Z",
      "updated": "2022-11-08T09:44:06.584Z",
      "status": "New",
      "category": "domain_abuse",
      "priority": "Informational",
      "title": "juhaokan.ga",
      "owner_id": "uhash:ER135KQ6oL",
      "owner_name": "ThreatQ - Partner",
      "organisation_id": "uhash:DimzHe41vx",
      "organisation_name": "ThreatQ - Partner"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:



The mapping for this feed is based on the JSON response from the **Recorded Future - Get Playbook Alerts by Category supplemental feed**. Each mapping is based on an item within the data list within the JSON response.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.panel_status.case_rule_label, .panel_status.entity_name, .panel_status.priority, .panel_status.entity_criticality</code>	Event.Title	Recorded Future Alert	<code>.panel_status.created</code>	Domain Abuse Alert: juhaokan.ga Priority: Informational Criticality: Medium	We use the four values to create a unique title
<code>.panel_status.title</code>	Event.Title	Recorded Future Alert	<code>.panel_status.created</code>	juhaokan.ga	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.panel_evidence_summary.*, .panel_evidence_whois.*	Event.Description	N/A	N/A	N/A	Description HTML is built based on available fields
.panel_status.status	Event.Attribute	Status	.panel_status.created	New	Updatable
.panel_status.case_rule_label	Event.Attribute	Category	.panel_status.created	Domain Abuse	Updatable
.panel_status.priority	Event.Attribute	Priority	.panel_status.created	Informational	Updatable
.panel_status.owner_name	Event.Attribute	Owner	.panel_status.created	Acme Corp	Updatable
.panel_status.organization_name	Event.Attribute	Organization	.panel_status.created	Acme Corp	N/A
.panel_status.assignee_name	Event.Attribute	Assignee	.panel_status.created	John Doe	N/A
.panel_status.lifecycle_stage	Event.Attribute	Lifecycle Stage	.panel_status.created	Disclosure	Only available for Cyber Vulnerability Alerts
.panel_status.entity_name	Related.Indicator	FQDN	.panel_status.created	jlonssdale.social	N/A
.panel_status.entity_name	Related.Vulnerability	N/A	.panel_status.created	jlonssdale.social	N/A
.panel_status.risk_score	Event.Attribute, Related.Indicator.Attribute	Risk Score	.panel_status.created	5	Updatable
.panel_status.risk_score	Event.Attribute, Related.Indicator.Attribute	Normalized Risk	.panel_status.created	High	Mapped using Risk Score Normalization Mapping user field; Updatable
.panel_status.entity_criticality	Event.Attribute, Related.Indicator.Attribute	Criticality	.panel_status.created	Low	Updatable
.panel_status.context_list[].context	Event.Attribute, Related.Indicator.Attribute	Context Data	.panel_status.created	Phishing Host	N/A
.panel_evidence_dns_ip_list[].entity	Related.Indicator	IP Address	.panel_status.created	217.160.0.153	N/A
.panel_evidence_dns_ip_list[].record_type	Related.Indicator.Attribute	Record Type	.panel_status.created	N/A	Updatable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.panel_evidence_dns. ip_ list[].risk_score	Related.Indicator.Attribute	Risk Score	.panel_status.create d	27	Updatable
.panel_evidence_dns. ip_ list[].risk_score	Related.Indicator.Attribute	Normalized Risk	.panel_status.create d	Medium	Mapped using Risk Score Normalization Mapping user field; Updatable
.panel_evidence_dns. ip_ list[].criticality	Related.Indicator.Attribute	Criticality	.panel_status.create d	Medium	Updatable
.panel_evidence_dns. ip_ list[].context_list[]. context	Related.Indicator.Attribute	Context Data	.panel_status.create d	Phishing Host	N/A
.panel_evidence_dns. mx_ list[].entity	Related.Indicator	FQDN	.panel_status.create d	mx00.ionos.co.uk	N/A
.panel_evidence_dns. mx_ list[].record_type	Related.Indicator.Attribute	Record Type	.panel_status.create d	N/A	Updatable
.panel_evidence_dns. mx_ list[].risk_score	Related.Indicator.Attribute	Risk Score	.panel_status.create d	0	Updatable
.panel_evidence_dns. mx_ list[].risk_score	Related.Indicator.Attribute	Normalized Risk	.panel_status.create d	Low	Mapped using Risk Score Normalization Mapping user field; Updatable
.panel_evidence_dns. mx_ list[].criticality	Related.Indicator.Attribute	Criticality	.panel_status.create d	0	Updatable
.panel_evidence_dns. mx_ list[].context_list[]. context	Related.Indicator.Attribute	Context Data	.panel_status.create d	Active Mail Server	N/A
.panel_evidence_dns. ns_ list[].entity	Related.Indicator	FQDN	.panel_status.create d	ns1025.ui-dns.org	N/A
.panel_evidence_dns. ns_ list[].record_type	Related.Indicator.Attribute	Record Type	.panel_status.create d	N/A	Updatable
.panel_evidence_dns. ns_ list[].risk_score	Related.Indicator.Attribute	Risk Score	.panel_status.create d	5	Updatable
.panel_evidence_dns. ns_ list[].risk_score	Related.Indicator.Attribute	Normalized Risk	.panel_status.create d	Low	Mapped using Risk Score Normalization Mapping user field; Updatable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.panel_evidence_dns_list[].criticality</code>	Related.Indicator.Attribute	Criticality	<code>.panel_status.created</code>	Low	Updatable
<code>.panel_evidence_dns_list[].context_list[].context</code>	Related.Indicator.Attribute	Context Data	<code>.panel_status.created</code>	Active Mail Server	N/A
<code>.panel_evidence_summary.affected_products[].name</code>	Related.Vulnerability.Attribute	Affected Product	<code>.panel_status.created</code>	MySQL	Also applied to main event
<code>.panel_evidence_summary.assessments[].evidence.data[].malwareIpAddress</code>	Related.Indicator	IP Address	<code>.panel_status.created</code>	N/A	N/A
<code>.panel_evidence_summary.assessments[].evidence.data[].malwareFamily</code>	Related.Malware	N/A	<code>.panel_status.created</code>	Lazarus	N/A
<code>.panel_evidence_summary.assessments[].evidence.data[].clientIpAddress</code>	Related.Asset	N/A	<code>.panel_status.created</code>	N/A	N/A

Recorded Future - Get Playbook Alerts by Category (Supplemental)

The Recorded Future - Get Playbook Alerts by Category supplemental feed related data for each of the ingested events retrieved from the Alert endpoint. The key `.data[].playbook_alert_id` is used to call the supplemental feed.

