# Recorded Future for IBM QRadar

A Threat Intelligence application for

Description, Installation, and Configuration Documentation

*Updated for Recorded Future for QRadar,* v3.1.3

# Table of contents


Table of contents

Application description

System requirements

Installation

Configuration
- Adding an authorized service
- Recorded Future application configuration

Application functionality
- IP Enrichment in IBM QRadar
- IP Lookups on Recorded Future
- IP, domain, file hash, and vulnerability lookups within dedicated QRadar tab
- Correlation and advanced searches
  - Correlation rules examples
  - Advanced searches example
- Recorded Future Alerts [v3.1.1]

Logging & Troubleshooting

Appendix
- **Appendix 1** - Recorded Future reference set name changes

# 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

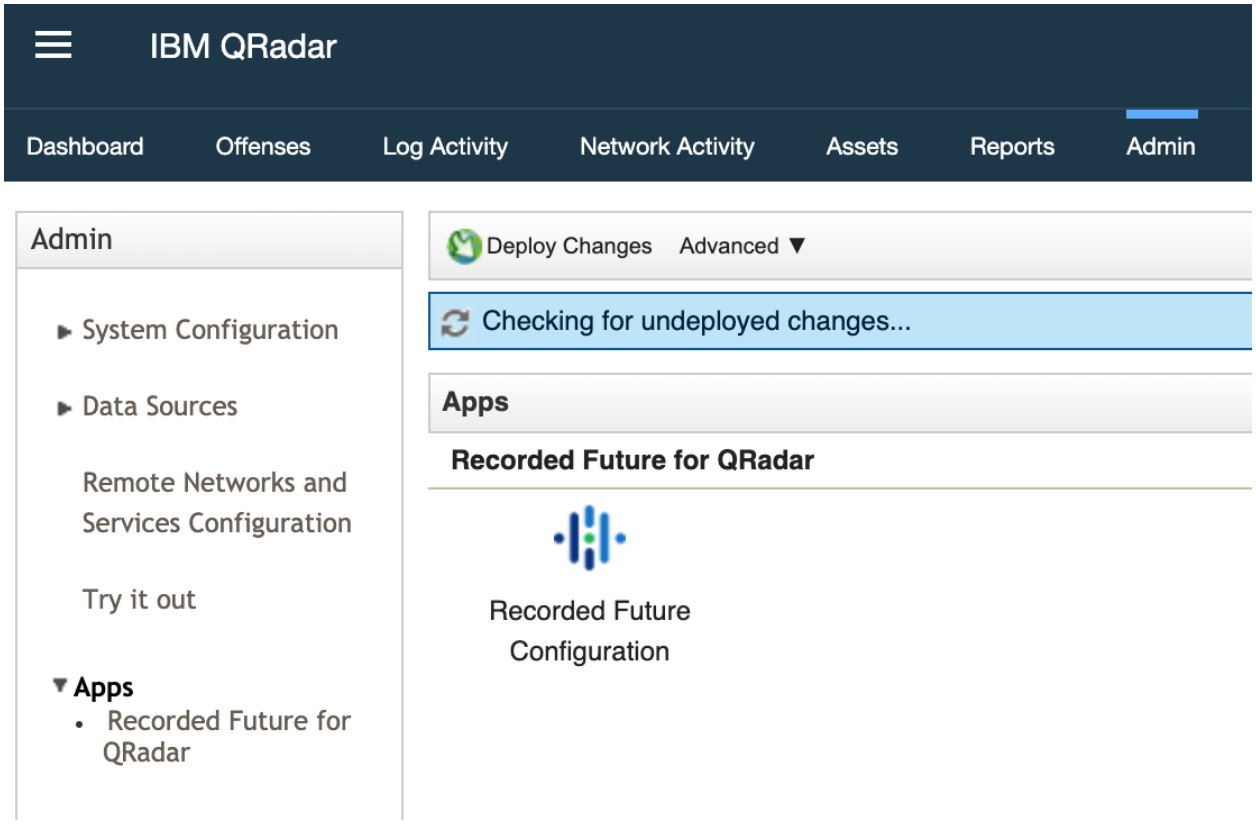
The preferred installation method for Recorded Future IBM QRadar application is through IBM's Security Application Exchange: https://exchange.xforce.ibmcloud.com/hub.

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.)

*****If you are upgrading from Recorded Future for QRadar v1.x or v2.x to v3.x, you will need a new Recorded Future API token Please submit an integration support ticket to Recorded Future issue a new token for Recorded Future v3.x *****

# 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.



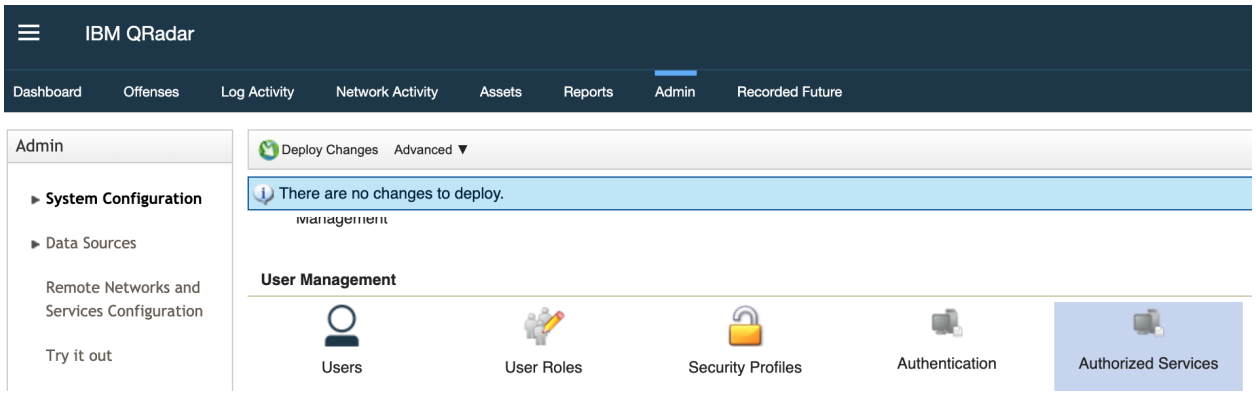
## Adding an authorized service

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

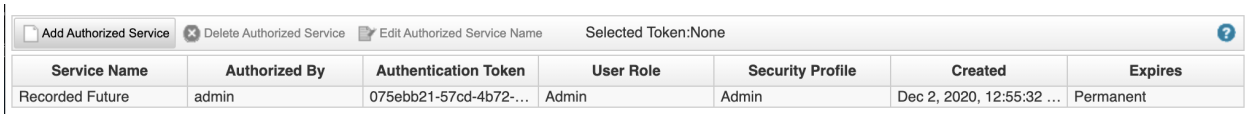
**Note**: QRoC customers get their AST from the "self Serve App" See: https://www.ibm.com/docs/en/qradar-on-cloud?topic=app-authorized-service-tokens

