Recorded Future for IBM QRadar

A Threat Intelligence application for

Description, Installation, and Configuration Documentation

Updated for Recorded Future for QRadar, v3.1

Table of contents

Application description

Recorded Future is continuously harvesting data from Open, Deep, and Dark Web sources in real-time including Social media, Forums, Blogs, IRC channels, Paste sites, email groups, onion sites via TOR, and more through a range of collection mechanisms. Thousands of sources are added to our index for customers each week and are currently mining and cross-correlating data from over 750,000+ sources in seven languages with a patented Temporal Analytics™ Engine.

The Recorded Future application for IBM QRadar enables:

- Advanced enrichment of IP, domains, URLs, and hashes indicators with Risk Score and associated Evidence from Recorded Future SOAR API collected and analysed data directly in IBM QRadar product. Feature available when hovering with the mouse cursor over any field containing an IP value.
- Lookup functionality for IP, domains, hashes, and vulnerabilities via a dedicated Recorded Future tab within QRadar, providing in-app information about risk scores and risk evidence for any indicator.
- Delivery of malicious or potentially malicious IP, domains, URLs, and hashes (created based on custom Threshold, Risk Bandwidths, or associated rules/evidence) consumed in IBM QRadar as Reference Sets which can be used for searches and correlations.
- Delivery of malicious or potentially malicious CVE Risk Lists (created based on custom Threshold, Risk Bandwidths, or associated rules/evidence) consumed in IBM QRadar as Reference Sets which can be used for searches and correlations with QRadar Vulnerability Management.

Thus, the Recorded Future application for IBM QRadar, enables faster detection of threats, better offenses triage, more granular correlation logic based on risk score or evidence, minimization of time for offenses, and alerts investigation by adding relevant and comprehensive context.

System requirements

- IBM QRadar version 7.3.3 patch 6, 7.4.1 patch 2, 7.4.2.
- IBM QRadar Authorized Service Security Token
- Recorded Future API Token
- Recorded Future account for accessing content when pivoting outside IBM QRadar to the Recorded Future platform (https://www.recordedfuture.com/contact/)

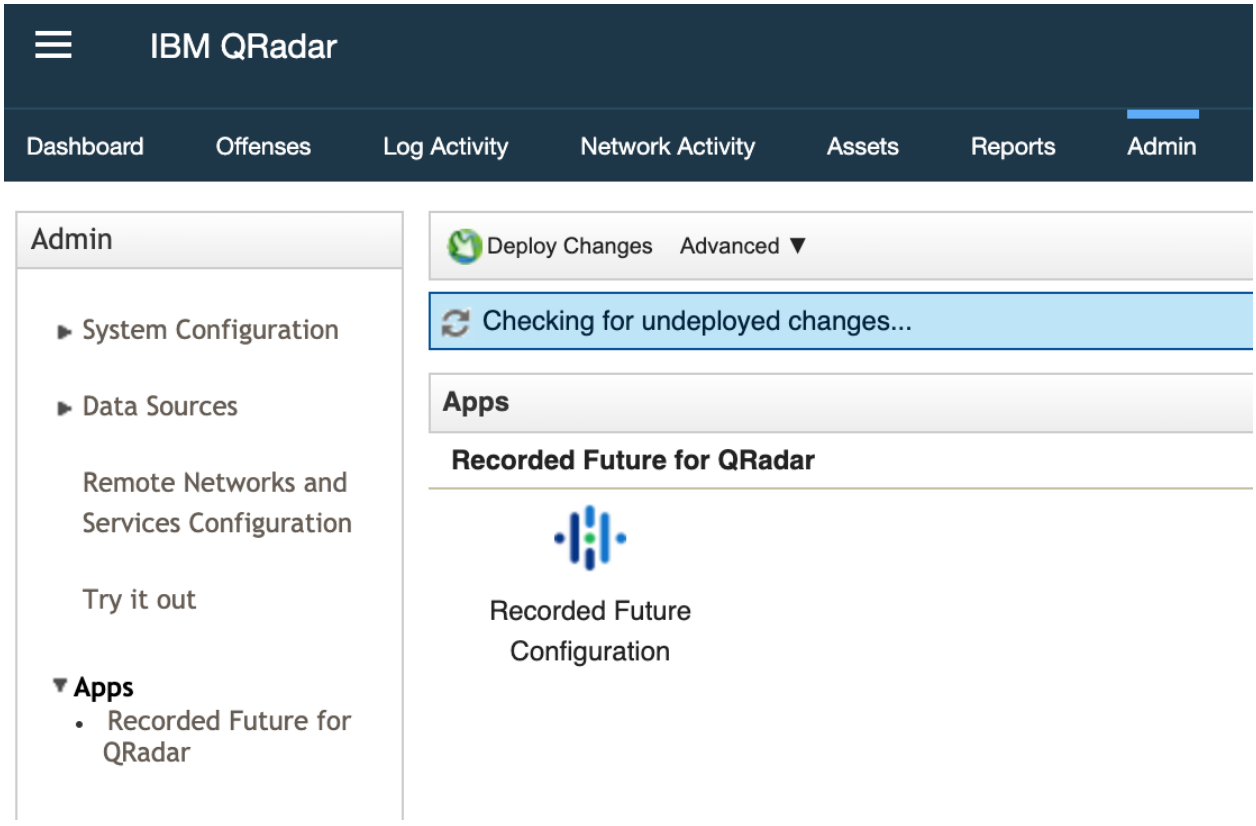
Installation

The preferred installation method for Recorded Future IBM QRadar application is through IBM's Security Application Exchange: https://exchange.xforce.ibmcloud.com/hub.

