Text

Description automatically generated

IPQualityScore App User Guide for the ThreatConnect Platform

**Version 1.0.0**

# **Support**

For assistance with this App, to report a bug, or feature requests please contact us via the following.

|  |  |
| --- | --- |
| **Support Portal** | https://www.ipqualityscore.com/contact-us |
| **Email** | Support@IPQualityScore.com |
| **Phone** | (800) 713-2618 |

# **Version History**

|  |  |  |
| --- | --- | --- |
| **Date** | **Version** | **Description** |
| 08th June 2021 | 1.0.0 | User Guide for the IPQualityScore Enrichment App. |

**Contents**

[Support 1](#_Toc69328868)

[Version History 1](#_Toc69328869)

[1. Introduction 3](#_Toc69328870)

[2. Configuration 4](#_Toc69328871)

[**2.1. Pre-Requisites** 4](#_Toc69328872)

[**2.2. IPQualityScore App Installation** 4](#_Toc69328873)

[**2.3. IPQualityScore App Configuration** 4](#_Toc69328874)

[3. Outputs 7](#_Toc69328875)

[4. IPQualityScore Playbook Templates 28](#_Toc69328876)

[**4.1. IPQualityScore Playbook Templates Installation** 28](#_Toc69328877)

[**4.2. IPQualityScore API Key Variable Set Up** 28](#_Toc69328878)

[**4.3. IPQualityScore Custom Attributes Set Up** 29](#_Toc69328879)

[**4.4. IPQualityScore Playbook Templates Activation** 32](#_Toc69328880)

[5. Running IP Address Reputation Playbook Template 32](#_Toc69328881)

[6. Running Email Address Reputation Playbook Template 36](#_Toc69328882)

[7. Running URL/Domain Reputation Playbook Template 39](#_Toc69328883)

[8. Threat Rating Metrics Table 43](#_Toc69328884)

# **1. Introduction**

**IPQualityScore** offers a variety of different risk analysis APIs designed to detect and mitigate online threats and abusive behaviour from even the most sophisticated bad actors. Whether its websites of all sizes or enterprise companies, IPQS has the right solutions to solve your challenges. These solutions include online fraud prevention, risk scoring, and threat mitigation. Customizable settings and international data coverage ensures our scoring models perfectly fit your audience.

**IP Reputation & Proxy Detection** service performs real-time lookups to instantly determine how risky a user, click, or transaction is based on an IP address and optional device information. In addition to analysing if the IP address is a proxy or VPN, the API returns over 20 relevant data points such as:

* Geo location data
* ISP
* Connection type
* Device details
* Recent reputation activity
* Overall fraud score
* Status as a proxy
* VPN
* Tor connection
* Other similar data points to classify reputation and risk

**Email Validation & Reputation** **API** provides real-time email address reputation scoring and validation with hundreds of syntax & DNS checks. The API can be leveraged to determine if the email address exists with the mail service provider and is able to accept new messages. In addition, users are also able to determine if the email address has a poor reputation and associated with any current threats. Lastly, users are able to detect disposable or temporary mail services as well as emails with a history of fraudulent behaviour online.

**Malicious URL Scanner API** scans links and domains in real-time to detect suspicious URLs using trusted machine learning models. These machine learning models can accurately identify phishing links, malware URLs, viruses, parked domains, and suspicious URLs with real-time risk scores. In addition, the machine learning models can confidently classify poor reputation domains, suspicious links, and phishing URLs with a real-time API integration.

Features such as parking domain detection, domain spam scores, reputation checks, and domain age, elevates URL intelligence to a whole new level.

This document describes how to configure the IPQualityScore Enrichment App provided by IPQualityScore in the ThreatConnect Platform. The IPQualityScore Enrichment Playbook App enables ThreatConnect Platform users to perform On-Demand Enrichment of IP Address Reputation, Email Address Reputation, Domain and URL Reputation using the IPQualityScore Enrichment source.

# **2. Configuration**

## **2.1. Pre-Requisites**

To configure the **IPQualityScore Enrichment** App in your ThreatConnect Playbooks, the following requirements need to be fulfilled:

* Access to ThreatConnect instance.
* Permission to execute ThreatConnect Playbooks.
* IPQualityScore API Key provisioned by IPQualityScore to authenticate requests to IPQualityScore API.
* IPQualityScore Enrichment app installed in ThreatConnect Instance.
* IPQualityScore Playbook Templates installed in ThreatConnect Instance.
* IPQualityScore specific Custom Attributes imported in ThreatConnect Instance.