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

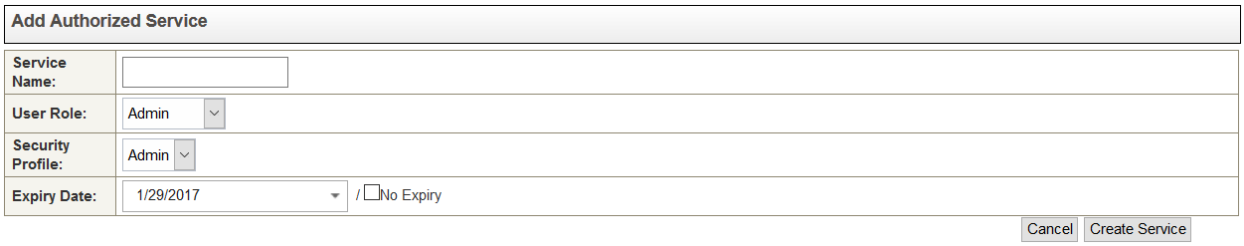
1. Click the “Admin” tab
2. On the navigation menu, click “System Configuration”
3. Click “Authorized Services”




4. Click “Add Authorized Service”

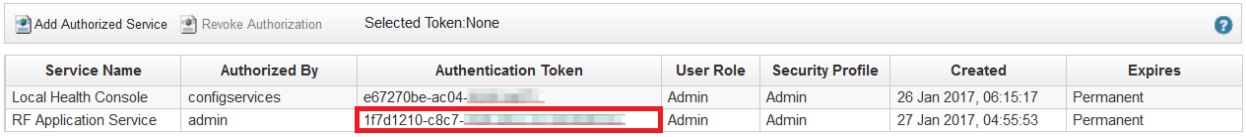



5. In the “Service Name” field, type a name for the authorized service.
6. From the “User Role” list, select “Admin”
7. Check “No Expiry” to ensure that the Token will never expire




8. Click “Create Service”

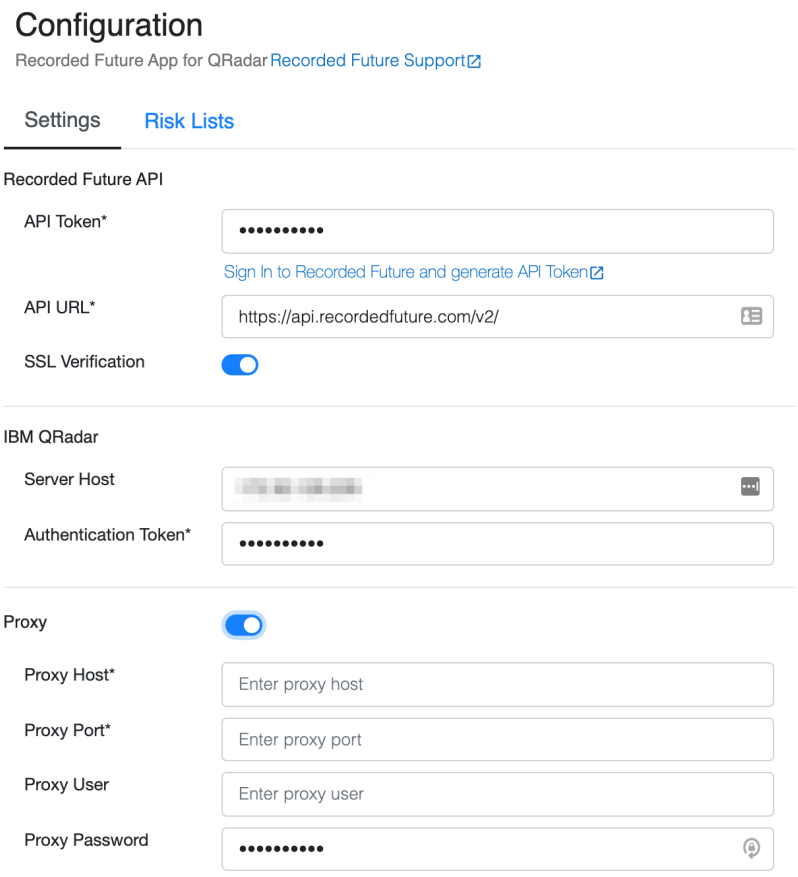
Once the service is created, the corresponding “Authentication Token” is displayed and can be copied from the list of Authorized Services. New in 7.4.3 The authorized service token cannot be made visible after you close the Authorized Service Created Successfully dialog. Copy the token to a secure location before you close the dialog. Link for reference: https://www.ibm.com/docs/en/qsip/7.5?topic=services-adding-authorized-service