POST `https://api.recordedfuture.com/playbook-alert/{{ category }}`



The API will return a slightly different response based on the category of the alert. See the Recorded Future Playbook Alerts feed for the mapping of the data.

Domain Abuse

Sample Response:

```
{
  "status": {
    "status_code": "Ok",
    "status_message": "Domain Abuse lookup successful"
  },
  "data": {
    "panel_status": {
      "entity_name": "lonsdale.social",
      "entity_criticality": "Low",
      "risk_score": 5,
      "context_list": [
        {
          "context": "Phishing Host"
        },
        {
          "context": "Active Mail Server"
        }
      ],
      "targets": [
        "idn:lonsdale.fr",
        "idn:lonsdale.us",
        "idn:lonsdale.porn",
        "idn:lonsdale.club"
      ],
      "status": "New",
      "priority": "High",
      "created": "2022-11-09T08:20:15.778Z",
      "case_rule_id": "report:nvAj-X",
      "case_rule_label": "Domain Abuse",
      "owner_id": "uhash:ER135KQ6oL",
      "owner_name": "ThreatQ - Partner",
      "organisation_id": "uhash:DimzHe41vx",
      "organisation_name": "ThreatQ - Partner"
    }
  }
}
```

```

    },
    "panel_action": [],
    "panel_evidence_summary": {
      "explanation": "Alert was created as a result of a triggered
typosquat detection",
      "resolved_record_list": [
        {
          "entity": "idn:ns1025.ui-dns.org",
          "risk_score": 5,
          "criticality": "Low",
          "record_type": "NS",
          "context_list": []
        },
        {
          "entity": "ip:217.160.0.153",
          "risk_score": 27,
          "criticality": "Medium",
          "record_type": "A",
          "context_list": [
            {
              "context": "Phishing Host"
            }
          ]
        },
        {
          "entity": "idn:mx00.ionos.co.uk",
          "risk_score": 0,
          "criticality": "0",
          "record_type": "MX",
          "context_list": [
            {
              "context": "Active Mail Server"
            }
          ]
        },
        {
          "entity": "idn:mx01.ionos.co.uk",
          "risk_score": 0,
          "criticality": "0",
          "record_type": "MX",
          "context_list": [
            {
              "context": "Active Mail Server"
            }
          ]
        }
      ],
      "screenshots": [
        {
          "description": "An image associated with the Playbook

```

```
Alert",
    "image_id": "img:349f92e2-fa93-4282-be15-e7a330130686",
    "created": "2022-11-09T08:20:51.685Z"
  }
],
},
"panel_evidence_dns": {
  "ip_list": [
    {
      "entity": "ip:217.160.0.153",
      "risk_score": 27,
      "criticality": "Medium",
      "record_type": "A",
      "context_list": [
        {
          "context": "Phishing Host"
        }
      ]
    }
  ],
  "mx_list": [
    {
      "entity": "idn:mx00.ionos.co.uk",
      "risk_score": 0,
      "criticality": "0",
      "record_type": "MX",
      "context_list": [
        {
          "context": "Active Mail Server"
        }
      ]
    }
  ],
  "ns_list": [
    {
      "entity": "idn:ns1115.ui-dns.de",
      "risk_score": 0,
      "criticality": "0",
      "record_type": "NS",
      "context_list": [
        {
          "context": "Active Mail Server"
        }
      ]
    },
    {
      "entity": "idn:ns1090.ui-dns.biz",
      "risk_score": 5,
      "criticality": "Low",
      "record_type": "NS",
      "context_list": []
    }
  ]
}
```

```

    }
  ]
},
"panel_evidence_whois": {
  "body": [
    {
      "provider": "whois",
      "entity": "idn:lonsdale.social",
      "attribute": "attr:whois",
      "value": {
        "privateRegistration": false,
        "status": "clientTransferProhibited addPeriod",
        "nameServers": [
          "idn:ns1066.ui-dns.com",
          "idn:ns1025.ui-dns.org",
          "idn:ns1115.ui-dns.de",
          "idn:ns1090.ui-dns.biz"
        ],
        "registrarName": "IONOS SE",
        "createdDate": "2022-11-08T19:44:16.000Z"
      },
      "added": "2022-11-09T08:21:13.682Z"
    },
    {
      "provider": "whois",
      "entity": "idn:btbo2.top",
      "attribute": "attr:whoisContacts",
      "value": {
        "organization": "REDACTED FOR PRIVACY",
        "city": "REDACTED FOR PRIVACY",
        "name": "REDACTED FOR PRIVACY",
        "state": "REDACTED FOR PRIVACY",
        "street1": "REDACTED FOR PRIVACY",
        "country": "REDACTED FOR PRIVACY",
        "postalCode": "REDACTED FOR PRIVACY",
        "telephone": "REDACTED FOR PRIVACY",
        "type": "technicalContact"
      },
      "added": "2022-11-08T10:28:20.712Z"
    }
  ]
},
"panel_log": [
  {
    "id": "uuid:26b4be48-e1e0-4773-97d7-b8c8260fe53b",
    "created": "2022-11-09T08:27:31.377Z",
    "modified": "2022-11-09T08:27:31.377Z",
    "action_priority": "Informational"
  }
]