Please note that in case of upgrade of Recorded Future IBM QRadar version 2.x to version 3.x and higher it will be necessary to reenter all sensitive data in the configuration page (Recorded Future API token, proxy password, etc.)

Configuration

Once the Recorded Future application is installed, the "Recorded Future Configuration" icon should be already visible under the "Admin" tab from IBM QRadar in the "Plug-ins" sections.



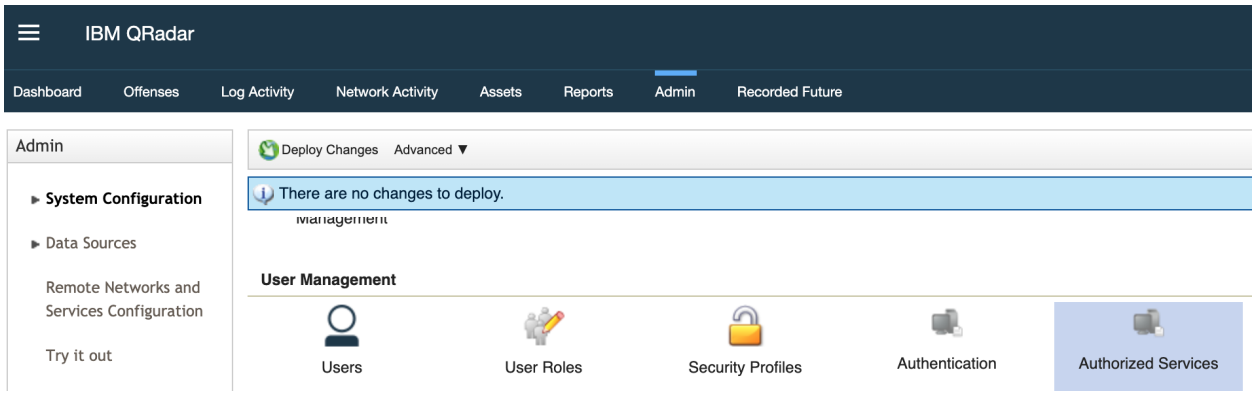
Adding an authorized service

The Recorded Future application requires an IBM QRadar Authorized Service Security Token to be able to populate Reference Sets with updated data.

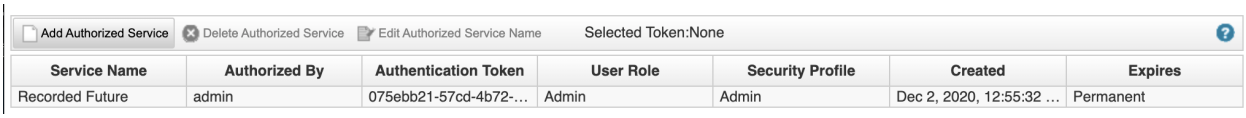
Note: QRoC customers get their AST from the "self Serve App" See: https://www.ibm.com/docs/en/qradar-on-cloud?topic=app-authorized-service-tokens

Please use the following steps to create such a Token that you can later use in the application configuration window:

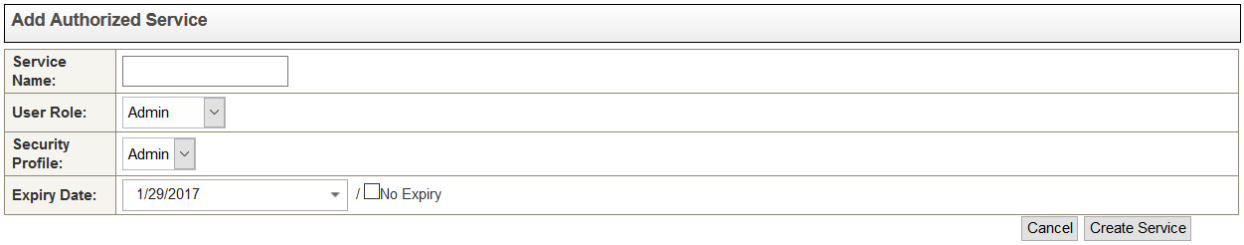
1. Click the “Admin” tab
2. On the navigation menu, click “System Configuration”
3. Click “Authorized Services”



4. Click “Add Authorized Service”

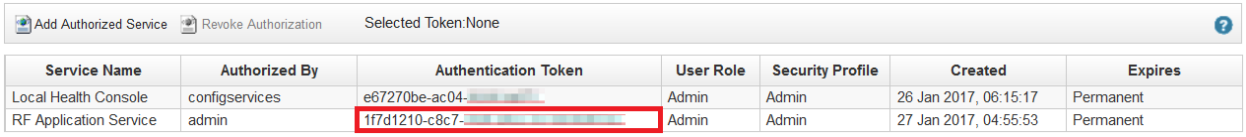


5. In the “Service Name” field, type a name for the authorized service.
6. From the “User Role” list, select “Admin”
7. Check “No Expiry” to ensure that the Token will never expire