| 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

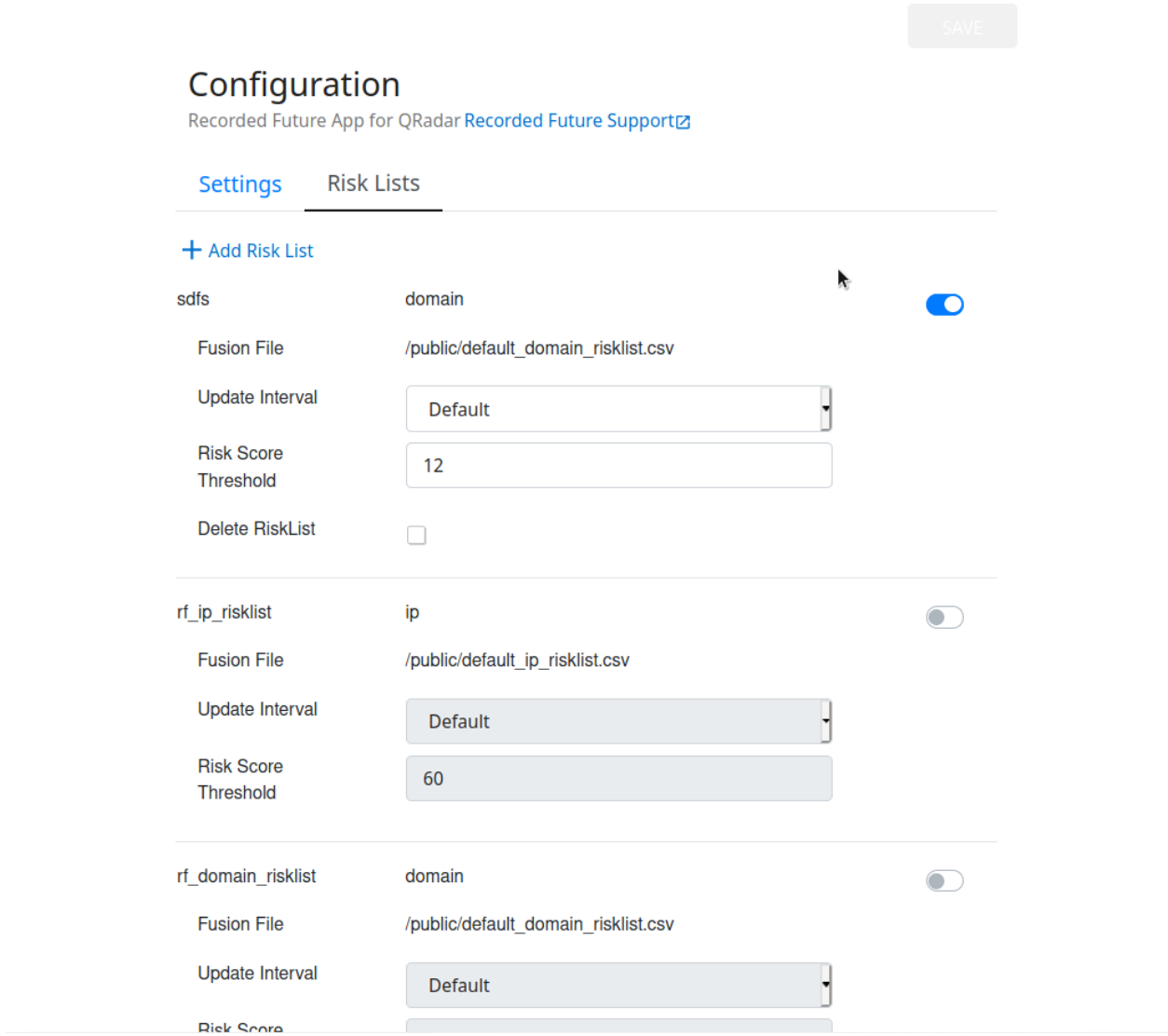
**Proxy Settings**

- 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:



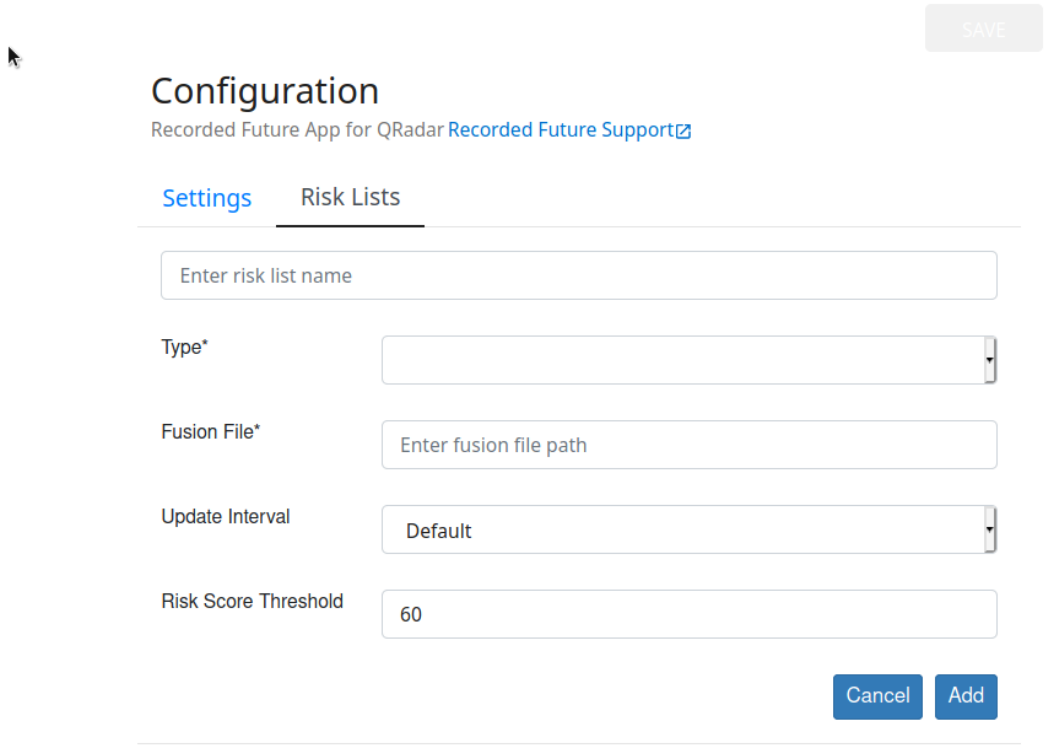

There are two types of risk lists:

- 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.

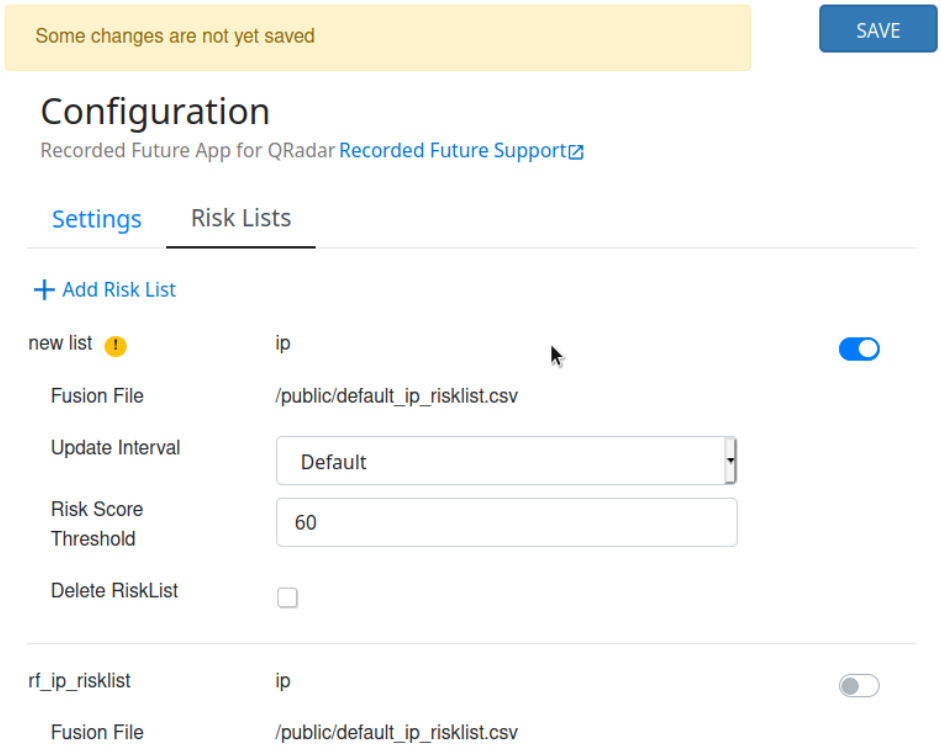
To create custom risk list click “Add risk list” link.  Add risk list form will open:




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

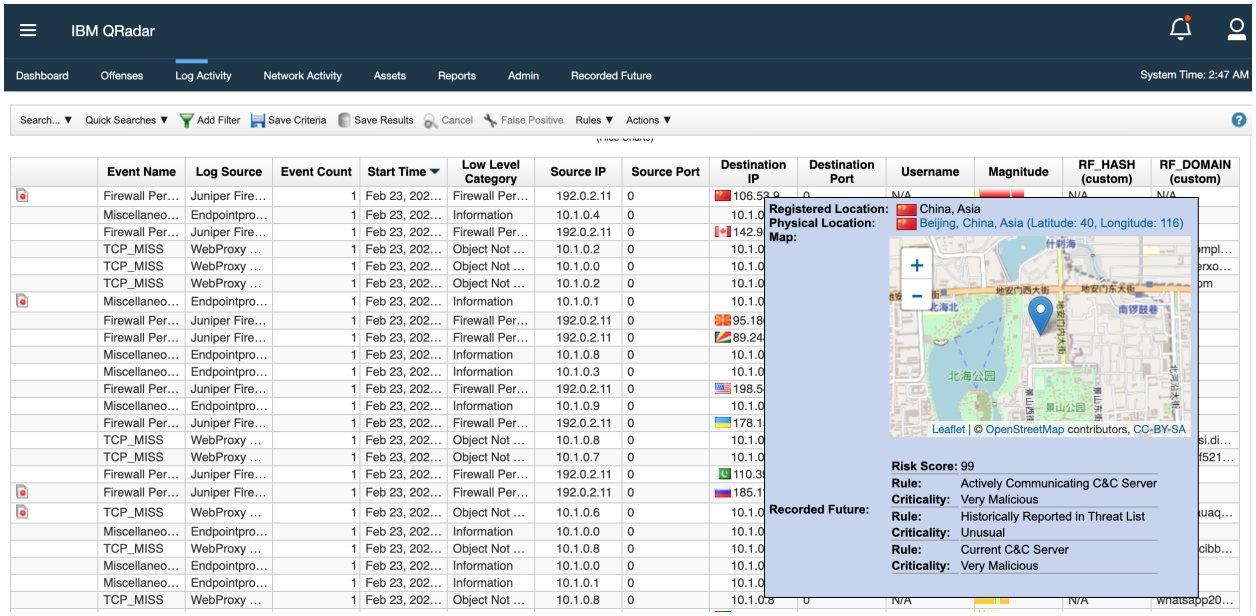
# Application functionality

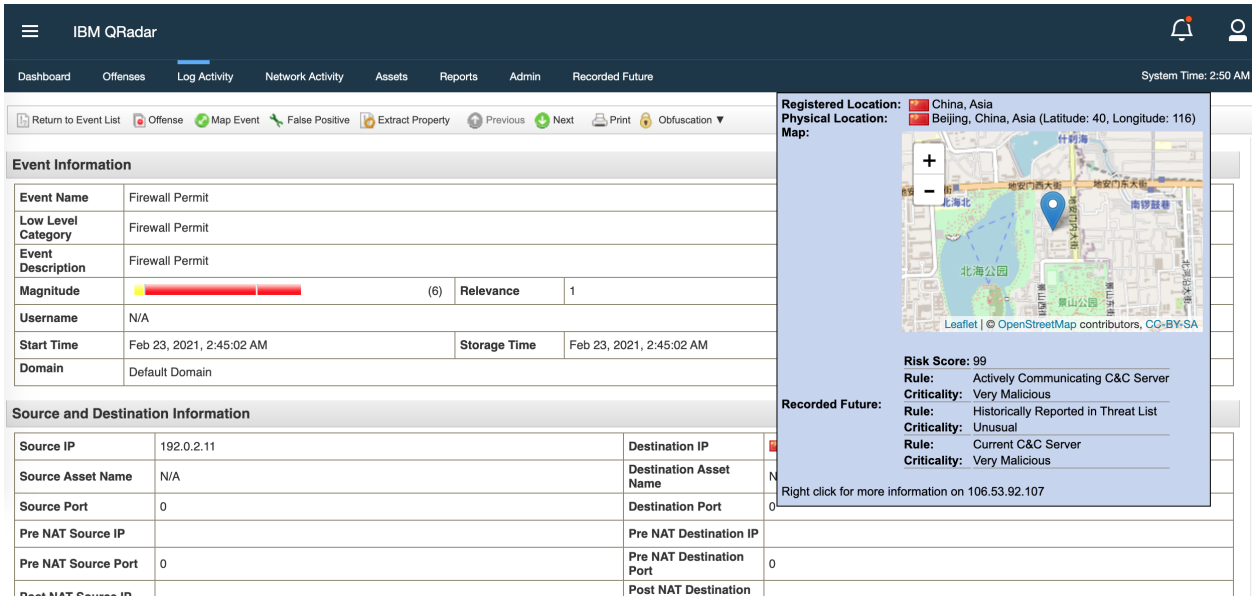
Recorded Future application's functionality is underpinned by the Recorded Future API, which is the repository from which QRadar retrieves the relevant data. The Recorded Future app automates enrichment of indicators, enables pivoting to additional context, and orchestrates the ingestion of indicators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

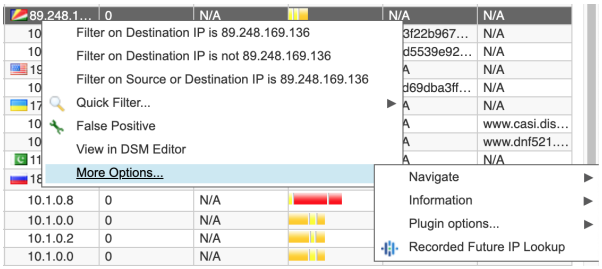
- IP Criticality level - Very Malicious, Malicious or Suspicious
- Recorded Future Risk Score
- Number of Recorded Future rules that generated the score
- The Recorded Future rules/evidence that contributed to the score

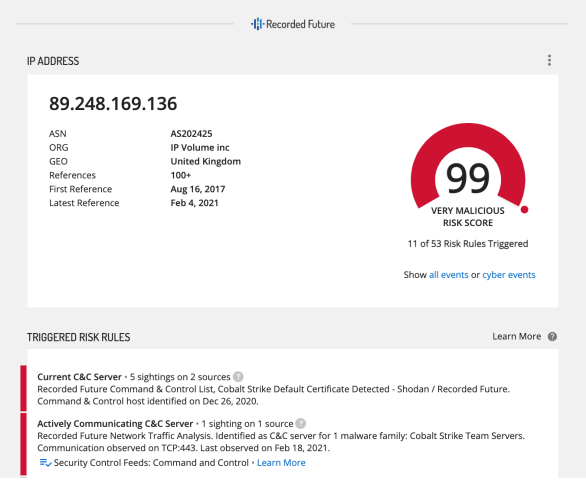





## IP Lookups on Recorded Future

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.

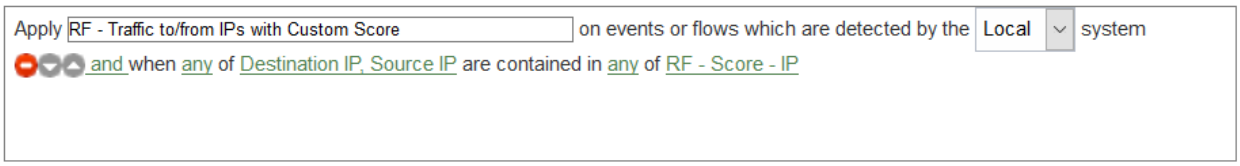
| Name | Type | Number of Elements | Associated Rules |
|---|---|---|---|
| RF - Current C2C Server | IP | 1,969 | 0 |
| RF - Recent Positive Malware Verdict | IP | 13,098 | 0 |
| RF - Recently Linked to Intrusion Method | IP | 18,411 | 0 |
| RF - Malicious Packet Source | IP | 12,103 | 0 |
| RF - Recent 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.