## **2.2. IPQualityScore App Installation**

**IPQualityScore Enrichment** App for ThreatConnect is available on ThreatConnect Marketplace at: <https://go.threatconnect.market> (We can update after vetting is complete and get all the materials from the customer)

Download the App package with tcx extension and install it in your ThreatConnect instance. For installation instructions, refer to the “Install an App” in the ThreatConnect System Administration Guide. For more information, contact your ThreatConnect Customer representatives.

## **2.3. IPQualityScore App Configuration**

**IPQualityScore Enrichment** **App** has the following configuration.

* **IPQualityScore API Key - String**
* API Key provisioned by IPQualityScore.
* **Enrichment Type** - **Dropdown**
* Dropdown containing “IP Address”, “Email Address” and URL.
* Depending on which enrichment type is chosen, different configurations will populate. A full list of configuration options are presented below.
* **IP Address/Email Address/URL - String**
* **Note:** URL accepts both URL and Domain as inputs

* **Strictness for IP Address – Dropdown, visible when IP Address Enrichment Type is selected (default to 0)**
* How in depth (strict) do you want this query to be? Higher values take longer to process and may provide a higher false-positive rate. We recommend starting at "0", the lowest strictness setting, and increasing to "1" or "2" depending on your levels of fraud.
* **User Agent - String, visible when IP Address Enrichment Type is selected**
* You can optionally provide the user agent string (browser). This enables the app to run additional checks to see if the user is a bot or running an invalid browser. This allows the app to evaluate the risk of the user as judged in the "fraud\_score".
* **User Language - String, visible when IP Address Enrichment Type is selected**
* You can optionally provide the app with the user's language header. This allows the app to evaluate the risk of the user as judged in the "fraud\_score".
* **Fast for IP Address - Boolean Dropdown, visible when IP Address Enrichment Type is selected**
* When this parameter is enabled the API will not perform certain forensic checks that take longer to process. Enabling this feature greatly increases the API speed without much impact on accuracy. This option is intended for services that require decision making in a time sensitive manner and can be used for any strictness level.
* **Mobile - Boolean Dropdown, visible when IP Address Enrichment Type is selected**
* You can optionally specify that this lookup should be treated as a mobile device. Recommended for mobile lookups that do not have a user agent attached to the request.
  + NOTE: This can cause unexpected and abnormal results if the device is not a mobile device.
* **Allow Public Access Points - Boolean Dropdown, visible when IP Address Enrichment Type is selected**
* Bypasses certain checks for IP addresses from education and research institutions, schools, and some corporate connections to better accommodate audiences that frequently use public connections.
* **Lighter Penalties- Boolean Dropdown, visible when IP Address Enrichment Type is selected**
* Is your scoring too strict? Enable this setting to lower detection rates and Fraud Scores for mixed quality IP addresses. If you experience any false positives with your traffic then enabling this feature will provide better results.
* **Strictness for Email Address - Dropdown, visible when Email Address Enrichment Type is selected (default to 0)**
* Sets how strictly spam traps and honeypots are detected by our system, depending on how comfortable you are with identifying emails suspected of being a spam trap. 0 is the lowest level which will only return spam traps with high confidence. Strictness levels above 0 will return increasingly more strict results, with level 2 providing the greatest detection rates.
* **Fast for Email Address - Boolean Dropdown, visible when Email Address Enrichment Type is selected**
* When this parameter is enabled the API will not perform an SMTP check with the mail service provider, which greatly increases the API speed. Syntax and DNS checks are still performed on the email address as well as our disposable email detection service. This option is intended for services that require decision making in a time sensitive manner.
* **Timeout in seconds (1-60) - String, visible when Email Address Enrichment Type is selected**
* Possible Values (1-60), Maximum number of seconds to wait for a reply from a mail service provider. If your implementation requirements do not need an immediate response, we recommend bumping this value to 20. Any results which experience a connection timeout will return the "timed\_out" variable as true. Default value is 7 seconds.
* **Suggest Domain - Boolean Dropdown, visible when Email Address Enrichment Type is selected**
* Force analyzes if the email address's domain has a typo and should be corrected to a popular mail service. By default, this test is currently only performed when the email is invalid or if the "recent abuse" status is true.
* **Abuse Strictness - Dropdown, visible when Email Address Enrichment Type is selected**
* Set the strictness level for machine learning pattern recognition of abusive email addresses with the "recent\_abuse" data point. Default level of 0 provides good coverage, however if you are filtering account applications and facing advanced fraudsters then we recommend increasing this value to level 1 or 2.
* **Strictness for URL - Dropdown, visible when URL Enrichment Type is selected (default to 0)**
* How strict should we scan this URL? Stricter checks may provide a higher false-positive rate. We recommend defaulting to level "0", the lowest strictness setting, and increasing to "1" or "2" depending on your levels of abuse.
* **Fast for URL - Boolean Dropdown, visible when URL Enrichment Type is selected**
* When enabled, the API will provide quicker response times using lighter checks and analysis. This setting defaults to false.
* **Fail on Error - Checkbox (default to True)**
* Fails the App when an error occurs, if set to True.
* **Fail on no results – Checkbox (default to False)**
* Fails the App when there are no results returned by the IPQualityScore API, if set to True.