8. Click “Create Service”

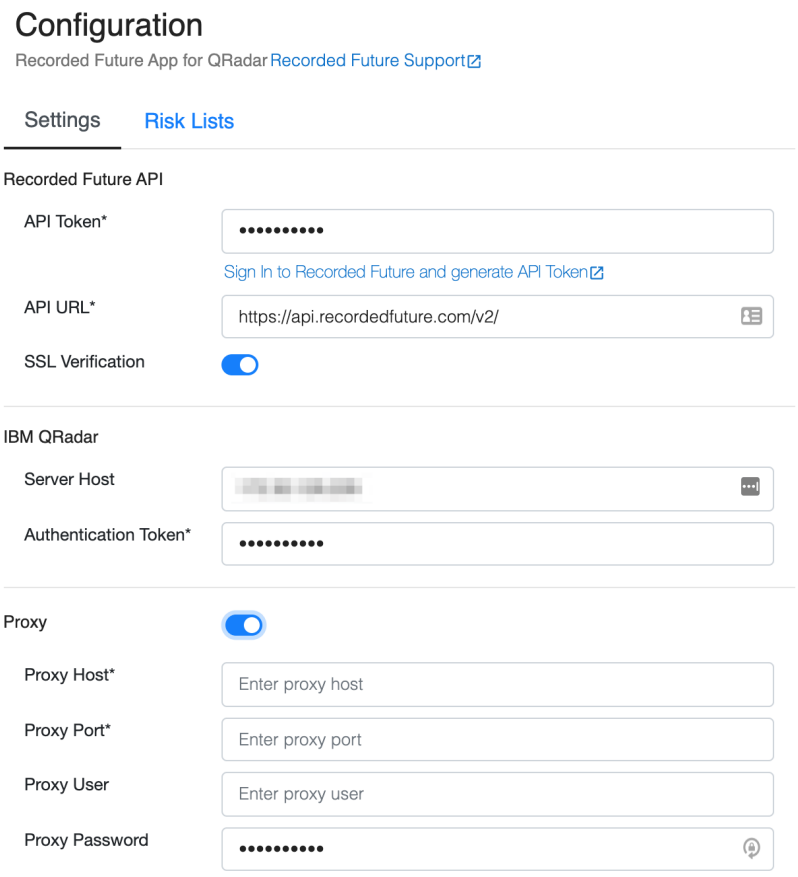
Once the service is created, the corresponding “Authentication Token” is displayed and can be copied from the list of Authorized Services.



Service Name	Authorized By	Authentication Token	User Role	Security Profile	Created	Expires
Local Health Console	configservices	e67270be-ac04-	Admin	Admin	26 Jan 2017, 06:15:17	Permanent
RF Application Service	admin	1f7d1210-c8c7-	Admin	Admin	27 Jan 2017, 04:55:53	Permanent

Recorded Future application configuration

The configuration page for the Recorded Future application, the name “Recorded Future Configuration” can be found in the “Admin” tab in the “Plug-ins” section. Once opened the configuration page will enable configuration of the following parameters on the “Settings” tab:



Recorded Future

- API Token - Recorded Future API Token
- API URL - URL of the Recorded future API instance
- SSL Verification switch - Allows to disable SSL certificates verification