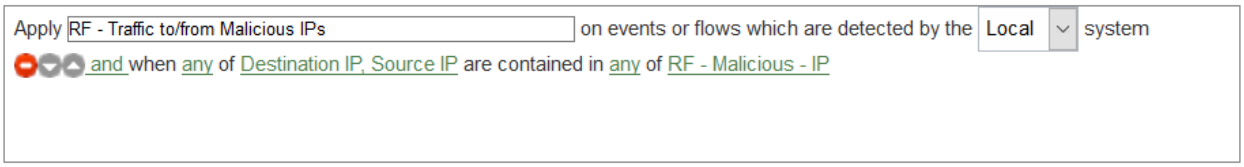
Further on, based on these Reference Sets, you can create rules for correlation against log or network activity or perform advanced searches.

### Correlation rules examples

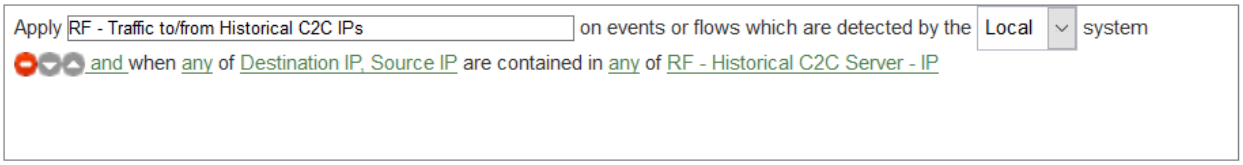
1. Identify any traffic to/from IPs, found in IBM QRadar's log or network activity, that has a Recorded Future risk score higher or equal to a threshold (set up in the application configuration window)




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.

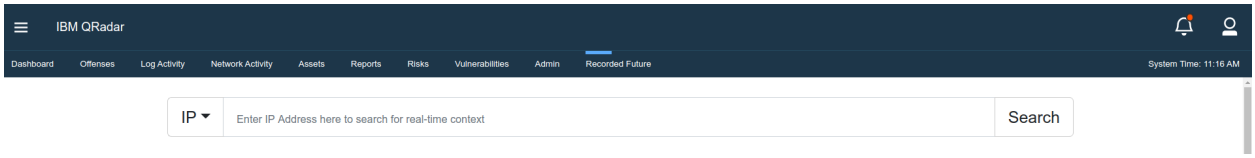
*SELECT destinationip AS "Destination IP", Count(*) AS 'Count' from events where ( referencesetcontains('RF - rf_ip_risklist - Very Malicious', "destinationip")) GROUP BY destinationip order by "Count" LAST 720 HOURS*

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

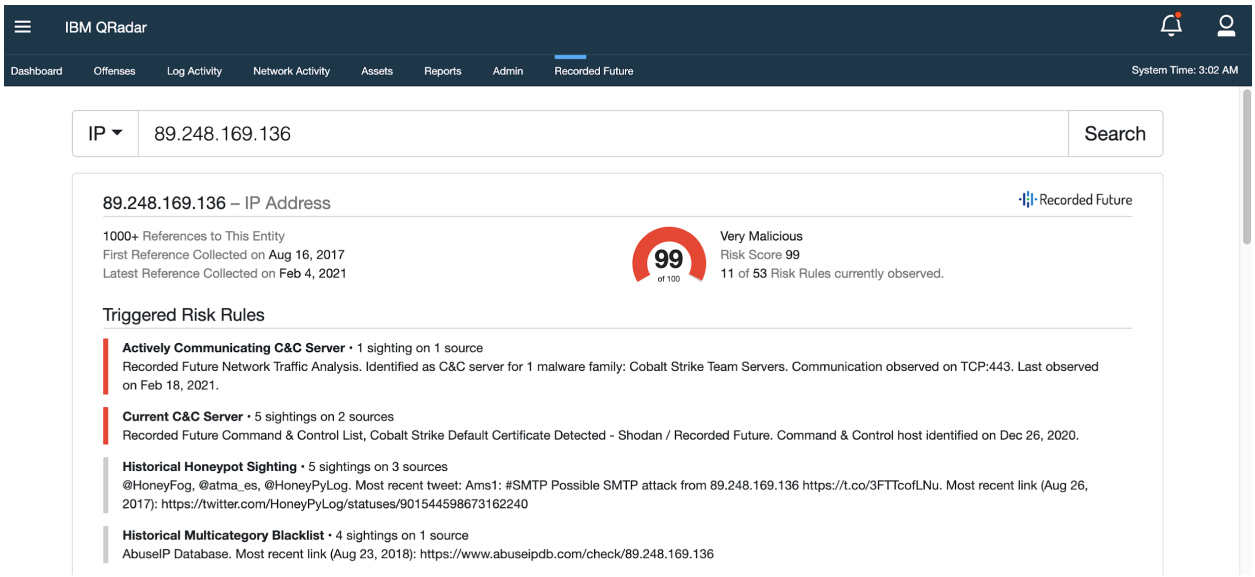
## Intelligence Cards in QRadar

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:




## Recorded Future Alerts Tab

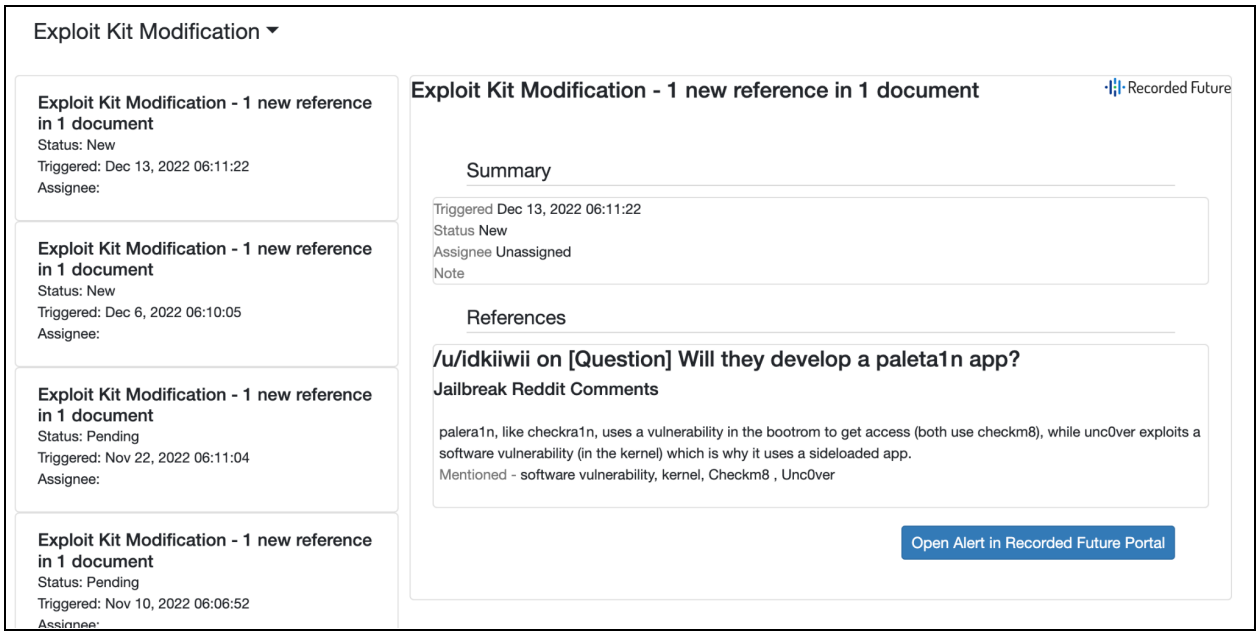
Recorded Future Alerts can now be brought into QRadar as of v3.1.1. This functionality is limited to viewing Recorded Future alerts details inside of QRadar. All alerts that are configured for a client’s Recoded Future enterprise will become available in the Recorded Future for QRadar App once the app is set up. Once in the ‘Recorded Future Alerts’ tab, end users can select which alert type they would like to view in QRadar using the alert drop down menu. Users can pivot from QRadar to the Recorded Future portal to begin triaging the Recorded Future alert.