# **3. Outputs**

|  |  |  |  |
| --- | --- | --- | --- |
| **Output Name** | **Data Type** | **Possible Values** | **Notes** |
| ipqs.ipreputation.json.raw | String | Response String object | Raw response object from IPQualityScore API for debugging purposes. |
| ipqs.ipreputation.results.data | String | Processed Response String object | Processed Response String object of IP reputation object. |
| ipqs.emailreputation.json.raw | String | Response String object | Raw response object from IPQualityScore API for debugging purposes. |
| ipqs.emailreputation.results.data | String | Processed Response String object | Processed Response String object of IP reputation object. |
| ipqs.urlreputation.json.raw | String | Response String object | Raw response object from IPQualityScore API for debugging purposes. |
| ipqs.urlreputation.results.data | String | Response String object | Raw response object from IPQualityScore API for debugging purposes. |

**ipqs.ipreputation.json.raw** , this output variable contains the JSON object containing the IP Address reputation data, that can be extracted using JMESPath App.

|  |  |  |
| --- | --- | --- |
| **Attribute Name** | **Attribute Type** | **Attribute Description** |
| proxy | boolean | Is this IP address suspected to be a proxy? (SOCKS, Elite, Anonymous, VPN, Tor, etc.) |
| host | string | The certificate name for passive DNS record |
| ISP | string | ISP if one is known. Otherwise "N/A". |
| Organization | string | Organization if one is known. Can be parent company or sub company of the listed ISP. Otherwise "N/A". |
| ASN | integer | Autonomous System Number if one is known. Null if nonexistent. |
| country\_code | string | Two character country code of IP address or "N/A" if unknown. |
| city | string | City of IP address if available or "N/A" if unknown. |
| region | string | Region (state) of IP address if available or "N/A" if unknown. |
| timezone | string | Timezone of IP address if available or "N/A" if unknown. |
| latitude | float | Latitude of IP address if available or "N/A" if unknown. |
| longitude | float | Longitude of IP address if available or "N/A" if unknown. |
| is\_crawler | boolean | Is this IP associated with being a confirmed crawler from a mainstream search engine such as Googlebot, Bingbot, Yandex, etc. based on hostname or IP address verification. |
| connection\_type | string | Classification of the IP address connection type as "Residential", "Corporate", "Education", "Mobile", or "Data Center". |
| recent\_abuse | boolean | This value will indicate if there has been any recently verified abuse across our network for this IP address. Abuse could be a confirmed chargeback, compromised device, fake app install, or similar malicious behavior within the past few days. |
| abuse\_velocity | string | Premium Account Feature - How frequently the IP address is engaging in abuse across the IPQS threat network. Values can be "high", "medium", "low", or "none". Can be used in combination with the **Fraud Score** to identify bad behavior. |
| bot\_status | boolean | Premium Account Feature - Indicates if bots or non-human traffic has recently used this IP address to engage in automated fraudulent behavior. Provides stronger confidence that the IP address is suspicious. |
| vpn | boolean | Is this IP suspected of being a VPN connection? This can include data center ranges which can become active VPNs at any time. The "proxy" status will always be true when this value is true. |
| tor | boolean | Is this IP suspected of being a TOR connection? This can include previously active TOR nodes and exits which can become active TOR exits at any time. The "proxy" status will always be true when this value is true. |
| active\_vpn | boolean | Premium Account Feature - Identifies active VPN connections used by popular VPN services and private VPN servers. |
| active\_tor | boolean | Premium Account Feature - Identifies active TOR exits on the TOR network. |
| mobile | boolean | Is this user agent a mobile browser? (will always be false if the user agent is not passed in the API request) |
| fraud\_score | float | The overall fraud score of the user based on the IP, user agent, language, and any other optionally passed variables. Fraud Scores **>= 75** are suspicious, but not necessarily fraudulent. We recommend flagging or blocking traffic with Fraud Scores **>= 85**, but you may find it beneficial to use a higher or lower threshold. |
| request\_id | string | A unique identifier for this request that can be used to lookup the request details or send a postback conversion notice. |
| operating\_system | string | Operating system name and version or "N/A" if unknown. Requires the "user\_agent" variable in the API Request. |
| browser | string | Browser name and version or "N/A" if unknown. Requires the "**user\_agent**" variable in the API Request. |
| device\_brand | string | Brand name of the device or "N/A" if unknown. Requires the "**user\_agent**" variable in the API Request. |
| device\_model | string | Model name of the device or "N/A" if unknown. Requires the "**user\_agent**" variable in the API Request. |
| transaction\_details | object | Additional scoring variables for risk analysis are available when [transaction scoring data](https://www.ipqualityscore.com/documentation/proxy-detection/transaction-scoring) is passed through the API request. These variables are also useful for scoring user data such as physical addresses, phone numbers, usernames, and transaction details. The data points below are populated when at least 1 transaction data parameter is present in the initial API request. The following transaction variables are "null" when the necessary transaction parameters are not passed with the initial API request. For instance, not passing the "billing\_email" will return "valid\_billing\_email" as null. |
| message | string | A generic status message, either success or some form of an error notice. |
| success | boolean | Was the request successful? |
| errors | String Array | Array of errors which occurred while attempting to process this request. |