```

```
}
}
```

Third Party Risk

Sample Response:

```
{
  "status": {
    "status_code": "Ok",
    "status_message": "Playbook alert bulk lookup successful."
  },
  "data": [
    {
      "playbook_alert_id": "task:220833e1-6a00-489c-8e6f-08cb11561aea",
      "panel_status": {
        "status": "New",
        "priority": "Moderate",
        "created": "2024-05-09T18:03:42.784Z",
        "updated": "2024-05-13T05:11:28.845Z",
        "case_rule_id": "report:r2TUUz",
        "case_rule_label": "Third Party Risk",
        "owner_id": "uhash:1RmVv0sQ33",
        "owner_name": "Acme Corp",
        "organisation_id": "uhash:4WfuvVnaap",
        "organisation_name": "Acme Corp",
        "owner_organisation_details": {
          "organisations": [
            {
              "organisation_id": "uhash:4WfuvVnaap",
              "organisation_name": "Acme Corp"
            }
          ]
        },
        "enterprise_id": "uhash:4WfuvVnaap",
        "enterprise_name": "Acme Corp"
      },
      "entity_id": "CEBTA",
      "entity_name": "Tele Communications",
      "entity_criticality": "Medium",
      "risk_score": 64,
      "targets": [
        {
          "name": "Infections Recently Reported in Company Infrastructure"
        },
        {
          "name": "Recent Possible Malware in Company Infrastructure"
        }
      ],
      "actions_taken": []
    }
  ],
}
```

```

    "panel_evidence_summary": {
      "assessments": [
        {
          "risk_rule": "Infections Recently Reported in Company
Infrastructure",
          "level": 2,
          "added": "2024-05-13T05:11:09.882Z",
          "evidence": {
            "type": "ip_rule",
            "summary": "4 sightings: Suspected Malicious Packet Source seen
for 1 IP Address on company infrastructure: 121.241.162.25. Recent Botnet
Traffic seen for 3 IP Addresses on company infrastructure: 203.199.243.0,
14.143.123.78, 14.143.187.214",
            "data": [
              {
                "name": "Suspected Malicious Packet Source",
                "criticality": 2,
                "number_of_ip_addresses": 1
              },
              {
                "name": "Recent Botnet Traffic",
                "criticality": 2,
                "number_of_ip_addresses": 3
              }
            ]
          }
        },
        {
          "risk_rule": "Recent Possible Malware in Company Infrastructure",
          "level": 2,
          "added": "2024-05-13T05:11:09.882Z",
          "evidence": {
            "type": "ip_rule",
            "summary": "1 sighting: Recent Positive Malware Verdict seen for
1 IP Address on company infrastructure: 14.142.45.148",
            "data": [
              {
                "name": "Recent Positive Malware Verdict",
                "criticality": 2,
                "number_of_ip_addresses": 1
              }
            ]
          }
        }
      ]
    }
  ]
}

```

Cyber Vulnerability

Sample Response:

```
{
  "status": {
    "status_code": "Ok",
    "status_message": "Playbook alert bulk lookup successful."
  },
  "data": [
    {
      "playbook_alert_id": "task:174cd0d2-2fad-482b-956d-97e3c3e06ab3",
      "panel_status": {
        "status": "New",
        "priority": "Informational",
        "assignee_name": "John Doe",
        "assignee_id": "uhash:12QsDAJfc1",
        "created": "2024-04-25T14:10:30.241Z",
        "updated": "2024-04-25T14:10:30.241Z",
        "case_rule_id": "report:k0g1wZ",
        "case_rule_label": "Cyber Vulnerability",
        "owner_id": "uhash:5ApZv0sR31",
        "owner_name": "Acme Corp",
        "organisation_id": "uhash:1WauvZmavb",
        "organisation_name": "Acme Corp",
        "owner_organisation_details": {
          "organisations": [
            {
              "organisation_id": "uhash:5ApZv0sR31",
              "organisation_name": "Acme Corp"
            }
          ]
        },
        "enterprise_id": "uhash:1WauvZmavb",
        "enterprise_name": "Acme Corp"
      },
      "entity_id": "vj-Vlg",
      "entity_name": "CVE-2024-4058",
      "entity_criticality": "Medium",
      "risk_score": 33,
      "lifecycle_stage": "Disclosure",
      "targets": [
        {
          "name": "Google Chrome"
        }
      ],
      "actions_taken": []
    },
    {
      "panel_evidence_summary": {
        "summary": {
          "targets": [
            {

```

```

        "name": "Google Chrome"
    },
    ],
    "lifecycle_stage": "Disclosure",
    "risk_rules": [
        {
            "rule": "Recently Referenced by Insikt Group",
            "description": "3 sightings on 1 source: Insikt Group. 3 reports including Google Patches Chrome Vulnerability CVE-2024-4059 and Additional Flaw Tracked as CVE-2024-4060. Most recent link (Apr 26, 2024): https://app.recordedfuture.com/portal/analyst-note/doc:vn9yUw"
        },
        {
            "rule": "Linked to Historical Cyber Exploit",
            "description": "21 sightings on 7 sources including: InfoSecPortal.ru | 0YD3ND»DmD'DD, Dm DZD±D½D¾D²D»DmD½D,Ñ, SecurityWeek, Anti-Malware.ru | DÐ¾D²D¾ÑÑ,D, D~D½Ñ,,D¾ÑD¹D°Ñ†D,D¾D½D½D¾D¹ D'DmD·D¾D¿D°ÑD½D¾ÑÑ,D,, xynik.com, Xakep.ru. Most recent tweet: D' Chrome D,ÑD¿ÑD°D²D,D»D, D°ÑD,D,Ñ†DmÑD°ÑfÑŽ ÑfÑD·D²D,D¾D¾ÑÑ,ÑD, D·D° D°D¾Ñ,D¾ÑÑfÑŽ ÑD°ÑD¿DmÑÑ,Ñ< D¿D¾D»ÑfÑ†D,D»D, 16 000 D'D¾D»D»D°ÑD¾D² DÐ° ÑÑ,D¾D¹ D½DmD'DmD»Dm Google D²Ñ<D¿ÑfÑÑ,D,D»D° D¾D±D½D¾D²D»DmD½D,Dm D'D»Ñ Chrome 124, D°D¾Ñ,D¾ÑD¾Dm D,ÑD¿ÑD°D²D»ÑDmÑ, Ñ†DmÑ,Ñ<ÑDm ÑÑD°D·Ñf ÑfÑD·D²D,D¾D¾ÑÑ,D,, D²D°D»ÑŽÑ†D°Ñ D°ÑD,D,Ñ†DmÑD°ÑfÑŽ D¿ÑD¾D±D»DmD¾Ñf CVE-2024-4058 D²â€| 0YD3ND'ÑD¾D±D½DmDm https://t.co/Tnmg7ZPfSg https://t.co/UpviubMKJY. Most recent link (Apr 26, 2024): https://twitter.com/pc7ooo/statuses/1783975885718098318"
        },
        {
            "rule": "Web Reporting Prior to CVSS Score",
            "description": "Reports involving CVE Vulnerability before CVSS score is released by NVD."
        }
    ]
},
    "affected_products": [
        {
            "name": "Google Chrome"
        }
    ],
    "insikt_notes": [
        {
            "id": "doc:vn9yUw",
            "title": "Google Patches Chrome Vulnerability CVE-2024-4059 and Additional Flaw Tracked as CVE-2024-4060",
            "published": "2024-04-26T13:22:37.371Z",
            "topic": "Validated Intelligence Event",
            "fragment": "In recent updates announced on April 24, 2024, Google has addressed a critical vulnerability CVE-2024-4058 in its Chrome web browser that could allow threat actors to take control of a user's system. The vulnerability is related to the ANGLE graphics layer engine and has a \"critical\" severity rating."
        }
    ]
}