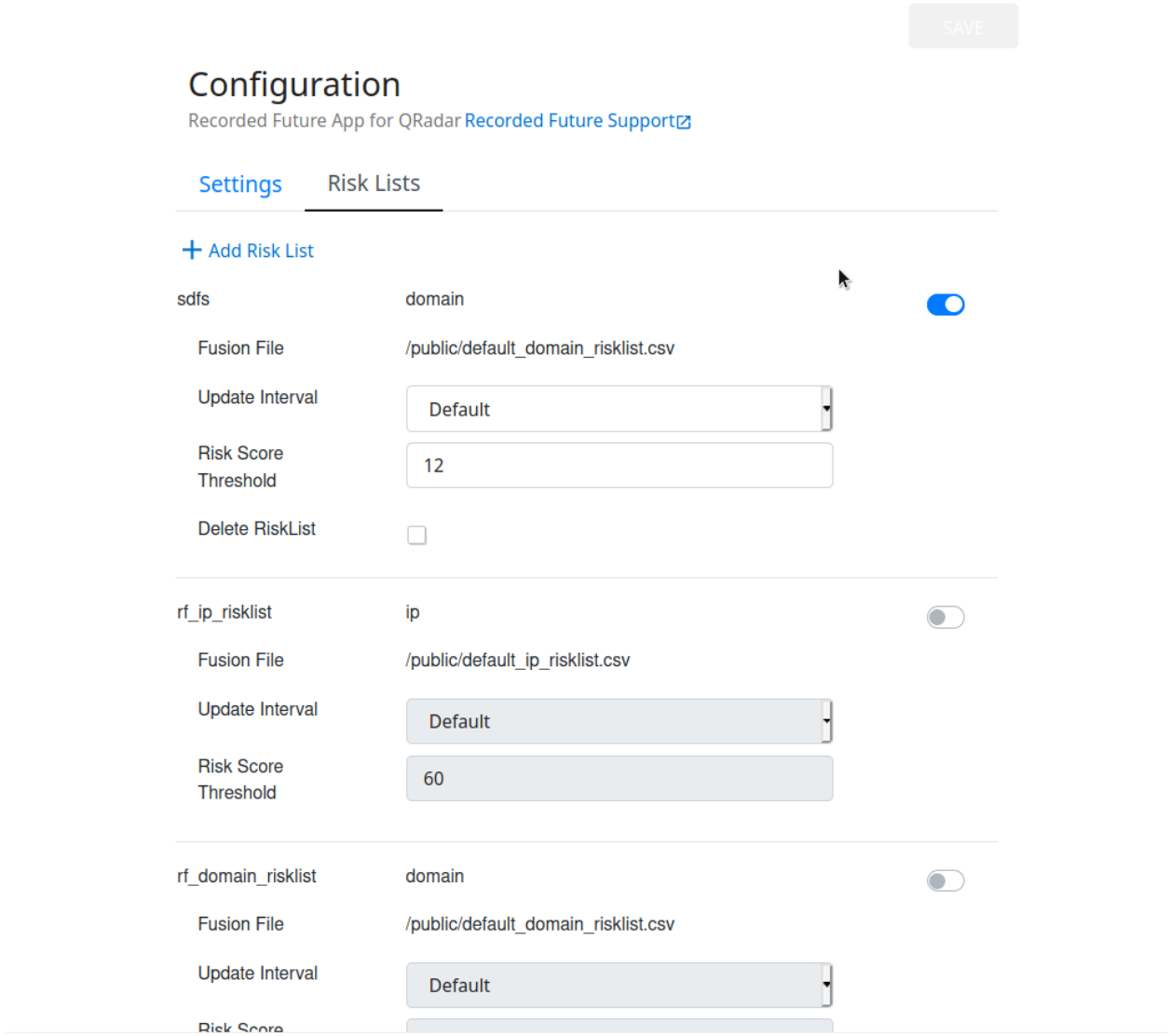
Proxy Settings

- Enabled Switch - parameter that controls the usage or not of an intermediary proxy server for connection between the Recorded Future app and Recorded Future online services (API)
- Host - refers to the proxy server connection address
- Port - refers to the proxy server connection port
- Username (optional) - refers to the username required for authentication to the proxy server
- Password (optional) - refers to the password required for authentication to the proxy server

IBM QRadar

- Server IP - parameter control the IP of the QRadar console server the Recorded Future app will be used for connection and population of the Reference Sets (by default it is automatically populated with the public QRadar console server IP)
  NOTE: For QRoC clients, the QRadar console FQDN should be used instead of an IP address.
- Server Token - refers to the “Authorized Service Security Token” associated to the “Authorized Service” created at the previous steps

The “Risk lists” tab allows configuring what Recorded Future risk lists will be used to create Reference Sets in IBM QRadar. It displays a list of currently configured risk lists:



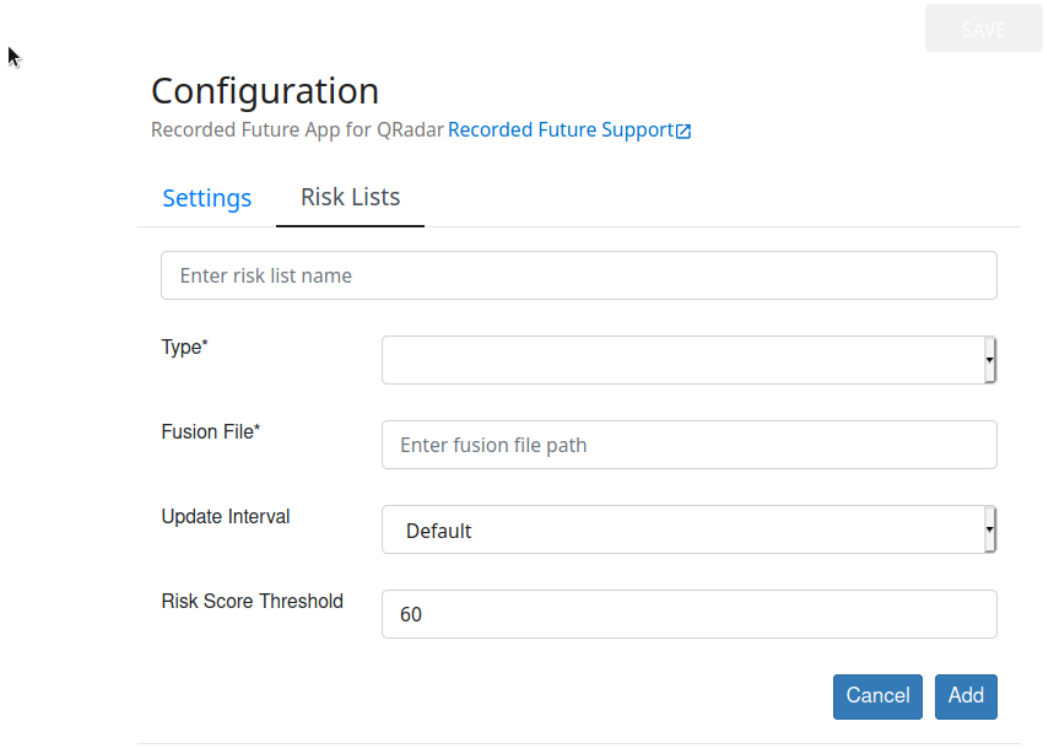
There are two types of risk lists:

- Predefined that are shipped with the Recorded Future app
- Custom that are created by users

The following controls are available for existing risk lists:

- Enable Switch - when disabled the risk list will not be downloaded and the related reference sets will be purged.
- Update interval - controls how often the risk list data will be updated. “Default” means to update data as soon as it changes on Recorded Future side.
- Risk Score Threshold - contains the minimum risk score an entity should have to be included in the “Score” reference set.
- Delete risk list - custom risk lists can be deleted by checking this checkbox and hitting SAVE button.

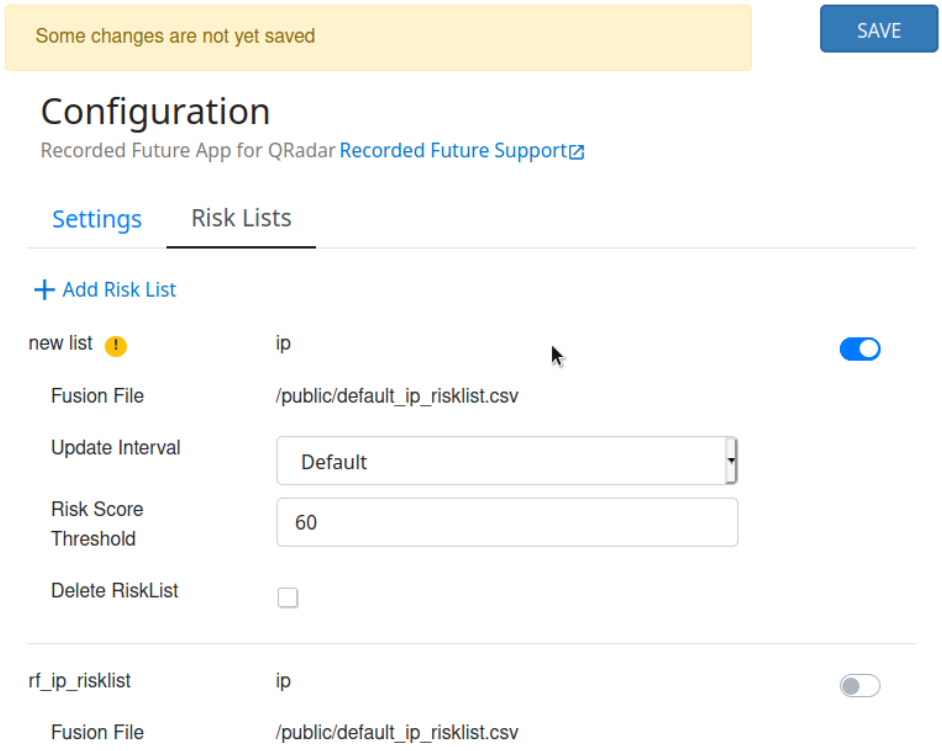
To create custom risk list click “Add risk list” link. Add risk list form will open:



The form controls are:

- Name - unique name of the risk list. Will be included in the names of reference sets based on this risk list.
- Type - type of the entities provided by the risk list. Can be one of Domain, URL, Hask, IP, or Vulnerability.
- Fusion File - path to the Recorded Future fusion file containing the risk list.
- Update Interval - how often to check the fusion file for updates. “Default” means to download updates as soon as they are available.
- Risk Score Threshold - contains the minimum risk score an entity should have to be included in the “Score” reference set.

After all the files have been filled click the “Add” button. New risk list will be added to the list:



The "!" badge next to the risk list name means that the risk list has not been saved to the configuration yet. After adding all the required risk lists click the SAVE button to save changes to the configuration.

Multi-Tenant Configuration

The app now supports multi-tenant configurations. One instance of the app has to be created for each tenant that needs access to our data. This also means that each tenant can have a different configuration and no data is shared. Use the IBM® QRadar® Assistant app to manage your app and content extension inventory, view app and content extension for you r multi tenant environment.
See: https://www.ibm.com/docs/en/qradar-common?topic=app-managing-multitenant-apps