**ipqs.ipreputation.results.data** , this output variable contains the JSON object containing the processed IP Address reputation data, that can be extracted using JMESPath App.

|  |  |  |
| --- | --- | --- |
| **Attribute Name** | **Attribute Type** | **Attribute Description** |
| IPQS\_Reputation | string | This value provides the IP reputation based on Fraud Score.  Possible Values are:   1. Critical 2. High Risk 3. Moderate Risk 4. Suspicious 5. Clean |
| TC\_Threat\_Rating | String | This Value provides Threat Connect Threat Rating Information  Possible Values are:   1. Critical Threat 2. High Threat 3. Moderate Threat 4. Suspicious |
| proxy | boolean | Is this IP address suspected to be a proxy? (SOCKS, Elite, Anonymous, VPN, Tor, etc.) |
| host | string | The certificate name for passive DNS record |
| ISP | string | ISP if one is known. Otherwise "N/A". |
| Organization | string | Organization if one is known. Can be parent company or sub company of the listed ISP. Otherwise "N/A". |
| ASN | integer | Autonomous System Number if one is known. Null if nonexistent. |
| country\_code | string | Two character country code of IP address or "N/A" if unknown. |
| city | string | City of IP address if available or "N/A" if unknown. |
| region | string | Region (state) of IP address if available or "N/A" if unknown. |
| timezone | string | Timezone of IP address if available or "N/A" if unknown. |
| latitude | float | Latitude of IP address if available or "N/A" if unknown. |
| longitude | float | Longitude of IP address if available or "N/A" if unknown. |
| is\_crawler | boolean | Is this IP associated with being a confirmed crawler from a mainstream search engine such as Googlebot, Bingbot, Yandex, etc. based on hostname or IP address verification. |
| connection\_type | string | Classification of the IP address connection type as "Residential", "Corporate", "Education", "Mobile", or "Data Center". |
| recent\_abuse | boolean | This value will indicate if there has been any recently verified abuse across our network for this IP address. Abuse could be a confirmed chargeback, compromised device, fake app install, or similar malicious behavior within the past few days. |
| abuse\_velocity | string | Premium Account Feature - How frequently the IP address is engaging in abuse across the IPQS threat network. Values can be "high", "medium", "low", or "none". Can be used in combination with the **Fraud Score** to identify bad behavior. |
| bot\_status | boolean | Premium Account Feature - Indicates if bots or non-human traffic has recently used this IP address to engage in automated fraudulent behavior. Provides stronger confidence that the IP address is suspicious. |
| vpn | boolean | Is this IP suspected of being a VPN connection? This can include data center ranges which can become active VPNs at any time. The "proxy" status will always be true when this value is true. |
| tor | boolean | Is this IP suspected of being a TOR connection? This can include previously active TOR nodes and exits which can become active TOR exits at any time. The "proxy" status will always be true when this value is true. |
| active\_vpn | boolean | Premium Account Feature - Identifies active VPN connections used by popular VPN services and private VPN servers. |
| active\_tor | boolean | Premium Account Feature - Identifies active TOR exits on the TOR network. |
| mobile | boolean | Is this user agent a mobile browser? (will always be false if the user agent is not passed in the API request) |
| fraud\_score | float | The overall fraud score of the user based on the IP, user agent, language, and any other optionally passed variables. Fraud Scores **>= 75** are suspicious, but not necessarily fraudulent. We recommend flagging or blocking traffic with Fraud Scores **>= 85**, but you may find it beneficial to use a higher or lower threshold. |
| request\_id | string | A unique identifier for this request that can be used to lookup the request details or send a postback conversion notice. |
| operating\_system | string | Operating system name and version or "N/A" if unknown. Requires the "user\_agent" variable in the API Request. |
| browser | string | Browser name and version or "N/A" if unknown. Requires the "**user\_agent**" variable in the API Request. |
| device\_brand | string | Brand name of the device or "N/A" if unknown. Requires the "**user\_agent**" variable in the API Request. |
| device\_model | string | Model name of the device or "N/A" if unknown. Requires the "**user\_agent**" variable in the API Request. |
| transaction\_details | object | Additional scoring variables for risk analysis are available when [transaction scoring data](https://www.ipqualityscore.com/documentation/proxy-detection/transaction-scoring) is passed through the API request. These variables are also useful for scoring user data such as physical addresses, phone numbers, usernames, and transaction details. The data points below are populated when at least 1 transaction data parameter is present in the initial API request. The following transaction variables are "null" when the necessary transaction parameters are not passed with the initial API request. For instance, not passing the "billing\_email" will return "valid\_billing\_email" as null. |
| message | string | A generic status message, either success or some form of an error notice. |
| success | boolean | Was the request successful? |
| errors | String Array | Array of errors which occurred while attempting to process this request. |