```

```

    },
    {
      "id": "doc:vm4TAU",
      "title": "CVE-2024-4058 allows Type Confusion affecting Google
Chrome",
      "published": "2024-04-25T16:31:33.504Z",
      "topic": "Informational",
      "fragment": "CVE-2024-4058 is a type confusion bug in the ANGLE
graphics layer engine. A manipulation with an unknown input can lead to a type
confusion vulnerability."
    },
    {
      "id": "doc:vmfmEu",
      "title": "Google Patches Four Vulnerabilities Affecting Chrome,
Including Critical-Severity Vulnerability CVE-2024-4058",
      "published": "2024-04-25T09:47:23.765Z",
      "topic": "Validated Intelligence Event",
      "fragment": "On April 24, 2024, Google patched four vulnerabilities
affecting the Chrome browser. This included CVE-2024-4058, a critical-
severity type confusion vulnerability that arises from a misinterpretation of
data types within the Almost Native Graphics Layer Engine (ANGLE) of the Chrome
browser. Successful exploitation of CVE-2024-4058 can allow threat actors to
execute arbitrary code or evade sandboxes remotely with minimal user
interaction, potentially leading to unauthorized access, data manipulation, and
system compromise."
    }
  ]
}

```

Code Repo Leakage

Sample Response:

```

{
  "status": {
    "status_code": "Ok",
    "status_message": "Playbook alert bulk lookup successful."
  },
  "data": [
    {
      "playbook_alert_id": "task:f19c105a-5997-4a13-b54f-7b64816954fa",
      "panel_status": {
        "status": "New",
        "priority": "Informational",
        "created": "2024-05-01T22:05:52.838Z",
        "updated": "2024-05-01T22:05:52.838Z",
        "case_rule_id": "report:q_dg1Y",

```

```

"case_rule_label": "Data Leakage on Code Repository",
"owner_id": "uhash:7RaVs0sR31",
"owner_name": "Acme Corp",
"organisation_id": "uhash:1XfyvKnbbp",
"organisation_name": "Acme Corp",
"owner_organisation_details": {
  "organisations": [
    {
      "organisation_id": "uhash:7RaVs0sR31",
      "organisation_name": "Acme Corp"
    }
  ],
  "enterprise_id": "uhash:1XfyvKnbbp",
  "enterprise_name": "Acme Corp"
},
"entity_id": "url:https://github.com/Inclusion-Bridge/2024-bridge-to-
data-fundamentals",
"entity_name": "https://github.com/Inclusion-Bridge/2024-bridge-to-
data-fundamentals",
"entity_criticality": "",
"risk_score": 0,
"targets": [
  {
    "name": "acme.org"
  }
],
"actions_taken": [],
},
"panel_evidence_summary": {
  "repository": {
    "id": "url:https://github.com/Inclusion-Bridge/2024-bridge-to-data-
fundamentals",
    "name": "https://github.com/Inclusion-Bridge/2024-bridge-to-data-
fundamentals",
    "owner": {
      "name": "aifenaik"
    }
  },
  "evidence": [
    {
      "assessments": [
        {
          "id": "attr:watchListEntityMention",
          "title": "Watch List Entity Mention",
          "value": "acme.org"
        }
      ],
      "targets": [
        {
          "name": "acme.org"
        }
      ]
    }
  ]
}

```

```

    }
  ],
  "url": "https://github.com/Inclusion-Bridge/2024-bridge-to-data-
fundamentals/commit/5002107a89ad09e3b45bf07d45d400f1a4738f5a",
  "content": "+Shenhua Group,276,37322,-0.8,1916.9,140911,37.9,Ling
Wen,\"Mining, Crude-Oil Production\",Energy,270,China,\"Beijing,
China\",http://www.shenhua.com.cn,8,202200,47962\n+Greenland Holding
Group,277,37240,12.8,1085.2,105495,-1.0,Zhang Yuliang,Real
estate,Financials,311,China,\"Shanghai, China\",http://
www.ldjt.com.cn,6,39887,8333\n+ACME,278,37105,5.5,1492.3,523194,22.9,Roger W.
Ferguson Jr.,\"Insurance: Life, Health (Mutual)\",Financials,291,USA,\"New
York, NY\",http://www.acme.org,20,12997,35583\n+Jardine
Matheson,279,37051,0.1,2503.0,71523,39.3,Ben Keswick,Motor Vehicles and
Parts,Motor Vehicles & Parts,273,China,\"Hong Kong, China\",http://
www.jardines.com,18,430000,21800\n+Oracle,280,37047,-3.1,8901.0,112180,-10.4,Sa
fra A. Catz,Computer Software,Technology,260,USA,\"Redwood City, CA\",http://
www.oracle.com,11,136000,47289",
  "published": "2024-05-01T22:03:09.273Z"
}
  ]
}
]
}

```

Recorded Future Fusion Files

The Recorded Future fusion files feed ingests threat intelligence information from the user selected Fusion feeds.