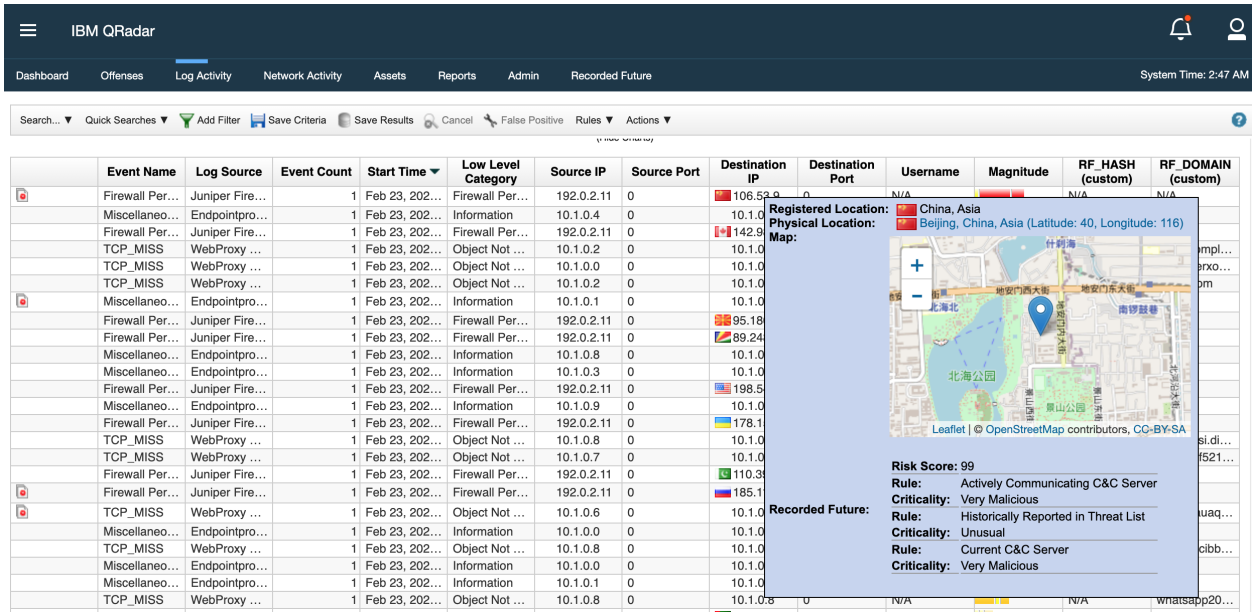
Application functionality

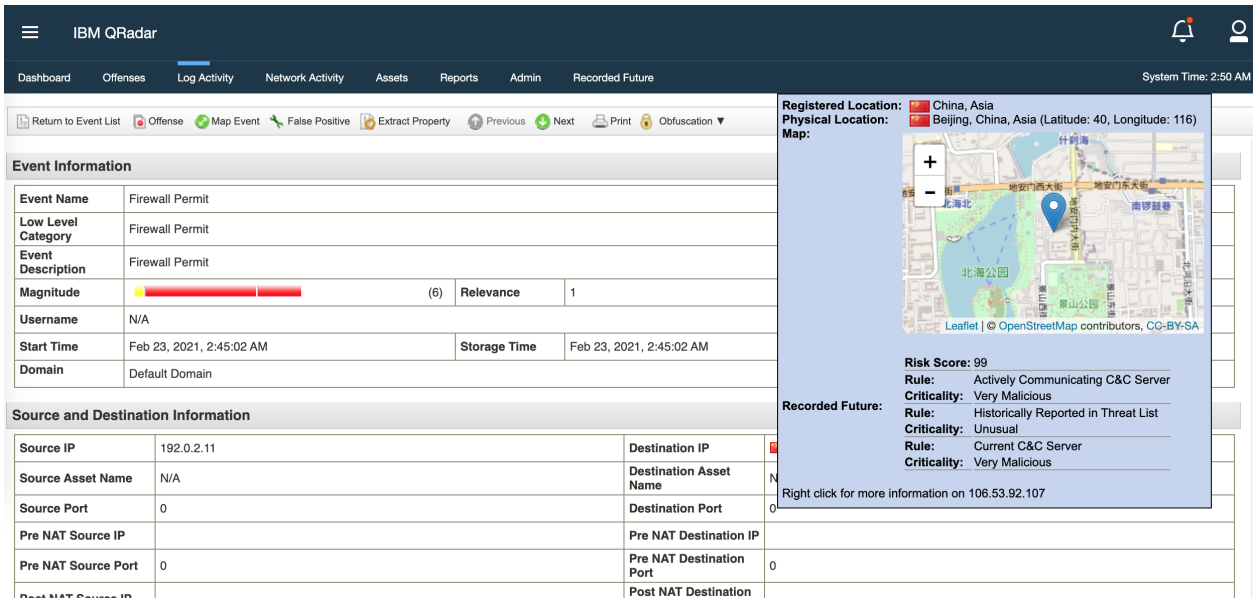
Recorded Future application's functionality is underpinned by the Recorded Future API, which is the repository from which QRadar retrieves the relevant data. The Recorded Future app. automates enrichment of indicators, enables pivoting to additional context, and orchestrates the ingestion of indicators levering the new QRadar application framework to facilitate advanced searches and correlation.