**ipqs.emailreputation.json.raw** , this output variable contains the JSON object containing the Email Address reputation data, that can be extracted using JMESPath App.

|  |  |  |
| --- | --- | --- |
| **Attribute Name** | **Attribute Type** | **Attribute Description** |
| valid | boolean | Does this email address appear valid? |
| disposable | boolean | Is this email suspected of belonging to a temporary or disposable mail service? Usually associated with fraudsters and scammers. |
| timed\_out | boolean | Did the connection to the mail service provider timeout during the verification? If so, we recommend increasing the **"timeout"** variable above the default 7 second value. Lookups that timeout with a **"valid"** result as false are most likely false and should be not be trusted. |
| deliverability | string | How likely is this email to be delivered to the user and land in their mailbox. Values can be "high", "medium", or "low". |
| catch\_all | boolean | Is this email likely to be a "catch all" where the mail server verifies all emails tested against it as valid? It is difficult to determine if the address is truly valid in these scenarios, since the email's server will not confirm the account's status. |
| leaked | boolean | Was this email address associated with a recent database leak from a third party? Leaked accounts pose a risk as they may have become compromised during a database breach. |
| suspect | boolean | This value indicates if the mail server is currently replying with a temporary error and unable to verify the email address. This status will also be true for "catch all" email addresses as defined below. If this value is true, then we suspect the **"valid"** result may be tainted and there is not a guarantee that the email address is truly valid. |
| smtp\_score | integer | Validity score of email server's SMTP setup. Range: "-1" - "3". Scores above "-1" can be associated with a valid email.   * **-1** = invalid email address * **0** = mail server exists, but is rejecting all mail * **1** = mail server exists, but is showing a temporary error * **2** = mail server exists, but accepts all email * **3** = mail server exists and has verified the email address |
| overall\_score | integer | Overall email validity score. Range: "0" - "4". Scores above "1" can be associated with a valid email.   * **0** = invalid email address * **1** = dns valid, unreachable mail server * **2** = dns valid, temporary mail rejection error * **3** = dns valid, accepts all mail * **4** = dns valid, verified email exists |
| first\_name | string | Suspected first name based on email. Returns "CORPORATE" if the email is suspected of being a generic company email. Returns "UNKNOWN" if the first name was not determinable. |
| common | boolean | Is this email from a common email provider? ("gmail.com", "yahoo.com", "hotmail.com", etc.) |
| generic | boolean | Is this email suspected as being a catch all or shared email for a domain? ("admin@", "webmaster@", "newsletter@", "sales@", "contact@", etc.) |
| dns\_valid | boolean | Does the email's hostname have valid DNS entries? Partial indication of a valid email. |
| honeypot | boolean | Is this email believed to be a "honeypot" or "SPAM trap"? **Bulk mail** sent to these emails increases your risk of being blacklisted by large ISPs & ending up in the spam folder. |
| spam\_trap\_score | string | Confidence level of the email address being an active SPAM trap. Values can be "high", "medium", "low", or "none". We recommend scrubbing emails with "high" or "medium" statuses. Avoid "low" emails whenever possible for any promotional mailings. |
| recent\_abuse | boolean | This value will indicate if there has been any recently verified abuse across our network for this email address. Abuse could be a confirmed chargeback, fake signup, compromised device, fake app install, or similar malicious behavior within the past few days. |
| fraud\_score | float | The overall Fraud Score of the user based on the email's reputation and recent behavior across the IPQS threat network. Fraud Scores **>= 75** are suspicious, but not necessarily fraudulent. |
| frequent\_complainer | boolean | Indicates if this email frequently unsubscribes from marketing lists or reports email as SPAM. |
| suggested\_domain | string | Default value is "N/A". Indicates if this email's domain should in fact be corrected to a popular mail service. This field is useful for catching user typos. For example, an email address with "gmai.com", would display a suggested domain of "gmail.com". This feature supports all major mail service providers. |
| first\_seen | object | This object contains human, timestamp, iso values |
| domain\_age | object | This object contains human, timestamp, iso values |
| sanitized\_email | string | Sanitized email address with all aliases and masking removed, such as multiple periods for Gmail.com. |
| request\_id | string | A unique identifier for this request that can be used to lookup the request details or send a postback conversion notice. |
| success | boolean | Was the request successful? |
| message | string | A generic status message, either success or some form of an error notice. |
| errors | array of strings | Array of errors which occurred while attempting to process this request. |

**ipqs.emailreputation.results.data**, this output variable contains the JSON object containing the Processed Email Address reputation data, that can be extracted using JMESPath App.