GET https://api.recordedfuture.com/v2/fusion/files?path={fusion_file_path}



Depending on the fetched Fusion File, the API response will be different. The following are examples and mappings for all of the possible files.

Command and Control IPs

[/public/detect/c2_scanned_ips.json](#)

Sample Response:

```
{
  "count": 2,
  "results": [
    {
      "ip": "2.56.116.210",
      "ports": [
        {
          "port": 26,
          "protocol": "TCP"
        },
        {
          "port": 24,
          "protocol": "TCP"
        },
        {
          "port": 50050,
          "protocol": "TCP"
        }
      ],
      "malware": ["Cobalt Strike"],
      "last_seen_active": "2106-02-07",
      "last_scan": "2024-05-14"
    },
    {
      "ip": "147.189.174.48",
      "ports": [
        {
          "port": 6666,
          "protocol": "TCP"
        }
      ],
      "malware": ["AsyncRAT"],
      "last_seen_active": "2024-05-12",
      "last_scan": "2024-05-14"
    }
  ]
}
```

ThreatQ provides the following default mapping for this pathway:



Mappings are based on each item within the results key.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.ip	Indicator.Value	IP Address	.last_seen_active	N/A	N/A
.ports[].port	Attribute	Scanned Port	.last_seen_active	8080	N/A
.malware[]	Malware	N/A	.last_seen_active	AsyncRAT	N/A
N/A	Attribute	Fusion File	.last_seen_active	c2_scanned_ips	N/A

Known TOR IPs

/public/policy/tor_ips.json

Sample Response:

```
[
  {
    "ip": "171.25.193.77",
    "name": "DFRI29",
    "flags": "EFGHRSDV"
  },
  {
    "ip": "171.25.193.78",
    "name": "DFRI27",
    "flags": "EFGHRSDV"
  },
  {
    "ip": "198.96.155.3",
    "name": "gurgle",
    "flags": "EFGHRSDV"
  }
]
```

ThreatQ provides the following default mapping for this pathway:



Mappings are based on each item within the array.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.ip	Indicator.Value	IP Address	N/A	N/A	N/A
.name	Attribute	TOR Name	N/A	gurgle	N/A
.flags	Attribute	TOR Flags	N/A	EFGHRSDV	N/A
N/A	Attribute	Fusion File	N/A	tor_ips	N/A

Active RAT C2 IPs

/public/detect/ratcontrollers_ips.json

Sample Response:

```
[
  {
    "hostnames": [],
    "ip": "208.100.26.240",
    "country": "",
    "asn": "",
    "port": "",
    "malware": "",
    "protocol": "",
    "signal": []
  },
  {
    "hostnames": [],
    "ip": "88.119.175.231",
    "country": "",
    "asn": "",
    "port": "",
    "malware": "",
    "protocol": "",
    "signal": []
  },
  {
    "hostnames": [],
    "ip": "103.97.176.121",
    "country": "",
    "asn": "",
    "port": "",
    "malware": "",
    "protocol": "",
    "signal": []
  }
]
```

ThreatQ provides the following default mapping for this pathway:



Mappings are based on each item within the array.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.ip	Indicator.Value	IP Address or URL	N/A	N/A	Type will depend on if the .ip value starts with http or not.
N/A	Attribute	Fusion File	N/A	ratcontrollers_ips	N/A
.asn	Attribute	ASN	N/A	N/A	N/A
.country	Attribute	Country	N/A	N/A	N/A
.malware	Malware	N/A	N/A	Nanocore RAT	N/A

Fast Flux IPs

/public/detect/fflux_ips.json

Sample Response:

```
[
  {
    "lastSeen": 1715817599000,
    "ip": "1.189.96.74"
  },
  {
    "lastSeen": 1715817599000,
    "ip": "83.48.172.198"
  },
  {
    "lastSeen": 1715817599000,
    "ip": "83.224.176.102"
  },
  {
    "lastSeen": 1715817599000,
    "ip": "37.84.163.136"
  }
]
```

ThreatQ provides the following default mapping for this pathway:

 Mappings are based on each item within the array.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.ip	Indicator.Value	IP Address	.lastSeen	N/A	N/A
N/A	Attribute	Fusion File	N/A	fflux_ips	N/A

Dynamic DNS IPs

/public/detect/ddns_ips.json

Sample Response:

```
[
  { "lastSeen": 1592813679718, "ip": "14.207.60.10" },
  { "lastSeen": 1602551372295, "ip": "31.184.203.121" },
  { "lastSeen": 1600696916364, "ip": "200.95.170.74" },
  { "lastSeen": 1715817599000, "ip": "31.46.242.12" },
  { "lastSeen": 1715817599000, "ip": "201.151.223.102" }
]
```

ThreatQ provides the following default mapping for this pathway:



Mappings are based on each item within the array.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.ip	Indicator.Value	IP Address	.lastSeen	N/A	N/A
N/A	Attribute	Fusion File	N/A	ddns_ips	N/A