*Click the ‘Recorded Future Alerts’ Tab*




*Select the alert type to view all relevant alerts*




*Select specific alert from the list on the left panel to view the details of the alert on the right*




*Use the 'Open Alert in Recorded Future Portal' button to pivot and view the full details of the alert*

# 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

# Appendix

**Appendix 1** - Recorded Future reference set name changes: Changes to the Recorded Future reference set were changed in the Recorded Future for QRadar v3.1 release. See below for the new reference set name mappings

| **Old format – "RF – ENTITYTYPE – RISKRULE"** | **New format – "RF – FUSIONFILENAME – RISKRULE"** |
|---|---|
| RF - Domain - Active Phishing URL | RF - rf_domain_risklist - Active Phishing URL |
| RF - Domain - Compromised URL | RF - rf_domain_risklist - Compromised URL |
| RF - Domain - Historical C&C DNS Name | RF - rf_domain_risklist - Historical C&C DNS Name |
| RF - Domain - Historical COVID-19-Related Domain Lure | RF - rf_domain_risklist - Historical COVID-19-Related Domain Lure |
| RF - Domain - Historical Malware Analysis DNS Name | RF - rf_domain_risklist - Historical Malware Analysis DNS Name |
| RF - Domain - Historical Phishing Lure | RF - rf_domain_risklist - Historical Phishing Lure |
| RF - Domain - Historical Punycode Domain | RF - rf_domain_risklist - Historical Punycode Domain |
| RF - Domain - Historical Threat Researcher | RF - rf_domain_risklist - Historical Threat Researcher |
| RF - Domain - Historical Typosquat Similarity - DNS Sandwich | RF - rf_domain_risklist - Historical Typosquat Similarity - DNS Sandwich |
| RF - Domain - Historical Typosquat Similarity - Typo or Homograph | RF - rf_domain_risklist - Historical Typosquat Similarity - Typo or Homograph |
| RF - Domain - Historically Active Weaponized Domain | RF - rf_domain_risklist - Historically Active Weaponized Domain |
| RF - Domain - Historically Detected Malware Operation | RF - rf_domain_risklist - Historically Detected Malware Operation |
| RF - Domain - Historically Detected Phishing Techniques | RF - rf_domain_risklist - Historically Detected Phishing Techniques |
| RF - Domain - Historically Linked to Cyber Attack | RF - rf_domain_risklist - Historically Linked to Cyber Attack |
| RF - Domain - Historically Referenced by Insikt Group | RF - rf_domain_risklist - Historically Referenced by Insikt Group |
| RF - Domain - Historically Reported as a Defanged DNS Name | RF - rf_domain_risklist - Historically Reported as a Defanged DNS Name |
| RF - Domain - Historically Reported by DHS AIS | RF - rf_domain_risklist - Historically Reported by DHS AIS |
| RF - Domain - Historically Reported by Insikt Group | RF - rf_domain_risklist - Historically Reported by Insikt Group |
| RF - Domain - Historically Reported Fraudulent Content | RF - rf_domain_risklist - Historically Reported Fraudulent Content |
| RF - Domain - Historically Reported in Threat List | RF - rf_domain_risklist - Historically Reported in Threat List |
| RF - Domain - Historically Reported Spam or Unwanted Content | RF - rf_domain_risklist - Historically Reported Spam or Unwanted Content |
| RF - Domain - Malicious | RF - rf_domain_risklist - Malicious |
| RF - Domain - Newly Registered Certificate With Potential for Abuse - DNS Sandwich | RF - rf_domain_risklist - Newly Registered Certificate With Potential for Abuse - DNS Sandwich |

| | |
|---|---|
| RF - Domain - Newly Registered Certificate With Potential for Abuse - Typo or Homograph | RF - rf_domain_risklist - Newly Registered Certificate With Potential for Abuse - Typo or Homograph |
| RF - Domain - Recent C&C DNS Name | RF - rf_domain_risklist - Recent C&C DNS Name |
| RF - Domain - Recent COVID-19-Related Domain Lure: Malicious | RF - rf_domain_risklist - Recent COVID-19-Related Domain Lure: Malicious |
| RF - Domain - Recent Fast Flux DNS Name | RF - rf_domain_risklist - Recent Fast Flux DNS Name |
| RF - Domain - Recent Phishing Lure: Malicious | RF - rf_domain_risklist - Recent Phishing Lure: Malicious |
| RF - Domain - Recent Phishing Lure: Suspicious | RF - rf_domain_risklist - Recent Phishing Lure: Suspicious |
| RF - Domain - Recent Punycode Domain | RF - rf_domain_risklist - Recent Punycode Domain |
| RF - Domain - Recent Threat Researcher | RF - rf_domain_risklist - Recent Threat Researcher |
| RF - Domain - Recent Typosquat Similarity - DNS Sandwich | RF - rf_domain_risklist - Recent Typosquat Similarity - DNS Sandwich |
| RF - Domain - Recent Typosquat Similarity - Typo or Homograph | RF - rf_domain_risklist - Recent Typosquat Similarity - Typo or Homograph |
| RF - Domain - Recently Active Weaponized Domain | RF - rf_domain_risklist - Recently Active Weaponized Domain |
| RF - Domain - Recently Detected Malware Operation | RF - rf_domain_risklist - Recently Detected Malware Operation |
| RF - Domain - Recently Detected Phishing Techniques | RF - rf_domain_risklist - Recently Detected Cryptocurrency Mining Techniques |
| RF - Domain - Recently Linked to Cyber Attack | RF - rf_domain_risklist - Recently Linked to Cyber Attack |
| RF - Domain - Recently Referenced by Insikt Group | RF - rf_domain_risklist - Recently Referenced by Insikt Group |
| RF - Domain - Recently Reported as a Defanged DNS Name | RF - rf_domain_risklist - Recently Reported as a Defanged DNS Name |
| RF - Domain - Recently Reported by Insikt Group | RF - rf_domain_risklist - Recently Reported by Insikt Group |
| RF - Domain - Recently Reported Fraudulent Content | RF - rf_domain_risklist - Recently Reported Fraudulent Content |
| RF - Domain - Recently Reported Spam or Unwanted Content | RF - rf_domain_risklist - Recently Reported Spam or Unwanted Content |
| RF - Domain - Recently Resolved to Host of Many DDNS Names | RF - rf_domain_risklist - Recently Resolved to Host of Many DDNS Names |
| RF - Domain - Recently Resolved to Malicious IP | RF - rf_domain_risklist - Recently Resolved to Malicious IP |
| RF - Domain - Recently Resolved to Suspicious IP | RF - rf_domain_risklist - Recently Resolved to Suspicious IP |
| RF - Domain - Recently Resolved to Unusual IP | RF - rf_domain_risklist - Recently Resolved to Unusual IP |
| RF - Domain - Recently Resolved to Very Malicious IP | RF - rf_domain_risklist - Recently Resolved to Very Malicious IP |
| RF - Domain - Recorded Future Predictive Risk Model | RF - rf_domain_risklist - Recorded Future Predictive Risk Model |
| RF - Domain - Score | RF - rf_domain_risklist - Score |
| RF - Domain - Trending in Recorded Future Analyst Community | RF - rf_domain_risklist - Trending in Recorded Future Analyst Community |
| RF - Domain - Very Malicious | RF - rf_domain_risklist - Very Malicious |
| RF - Hash - Historically Reported in Threat List | RF - rf_hash_risklist - Historically Reported in Threat List |
| RF - Hash - Linked to Attack Vector | RF - rf_hash_risklist - Linked to Attack Vector |