IP Enrichment in IBM QRadar

The Recorded Future application enables users to get a fast understanding of IP risk level directly in IBM QRadar UI by hovering the mouse cursor over a field containing an IP Address. The data enriched for an IP, when performing such action is:

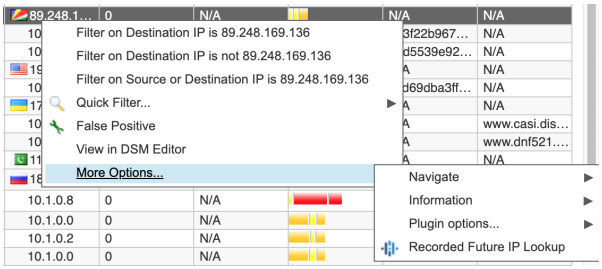
- IP Criticality level - Very Malicious, Malicious or Suspicious
- Recorded Future Risk Score
- Number of Recorded Future rules that generated the score
- The Recorded Future rules/evidence that contributed to the score

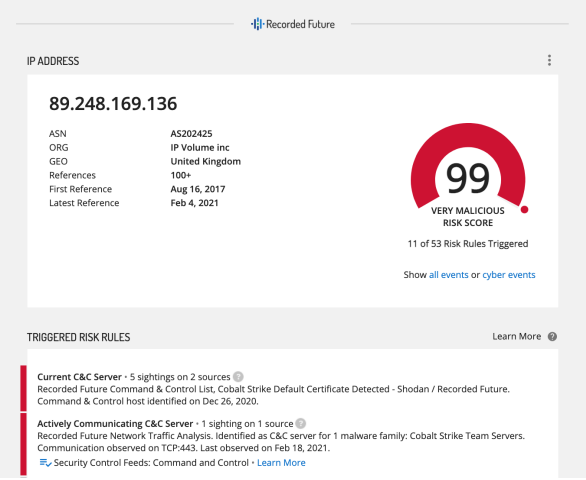




IP Lookups on Recorded Future

The Recorded Future application enables users to get a deeper understanding of IP risk level and associated context by pivoting to the Recorded Future platform and visualizing the IP Intel Card. This is possible via the right-click menu option presented for any field containing an IP Address.





Correlation and advanced searches

Recorded Future application enables correlation and advanced searches based on IP Reference Sets that are updated on the time interval set in the application configuration. A

series of Reference Sets are automatically created as soon as the application is properly configured, that provide high flexibility to the users wanting to identify threats that might impact their company:

1. A reference set created based on the custom Score threshold

Name	Type	Number of Elements	Associated Rules
RF - Score	IP	2,312	0

2. Reference sets created based on the risk bandwidths recommended by Recorded Future

RF - Very Malicious	IP	1,969	0
RF - Malicious	IP	76,293	0

3. Reference sets created based on the evidences/rules associated to each of the IPs known and scored by Recorded Future.

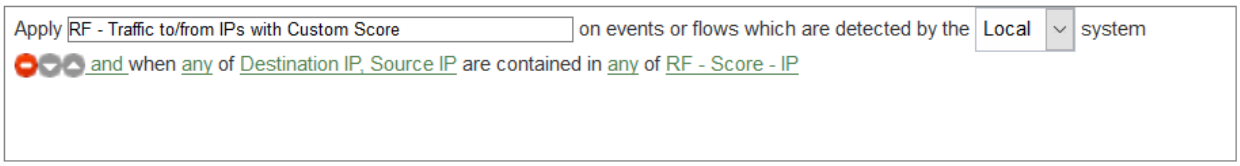
Name	Type	Number of Elements	Associated Rules
RF - Current C2C Server	IP	1,969	0
RF - Recent Positive Malware Verdict	IP	13,098	0
RF - Recently Linked to Intrusion Method	IP	18,411	0
RF - Malicious Packet Source	IP	12,103	0
RF - Recent Threat Researcher	IP	12,362	0
RF - Recent Botnet Traffic	IP	867	0
RF - Phishing Host	IP	23,329	0
RF - Recent Multicategory Blacklist	IP	92,176	0
RF - Recent Honeypot Sighting	IP	65,491	0
RF - Tor Node	IP	7,104	0
RF - Recent Open Proxies	IP	87,793	0
RF - Recent SSH or Dictionary Attacker	IP	2,448	0

More than 35 rules/evidence are available in Recorded Future data associated to IPs and all of them can be used for a granular correlation logic and proper identification of specific or relevant threats to the company. Additional details about the rules can be found here: https://support.recordedfuture.com/hc/en-us/articles/115000897208-Risk-Scoring-in-Recorded-Future.

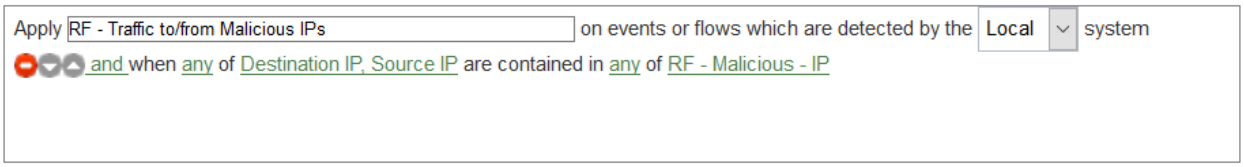
Further on, based on these Reference Sets, you can create rules for correlation against log or network activity or perform advanced searches.