Potentially Undetectable Malware

/public/detect/low_detect_malware_hashes.json

Sample Response:

```
[
  {
    "lastSeen": 1637938630146,
    "hash": "00af0726cdaf4dd07375ed03513a5ce3e5055a285b932b20bc06c85d92b00e9f",
    "algorithm": "SHA-256"
  },
  {
    "lastSeen": 1517420645494,
    "hash": "0bcc5b3fbed425984f6ce7fbf1a62a7f",
    "algorithm": "MD5"
  },
  {
    "lastSeen": 1565960362167,
    "hash": "0f6bfff19fd5fe46f577853c7de074072fba5c04831fddac820eacd897622d343",
    "algorithm": "SHA-256"
  },
  {
    "lastSeen": 1574942448466,
    "hash": "be62ca209f803671935370c9d05ad5d25acd55d47029f19fca75df6b74dfb957",
    "algorithm": "SHA-256"
  },
  {
    "lastSeen": 1557138379174,
    "hash": "e3a318797bdc6d45917364efdf329dd8fd6a39f1178d71dc1945ff94a425b209",
    "algorithm": "SHA-256"
  },
  {
    "lastSeen": 1572496263780,
    "hash": "39e4251cacd684dc4886bddfefdda3cf78c0d6d4",
    "algorithm": "SHA-1"
  },
  {
    "lastSeen": 1572496263780,
    "hash": "222f4b0b2a69666cb0843af04a2d234378e284a9c05fb2ae0e6754fb52b1ee34df361fd1d3b70f3bbcd2b7611d64d5622558b4b6c127263",
    "algorithm": "SHA-512"
  }
]
```

ThreatQ provides the following default mapping for this pathway:



Mappings are based on each item within the the array.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.hash	Indicator.Value	.algorithm	.lastSeen	N/A	N/A
N/A	Attribute	Fusion File	N/A	low_detect_malware_hashes	N/A

Weaponized Domains

/public/detect/weaponized_domains.json

Sample Response:

```
{
  "count": 2,
  "results": [
    {
      "domain": "dswa.1337.cx",
      "last_seen": "2024-05-15",
      "service_provider": "Afraid.org",
      "detection_strings": {
        "phishing site": false,
        "spam site": false,
        "spam image": false,
        "mining site": false,
        "malicious site": false,
        "suspicious site": false,
        "malware site": true,
        "malware hd site": false,
        "fraudulent site": false
      }
    },
    {
      "domain": "7.24-7.ro",
      "last_seen": "2024-05-13",
      "service_provider": "Afraid.org",
      "detection_strings": {
        "phishing site": true,
        "spam site": false,
        "spam image": false,
        "mining site": false,
        "malicious site": false,
        "suspicious site": false,
        "malware site": true,
        "malware hd site": false,
        "fraudulent site": false
      }
    }
  ]
}
```

ThreatQ provides the following default mapping for this pathway:



Mappings are based on each item within the results key.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.domain	Indicator.Value	FQDN	.last_seen	N/A	N/A
N/A	Attribute	Fusion File	N/A	weaponized_domains	N/A
.service_provider	Attribute	Service Provider	.last_seen	Afraid.org	N/A
.detection_strings[phishing site]	Attribute	Threat Type	.last_seen	Phishing	Only if flag is true

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.detection_strings[spam site]	Attribute	Threat Type	.last_seen	Spam	Only if flag is true
.detection_strings[spam image]	Attribute	Threat Type	.last_seen	Spam	Only if flag is true
.detection_strings[mining site]	Attribute	Threat Type	.last_seen	Cryptomining	Only if flag is true
.detection_strings[malicious site]	Attribute	Disposition	.last_seen	Malicious	Only if flag is true
.detection_strings[suspicious site]	Attribute	Disposition	.last_seen	Suspicious	Only if flag is true
.detection_strings[malware site]	Attribute	Threat Type	.last_seen	Malware	Only if flag is true
.detection_strings[malware hd site]	Attribute	Threat Type	.last_seen	Malware	Only if flag is true
.detection_strings[fraudulent site]	Attribute	Threat Type	.last_seen	Fraud	Only if flag is true

Exploits in the Wild Hashes

/public/prevent/exploits_itw_hashes.json

Sample Response:

```
{
  "count": 97644,
  "results": [
    {
      "hash": "6131945bc2925a227c748f6e65d3108d0519fe03887a2353b516d75c26afb03e",
      "algorithm": "sha256",
      "cybervulnerabilities": ["CVE-2010-2568"],
      "malware": "unknown",
      "days_with_sighting": 16,
      "last_seen": "2024-05-14"
    },
    {
      "hash": "a63570d7200cb3628f2a8887bc9d5cf0",
      "algorithm": "md5",
      "cybervulnerabilities": ["CVE-2022-42889"],
      "malware": "unknown",
      "days_with_sighting": 1,
      "last_seen": "2024-05-08"
    }
  ]
}
```

ThreatQ provides the following default mapping for this pathway:



Mappings are based on each item within the results key.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.hash	Indicator.Value	.algorithm	.last_seen	N/A	N/A
N/A	Attribute	Fusion File	N/A	exploits_itw_hashes	N/A
.cybervulnerabilities[]	Indicator.Value, Vulnerability.Value	CVE	.last_seen	CVE-2022-42889	N/A
.malware	Malware.Value	N/A	.last_seen	Lokibot	Ingested if not 'unknown'

Average Feed Run



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

Recorded Future Domain Risk List

METRIC	RESULT
Run Time	1 minute
Indicators	393
Indicator Attributes	3,226

Recorded Future IP Risk List

METRIC	RESULT
Run Time	1 minute
Indicators	95
Indicator Attributes	1,979

Recorded Future URL Risk List

METRIC	RESULT
Run Time	23 minutes

METRIC	RESULT
Indicators	10,653
Indicator Attributes	92,877

Recorded Future Vulnerability Risk

METRIC	RESULT
Run Time	1 minute
Indicators	3
Indicator Attributes	158
Vulnerabilities	5
Vulnerability Attributes	158

Recorded Future Hash Risk List

METRIC	RESULT
Run Time	1 minute
Indicators	534
Indicator Attributes	4,707

Recorded Future Analyst Note

METRIC	RESULT
Run Time	2 minutes
Attack Patterns	1
Attack Pattern Attributes	2
Indicators	113
Indicator Attributes	732
Malware	24
Malware Attributes	131
Reports	19
Reports Attributes	335

Recorded Future Alerts

METRIC	RESULT
Run Time	1 minute
Events	13
Events Attributes	65
Indicators	48

METRIC	RESULT
Indicator Attributes	151
Malware	6
Malware Attributes	6
Adversary	2
Adversary Attributes	2

Recorded Future Playbook Alerts

METRIC	RESULT
Run Time	1 minute
Events	23
Events Attributes	115
Indicators	14
Indicator Attributes	24