| | |
|---|---|
| RF - Hash - Linked to Cyber Attack | RF - rf_hash_risklist - Linked to Cyber Attack |
| RF - Hash - Linked to Malware | RF - rf_hash_risklist - Linked to Malware |
| RF - Hash - Linked to Vulnerability | RF - rf_hash_risklist - Linked to Vulnerability |
| RF - Hash - Malicious | RF - rf_hash_risklist - Malicious |
| RF - Hash - Positive Malware Verdict | RF - rf_hash_risklist - Positive Malware Verdict |
| RF - Hash - Recently Active Targeting Vulnerabilities in the Wild | RF - rf_hash_risklist - Recently Active Targeting Vulnerabilities in the Wild |
| RF - Hash - Referenced by Insikt Group | RF - rf_hash_risklist - Referenced by Insikt Group |
| RF - Hash - Reported by DHS AIS | RF - rf_hash_risklist - Reported by DHS AIS |
| RF - Hash - Reported by Insikt Group | RF - rf_hash_risklist - Reported by Insikt Group |
| RF - Hash - Score | RF - rf_hash_risklist - Score |
| RF - Hash - Threat Researcher | RF - rf_hash_risklist - Threat Researcher |
| RF - Hash - Trending in Recorded Future Analyst Community | RF - rf_hash_risklist - Trending in Recorded Future Analyst Community |
| RF - Hash - Very Malicious | RF - rf_hash_risklist - Very Malicious |
| RF - Ip - Actively Communicating C&C Server | RF - rf_ip_risklist - Actively Communicating C&C Server |
| RF - Ip - Current C&C Server | RF - rf_ip_risklist - Current C&C Server |
| RF - Ip - Historical Bad SSL Association | RF - rf_ip_risklist - Historical Bad SSL Association |
| RF - Ip - Historical Botnet Traffic | RF - rf_ip_risklist - Historical Botnet Traffic |
| RF - Ip - Historical C&C Server | RF - rf_ip_risklist - Historical C&C Server |
| RF - Ip - Historical Honeypot Sighting | RF - rf_ip_risklist - Historical Honeypot Sighting |
| RF - Ip - Historical Multicategory Blocklist | RF - rf_ip_risklist - Historical Multicategory Blacklist |
| RF - Ip - Historical Open Proxies | RF - rf_ip_risklist - Historical Open Proxies |
| RF - Ip - Historical Positive Malware Verdict | RF - rf_ip_risklist - Historical Positive Malware Verdict |
| RF - Ip - Historical Spam Source | RF - rf_ip_risklist - Historical Spam Source |
| RF - Ip - Historical SSH/Dictionary Attacker | RF - rf_ip_risklist - Historical SSH/Dictionary Attacker |
| RF - Ip - Historical Threat Researcher | RF - rf_ip_risklist - Historical Threat Researcher |
| RF - Ip - Historically Linked to APT | RF - rf_ip_risklist - Historically Linked to APT |
| RF - Ip - Historically Linked to Cyber Attack | RF - rf_ip_risklist - Historically Linked to Cyber Attack |
| RF - Ip - Historically Linked to Intrusion Method | RF - rf_ip_risklist - Historically Linked to Intrusion Method |
| RF - Ip - Historically Referenced by Insikt Group | RF - rf_ip_risklist - Historically Referenced by Insikt Group |
| RF - Ip - Historically Reported as a Defanged IP | RF - rf_ip_risklist - Historically Reported as a Defanged IP |
| RF - Ip - Historically Reported by DHS AIS | RF - rf_ip_risklist - Historically Reported by DHS AIS |
| RF - Ip - Historically Reported by Insikt Group | RF - rf_ip_risklist - Historically Reported by Insikt Group |
| RF - Ip - Historically Reported in Threat List | RF - rf_ip_risklist - Historically Reported in Threat List |
| RF - Ip - Honeypot Host | RF - rf_ip_risklist - Honeypot Host |
| RF - Ip - Malicious | RF - rf_ip_risklist - Malicious |
| RF - Ip - Malicious Packet Source | RF - rf_ip_risklist - Malicious Packet Source |
| RF - Ip - Phishing Host | RF - rf_ip_risklist - Phishing Host |