|  |  |  |
| --- | --- | --- |
| **Attribute Name** | **Attribute Type** | **Attribute Description** |
| IPQS\_Reputation | string | This value provides the IP reputation based on Fraud Score.  Possible Values are:   1. Critical 2. High Risk 3. Moderate Risk 4. Low Risk 5. Invalid 6. Clean |
| TC\_Threat\_Rating | String | This Value provides Threat Connect Threat Rating Information  Possible Values are:   1. Critical Threat 2. High Threat 3. Moderate Threat 4. Low Threat 5. Suspicious |
| valid | boolean | Does this email address appear valid? |
| disposable | boolean | Is this email suspected of belonging to a temporary or disposable mail service? Usually associated with fraudsters and scammers. |
| timed\_out | boolean | Did the connection to the mail service provider timeout during the verification? If so, we recommend increasing the **"timeout"** variable above the default 7 second value. Lookups that timeout with a **"valid"** result as false are most likely false and should be not be trusted. |
| deliverability | string | How likely is this email to be delivered to the user and land in their mailbox. Values can be "high", "medium", or "low". |
| catch\_all | boolean | Is this email likely to be a "catch all" where the mail server verifies all emails tested against it as valid? It is difficult to determine if the address is truly valid in these scenarios, since the email's server will not confirm the account's status. |
| leaked | boolean | Was this email address associated with a recent database leak from a third party? Leaked accounts pose a risk as they may have become compromised during a database breach. |
| suspect | boolean | This value indicates if the mail server is currently replying with a temporary error and unable to verify the email address. This status will also be true for "catch all" email addresses as defined below. If this value is true, then we suspect the **"valid"** result may be tainted and there is not a guarantee that the email address is truly valid. |
| smtp\_score | integer | Validity score of email server's SMTP setup. Range: "-1" - "3". Scores above "-1" can be associated with a valid email.   * **-1** = invalid email address * **0** = mail server exists, but is rejecting all mail * **1** = mail server exists, but is showing a temporary error * **2** = mail server exists, but accepts all email * **3** = mail server exists and has verified the email address |
| overall\_score | integer | Overall email validity score. Range: "0" - "4". Scores above "1" can be associated with a valid email.   * **0** = invalid email address * **1** = dns valid, unreachable mail server * **2** = dns valid, temporary mail rejection error * **3** = dns valid, accepts all mail * **4** = dns valid, verified email exists |
| first\_name | string | Suspected first name based on email. Returns "CORPORATE" if the email is suspected of being a generic company email. Returns "UNKNOWN" if the first name was not determinable. |
| common | boolean | Is this email from a common email provider? ("gmail.com", "yahoo.com", "hotmail.com", etc.) |
| generic | boolean | Is this email suspected as being a catch all or shared email for a domain? ("admin@", "webmaster@", "newsletter@", "sales@", "contact@", etc.) |
| dns\_valid | boolean | Does the email's hostname have valid DNS entries? Partial indication of a valid email. |
| honeypot | boolean | Is this email believed to be a "honeypot" or "SPAM trap"? **Bulk mail** sent to these emails increases your risk of being blacklisted by large ISPs & ending up in the spam folder. |
| spam\_trap\_score | string | Confidence level of the email address being an active SPAM trap. Values can be "high", "medium", "low", or "none". We recommend scrubbing emails with "high" or "medium" statuses. Avoid "low" emails whenever possible for any promotional mailings. |