Recorded Future Fusion Files

METRIC	RESULT
Run Time	11 minutes
Indicators	36,424
Indicator Attributes	74,979
Malware	141
Malware Attributes	143
Vulnerabilities	222
Vulnerability Attributes	222

Known Issues / Limitations

- The 5 main Recorded Future feeds take progressively longer to complete as more and more lists are specified for the **Recorded Future List** configuration parameter. ThreatQ recommends pulling a targeted subset of lists for each feed instead of all of the available lists.
- If Recorded Future deletes a list, the feed will return an empty response for it.
- The Recorded Future **Analyst Notes** and **Alerts** feeds have an API limit and will only return the first 1,000 results.
- Recorded Future CDF 2.8.7 introduced the **All** option for the **List to be Retrieved** configuration parameter with the Recorded Future Domain, Risk List Recorded Future Hash Risk List, Recorded Future IP Risk List, and Recorded Future URL Risk List feeds. There is a known bug where users can select the **All** option and also individual items in the list. Doing will cause the feed to error when run. If you are using the **All** option, you must unselect all other individual items for the **List to be Retrieved** configuration for that feed.



Feed runs will typically complete within 40 minutes using this option so it is advised to schedule run times no more frequently than one hour.

Change Log

- **Version 2.10.1**
 - Resolved an issue where the Analyst Note feed ingested data with undesired text tags.
 - Add the following configuration parameters to all feeds:
 - Enable SSL Verification
 - Disable Proxies
- **Version 2.10.0**
 - All feeds except Alerts, Analyst Note, and Fusion Files: added two new configuration parameters:
 - **Normalize Risk Score** - enable this option to ingest a normalized risk score value as a scorable attribute.
 - **Risk Score Normalization Mapping** - allows you to configure mapping to normalize risk score values to the scorable attribute, `Normalized Risk`.
- **Version 2.9.1**
 - Made the following changes to the Recorded Future Analyst Note feed:
 - Removed the **Ingest Selected Entities as Indicators** configuration option.
 - Added the following new configuration parameters:
 - **Ingest Selected Primary Entities as Indicators** - indicators of compromise from the "primary" entities list (note_entities) can now be ingested as indicator objects. Email Addresses from the "primary" entities list can now be ingested as indicators. Context (i.e. Malware, Adversaries, Attributes, & Attack Patterns) from the "primary" entities list will now be applied to the indicators of compromise from the "primary" entities list.
 - **Ingest Selected Supporting Entities as Indicators** - indicators from the "supporting" entities list (context_entities) can now be ingested as indicator objects. Identities (Email Addresses) will now only be ingested from the "supporting" entities list
 - "Product" entities will only be brought in as the "Affected Product" attribute when a vulnerability is associated. Otherwise, the attribute name will just be, "Product".
 - Fixes issue where reference URLs in the description would have a `url:` prefix.
 - Topics are now ingested as tags.
- **Version 2.9.0**
 - The Recorded Future Analyst Note feed has been rewritten. Changes with the new feed include:
 - Reports are now ingested with a rich text description (HTML).
 - Full lists of entities, recommended queries, topics, authors, and metadata are now included in the feed.
 - References have been moved from the attributes section to the description.
 - `EmailAddress` entities are now extracted and related as Identity objects.
 - **InternetDomainName, IpAddress, and Hash entities will now only be extracted and ingested as indicators if you elect to do so - which is not advised.**
 - `Organization` entities are now filtered before being related as adversaries. This change is to prevent benign organizations from being related.

- You can now choose to ingest CVEs as Vulnerability (default) or Indicator objects.
- Hashtag entities are now extracted and added as tags to reports.
- Product entity attribute has been renamed to Affected Product to be more consistent with other feeds.
- Analyst notes are no longer inherited to related object's descriptions.
- Default Indicator status is now Review.
- Performed the following updates to the **Risk Lists** feeds:
 - Added a new user field: **Filter Out Entries with No New Evidence**. This allows you to filter out indicators that do not have any new evidence within the feed run timeframe and will help limit the amount of indicators that the feeds ingest, improving overall system performance. You can perform a historical manual run to ingest the full list of indicators.
- Performed the following updates to the **Recorded Future Playbook Alerts** feed:
 - Updated the default indicator status to Review.
 - Added enhanced Event Title and Description.
 - Events now include the category, priority, and criticality as part of the ingested Event Title.
 - Events now include a rich text description with context such as targets, assessments & WHOIS information
 - Added support for ingesting additional alert types & context data:
 - Cyber Vulnerabilities
 - Third Party Risks
 - Code Repo Leakages
 - Domain Abuse alerts now include WHOIS information.
 - Renamed the Organisation attribute to the more common, Organization spelling.
 - The category attribute will now reflect the case_rule_label value, rather than the more programmatic category value from the initial feed response.
 - Added better handling of shared attributes between the offending entity and event alert.
 - Malware Families are now parsed out from assessment results (if available).
 - Assets (Client IPs) are now parsed out from assessment results (if available).
- Performed the following updates to the **Recorded Future Alerts** feed:
 - Alerts will now be ingested with a rich description containing a "Hits" table with the triggered entities and their respective documents.
 - This feed will no longer ingest document URLs as indicators.
 - This feed will only ingest CVEs (if enabled) and Hashes as indicators from the relevant document entities.
 - InternetDomainNames, URLs, IP Addresses, etc. have been removed as they are likely to be benign.
 - You'll now be able to see the entities within the description of the event/alert.
 - Document entities will now be related to the event/alert.
 - The Triggered Rule URL attribute has been removed as it is no longer relevant.
 - Added Logotype as an extracted attribute.
 - Moved the Reference URL attribute to the event description.
 - Updated the default indicator status to Review.
 - Removed ability to add "Person" entities as related adversaries.