| | |
|---|---|
| RF - Ip - Recent Botnet Traffic | RF - rf_ip_risklist - Recent Botnet Traffic |
| RF - Ip - Recent C&C Server | RF - rf_ip_risklist - Recent C&C Server |
| RF - Ip - Recent Honeypot Sighting | RF - rf_ip_risklist - Recent Honeypot Sighting |
| RF - Ip - Recent Host of Many DDNS Names | RF - rf_ip_risklist - Recent Host of Many DDNS Names |
| RF - Ip - Recent Multicategory Blocklist | RF - rf_ip_risklist - Recent Multicategory Blacklist |
| RF - Ip - Recent Open Proxies | RF - rf_ip_risklist - Recent Open Proxies |
| RF - Ip - Recent Positive Malware Verdict | RF - rf_ip_risklist - Recent Positive Malware Verdict |
| RF - Ip - Recent SSH/Dictionary Attacker | RF - rf_ip_risklist - Recent SSH/Dictionary Attacker |
| RF - Ip - Recent Threat Researcher | RF - rf_ip_risklist - Recent Threat Researcher |
| RF - Ip - Recently Active C&C Server | RF - rf_ip_risklist - Recently Active C&C Server |
| RF - Ip - Recently Linked to APT | RF - rf_ip_risklist - Recently Linked to APT |
| RF - Ip - Recently Linked to Intrusion Method | RF - rf_ip_risklist - Recently Linked to Intrusion Method |
| RF - Ip - Recently Referenced by Insikt Group | RF - rf_ip_risklist - Recently Referenced by Insikt Group |
| RF - Ip - Recently Reported as a Defanged IP | RF - rf_ip_risklist - Recently Reported as a Defanged IP |
| RF - Ip - Recently Reported by Insikt Group | RF - rf_ip_risklist - Recently Reported by Insikt Group |
| RF - Ip - Recently Transferring Data to C&C Server | RF - rf_ip_risklist - Recently Transferring Data to C&C Server |
| RF - Ip - Resolution of Fast Flux DNS Name | RF - rf_ip_risklist - Resolution of Fast Flux DNS Name |
| RF - Ip - Score | RF - rf_ip_risklist - Score |
| RF - Ip - Tor Node | RF - rf_ip_risklist - Tor Node |
| RF - Ip - Trending in Recorded Future Analyst Community | RF - rf_ip_risklist - Trending in Recorded Future Analyst Community |
| RF - Ip - Unusual IP | RF - rf_ip_risklist - Unusual IP |
| RF - Ip - Very Malicious | RF - rf_ip_risklist - Very Malicious |
| RF - Ip - Vulnerable Host | RF - rf_ip_risklist - Vulnerable Host |
| RF - Vulnerability - Cyber Exploit Signal: Critical | RF - rf_vulnerability_risklist - Cyber Exploit Signal: Critical |
| RF - Vulnerability - Cyber Exploit Signal: Important | RF - rf_vulnerability_risklist - Cyber Exploit Signal: Important |
| RF - Vulnerability - Cyber Exploit Signal: Medium | RF - rf_vulnerability_risklist - Cyber Exploit Signal: Medium |
| RF - Vulnerability - Exploited in the Wild by Malware | RF - rf_vulnerability_risklist - Exploited in the Wild by Malware |
| RF - Vulnerability - Exploited in the Wild by Recently Active Malware | RF - rf_vulnerability_risklist - Exploited in the Wild by Recently Active Malware |
| RF - Vulnerability - Historical Unverified Proof of Concept Available | RF - rf_vulnerability_risklist - Historical Unverified Proof of Concept Available |
| RF - Vulnerability - Historical Verified Proof of Concept Available | RF - rf_vulnerability_risklist - Historical Verified Proof of Concept Available |
| RF - Vulnerability - Historical Verified Proof of Concept Available Using Remote Execution | RF - rf_vulnerability_risklist - Historical Verified Proof of Concept Available Using Remote Execution |
| RF - Vulnerability - Historically Exploited in the Wild by Malware | RF - rf_vulnerability_risklist - Historically Exploited in the Wild by Malware |
| RF - Vulnerability - Historically Linked to Exploit Kit | RF - rf_vulnerability_risklist - Historically Linked to Exploit Kit |
| RF - Vulnerability - Historically Linked to Malware | RF - rf_vulnerability_risklist - Historically Linked to Malware |
| RF - Vulnerability - Historically Linked to Penetration Testing Tools | RF - rf_vulnerability_risklist - Historically Linked to Penetration |

| | |
|---|---|
| | Testing Tools |
| RF - Vulnerability - Historically Linked to Ransomware | RF - rf_vulnerability_risklist - Historically Linked to Ransomware |
| RF - Vulnerability - Historically Linked to Remote Access Trojan | RF - rf_vulnerability_risklist - Historically Linked to Remote Access Trojan |
| RF - Vulnerability - Historically Referenced by Insikt Group | RF - rf_vulnerability_risklist - Historically Referenced by Insikt Group |
| RF - Vulnerability - Historically Reported by Insikt Group | RF - rf_vulnerability_risklist - Historically Reported by Insikt Group |
| RF - Vulnerability - Linked to Historical Cyber Exploit | RF - rf_vulnerability_risklist - Linked to Historical Cyber Exploit |
| RF - Vulnerability - Linked to Recent Cyber Exploit | RF - rf_vulnerability_risklist - Linked to Recent Cyber Exploit |
| RF - Vulnerability - Malicious | RF - rf_vulnerability_risklist - Malicious |
| RF - Vulnerability - NIST Severity: Critical | RF - rf_vulnerability_risklist - NIST Severity: Critical |
| RF - Vulnerability - NIST Severity: High | RF - rf_vulnerability_risklist - NIST Severity: High |
| RF - Vulnerability - NIST Severity: Low | RF - rf_vulnerability_risklist - NIST Severity: Low |
| RF - Vulnerability - NIST Severity: Medium | RF - rf_vulnerability_risklist - NIST Severity: Medium |
| RF - Vulnerability - Recent Unverified Proof of Concept Available | RF - rf_vulnerability_risklist - Recent Unverified Proof of Concept Available |
| RF - Vulnerability - Recent Verified Proof of Concept Available Using Remote Execution | RF - rf_vulnerability_risklist - Recent Verified Proof of Concept Available Using Remote Execution |
| RF - Vulnerability - Recently Linked to Exploit Kit | RF - rf_vulnerability_risklist - Recently Linked to Exploit Kit |
| RF - Vulnerability - Recently Linked to Malware | RF - rf_vulnerability_risklist - Recently Linked to Malware |
| RF - Vulnerability - Recently Linked to Penetration Testing Tools | RF - rf_vulnerability_risklist - Recently Linked to Penetration Testing Tools |
| RF - Vulnerability - Recently Linked to Ransomware | RF - rf_vulnerability_risklist - Recently Linked to Ransomware |
| RF - Vulnerability - Recently Linked to Remote Access Trojan | RF - rf_vulnerability_risklist - Recently Linked to Remote Access Trojan |
| RF - Vulnerability - Recently Referenced by Insikt Group | RF - rf_vulnerability_risklist - Recently Referenced by Insikt Group |
| RF - Vulnerability - Recently Reported by Insikt Group | RF - rf_vulnerability_risklist - Recently Reported by Insikt Group |
| RF - Vulnerability - Score | RF - rf_vulnerability_risklist - Score |
| RF - Vulnerability - Vendor Severity: Critical | RF - rf_vulnerability_risklist - Vendor Severity: Critical |
| RF - Vulnerability - Vendor Severity: High | RF - rf_vulnerability_risklist - Vendor Severity: High |
| RF - Vulnerability - Vendor Severity: Low | RF - rf_vulnerability_risklist - Vendor Severity: Low |
| RF - Vulnerability - Vendor Severity: Medium | RF - rf_vulnerability_risklist - Vendor Severity: Medium |
| RF - Vulnerability - Very Malicious | RF - rf_vulnerability_risklist - Very Malicious |
| RF - Vulnerability - Web Reporting Prior to CVSS Score | RF - rf_vulnerability_risklist - Web Reporting Prior to CVSS Score |
| RF - Vulnerability - Web Reporting Prior to NVD Disclosure | RF - rf_vulnerability_risklist - Web Reporting Prior to NVD Disclosure |