Correlation rules examples

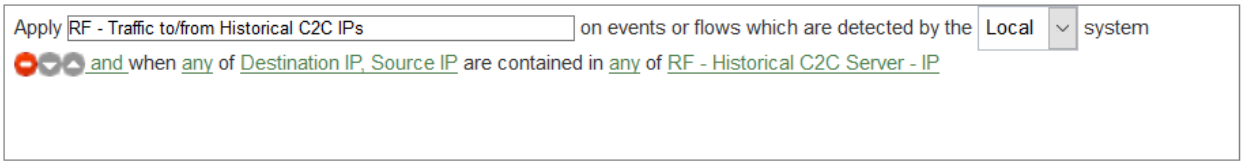
1. Identify any traffic to/from IPs, found in IBM QRadar's log or network activity, that has a Recorded Future risk score higher or equal to a threshold (set up in the application configuration window)



2. Identify any traffic to/from IPs, found in IBM QRadar's log or network activity, that is considered by Recorded Future as being malicious



3. Identify any traffic to/from IPs, found in IBM QRadar's log or network activity, that are known by Recorded Future as "Historical C&C Servers"



Advanced searches example

This returns all Destination IP's that have been matched against the "RF - rf_ip_risklist - Very Malicious" Reference set.

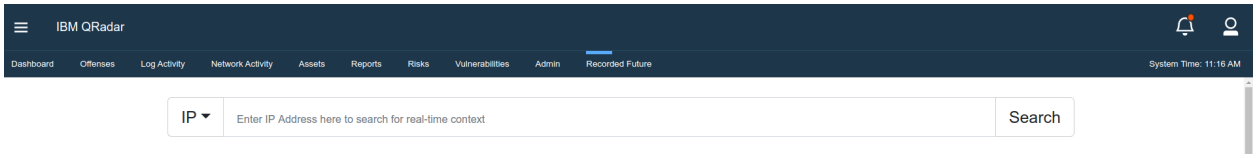
SELECT destinationip AS "Destination IP", Count(*) AS 'Count' from events where (referencesetcontains('RF - rf_ip_risklist - Very Malicious', "destinationip")) GROUP BY destinationip order by "Count" LAST 720 HOURS

This returns all Destination IP's that have been matched against the "RF - rf_ip_risklist - Very Malicious" Reference set.

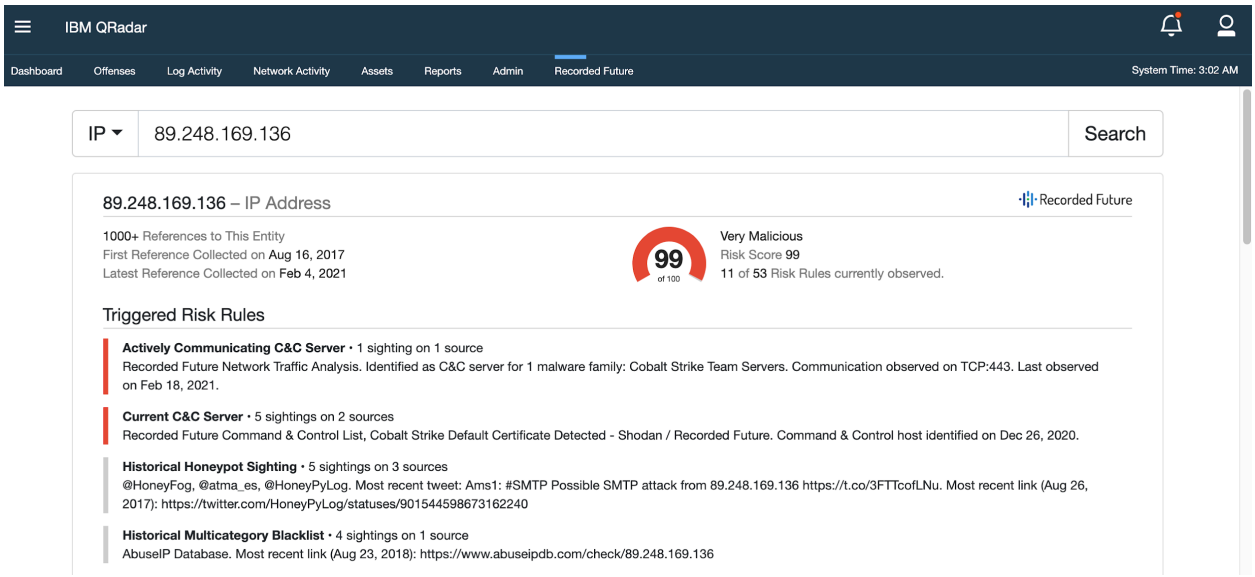
Intelligence Cards in QRadar

Intelligence Cards allow you to quickly see a variety of information about a given IP, domain, hash, URL or vulnerability within Recorded Future. Related entities such as malware and other IPs, domains and hashes are shown, as well as when the entity was first and last seen. Intelligence Cards can be viewed directly within QRadar. To get Intelligence card for an entity:

1. Click the “Recoded Future” tab. The Recoreded Future enrichment page will open



2. Select entity type from the dropdown on the left.
3. Enter an entity to search data for (IP address, domain name etc.)
4. Click the “Search” button. If entity is known to the Recorded Future the intelligence card will be shown:



Logging & Troubleshooting

Please refer to the following URL for instructions on how to download QRadar Application logs.
https://www.securitylearningacademy.com/course/view.php?id=4818