- Added filtering of the Organization entities to prevent adding benign organizations as related adversaries.
 - Resolved an issue where the feed would ingest MITRE Technique IDs that do not align with existing MITRE Attack Patterns within the system.
- Added a new feed: **Recorded Future Fusion Files**.
- **Version 2.8.7**
 - Added an **All** option to the **List to be Retrieved** parameter for the following feeds:

 Feed runs will typically complete within 40 minutes using this option so it is advised to schedule run times no more frequently than one hour.

 - Recorded Future Domain Risk List
 - Recorded Future Hash Risk List
 - Recorded Future IP Risk List
 - Recorded Future URL Risk List
 - Added new Known Issue regarding the **All** option for the **List to be Retrieved** parameter. If utilizing the **All** option, all other items in the **List to be Retrieved** parameter must be unselected. Attempting to run a feed with the **All** and other items in the list selected will cause the feed to fail.
 - Added a new attribute for the Recorded Future playbook Alerts feed: **Context data**.
 - Added **Target Entities** for related entities in the Recorded Future Alerts feed.
- **Version 2.8.6**
 - Performed optimization improvements for all feeds that contain the Risk List in their name in a effort to reduce the possibility of timeout errors.
- **Version 2.8.5**
 - Resolved a timeout error that was caused by large evidence details.
 - Removed the following no longer supported lists from Recorded Future Domain Risk List:
 - **Historical Malware Analysis DNS Name**
 - **Recent Malware Analysis DNS Name**
 - Added the following new lists to Recorded Future Domain Risk List:
 - **Frequently Abused Free DNS Provider**
 - **Historically Suspected Malware Operation**
 - **Recently Suspected Malware Operation**
 - **Recent Cryptocurrency Mining Pool**
 - Added the following new lists to Recorded Future IP Risk List
 - **Historical Malicious Infrastructure Admin Server**
 - **Recent Malicious Infrastructure Admin Server**
 - Added the following new lists to Recorded Future URL Risk List
 - **Historically Suspected Malware Distribution**
 - **Recently Suspected Malware Distribution**
 - **Recent Reported C&C URL**
 - **Historical Reported C&C URL**
- **Version 2.8.4**
 - Commonly updated attributes, such as attributes that involve timestamps and criticality, will now be updated when ingesting new data as opposed to creating duplicate attributes. See the Mapping Tables of each feed for details.
- **Version 2.8.3**

- Introduced a results limitation for the **Recorded Future Analyst Note** feed to resolve an offset issue.
- Added the following new **Topic** configuration options for the **Recorded Future Analyst Note** feed:
 - Geopolitical Intelligence Summary
 - Geopolitical Flash Event
 - Geopolitical Threat Forecast
 - Geopolitical Validated Event
 - Insikt Research Lead
 - Regular Vendor Vulnerability Disclosures
 - Sigma Rule
 - The Record by Recorded Future
- Added a new issue to the **Known Issues / Limitations** chapter regarding the API limit for the Analyst Notes and Alerts feeds.
- **Version 2.8.2**
 - Improved the **Recorded Future Alerts** feed to ingest more information regarding alerts.
 - Added new configuration field for the feed: **Save CVE Data As**.
 - Guide Update - updated Recorded Future Alerts sample response, default mapping table, Related Indicator Type mapping, and added a new Related Indicator Attributes mapping entry.
- **Version 2.8.1**
 - Updated the Recorded Future Alerts endpoint to API version 3.
 - Removed support from the following problematic lists:
 - Positive Malware Verdict
 - Historical Ransomware Distribution URL
 - Recent Ransomware Distribution URL
- **Version 2.8.0**
 - The integration now synchronizes Risk lists.
- **Version 2.7.0**
 - Added a new feed: Recorded Future Playbook Alerts.
 - Added the ability to filter by minimum risk score for the Risk List feeds (Recorded Future Domain Risk List, Recorded Future IP Risk List, Recorded Future URL Risk List, Recorded Future Vulnerability Risk List and Recorded Future Hash Risk List).
 - Added the ability to select the hash types that are ingested by the Recorded Future Hash Risk List, Recorded Future Analyst Note, and Recorded Future Alerts feeds.
 - Added the ability to ingest SHA-1 indicators.
- **Version 2.6.2**
 - Synchronized the Risk lists for the Risk List feeds to match option updates that Recorded Future performed.
 - Added time constrained data ingestion for all feeds so manual runs can be performed. Previously, the manual run option was only supported by the Analyst Note feed.
- **Version 2.6.1**
 - Fixed a parsing error that would occur when no evidence details are provided.
- **Version 2.6.0**
 - Removed lists from Recorded Future Domain Risk List feed:
 - Ransomware Distribution URL
 - Ransomware Payment DNS Name

- Removed lists from Recorded Future Vulnerability Risk feed:
 - Observed Exploit/Tool Development in the Wild
 - Historically Observed Exploit/Tool Development in the Wild
- **Version 2.5.0**
 - Refactored Recorded Future Feeds (aside from Analyst Note).
 - Fixed a bug that caused an Error applying FilterMapping error from the URL Risk List and other similar feeds.
 - Removed lists that are no longer support that would cause the feed to throw a 404 error. Lists removed include:
 - Recorded Future Domain Risk List:
 - C&C URL
 - Recorded Future URL Risk List:
 - C&C
 - Compromised URL
 - Historically Detected Malicious Browser Exploits
 - Recently Detected Malicious Browser Exploits
 - Recently Detected Suspicious Content
 - Historically Detected Suspicious Content
 - Recorded Future Vulnerability Risk List:
 - Recently Observed Exploit/Tool Development in the Wild
- **Version 2.4.1**
 - Fixed a parsing error with Analyst Note.
- **Version 2.4.0**
 - Added Alert details
- **Version 2.3.0**
 - Added support for MITRE Attack Pattern Sub-Techniques
 - Added 'Save CVE Data As' user configuration parameter for Recorded Future Vulnerability Risk List
- **Version 2.2.0**
 - Added support to multiple selection for list
 - Fixed issue with MITRE map
- **Version 2.1.0**
 - Added support for configuration list in the request
- **Version 2.0.1**
 - Fixed issue with attributes
- **Version 2.0.0**
 - Added Analyst Note Integration
- **Version 1.0.0**
 - Initial release