| recent\_abuse | boolean | This value will indicate if there has been any recently verified abuse across our network for this email address. Abuse could be a confirmed chargeback, fake signup, compromised device, fake app install, or similar malicious behavior within the past few days. |
| fraud\_score | float | The overall Fraud Score of the user based on the email's reputation and recent behavior across the IPQS threat network. Fraud Scores **>= 75** are suspicious, but not necessarily fraudulent. |
| frequent\_complainer | boolean | Indicates if this email frequently unsubscribes from marketing lists or reports email as SPAM. |
| suggested\_domain | string | Default value is "N/A". Indicates if this email's domain should in fact be corrected to a popular mail service. This field is useful for catching user typos. For example, an email address with "gmai.com", would display a suggested domain of "gmail.com". This feature supports all major mail service providers. |
| first\_seen | object | This object contains human, timestamp, iso values |
| domain\_age | object | This object contains human, timestamp, iso values |
| sanitized\_email | string | Sanitized email address with all aliases and masking removed, such as multiple periods for Gmail.com. |
| request\_id | string | A unique identifier for this request that can be used to lookup the request details or send a postback conversion notice. |
| success | boolean | Was the request successful? |
| message | string | A generic status message, either success or some form of an error notice. |
| errors | array of strings | Array of errors which occurred while attempting to process this request. |

**ipqs.urlreputation.json.raw** , this output variable contains the JSON object containing the Malicious URL data, that can be extracted using JMESPath App.

|  |  |  |
| --- | --- | --- |
| **Attribute Name** | **Attribute Type** | **Attribute Description** |
| unsafe | boolean | Is this domain suspected of being unsafe due to phishing, malware, spamming, or abusive behavior? View the confidence level by analyzing the "risk\_score" |
| domain | boolean | Domain name of the final destination URL of the scanned link, after following all redirects. |
| ip\_address | string | The IP address corresponding to the server of the domain name. |
| server | string | The server banner of the domain's IP address. For example: "nginx/1.16.0". Value will be "N/A" if unavailable. |
| content\_type | string | MIME type of URL's content. For example "text/html; charset=UTF-8". Value will be "N/A" if unavailable. |
| risk\_score | integer | The IPQS risk score which estimates the confidence level for malicious URL detection. Risk Scores 85+ are high risk, while Risk Scores = 100 are confirmed as accurate |
| status\_code | integer | HTTP Status Code of the URL's response. This value should be "200" for a valid website. Value is "0" if URL is unreachable. |
| page\_size | integer | Total number of bytes to download the URL's content. Value is "0" if URL is unreachable. |
| domain\_rank | integer | Estimated popularity rank of website globally. Value is "0" if the domain is unranked or has low traffic. |
| dns\_valid | boolean | The domain of the URL has valid DNS records. |
| suspicious | boolean | Is this URL suspected of being malicious or used for phishing or abuse? Use in conjunction with the "risk\_score" as a confidence level. |
| phishing | boolean | Is this URL associated with malicious phishing behavior? |
| malware | boolean | Is this URL associated with malware or viruses? |
| parking | boolean | Is the domain of this URL currently parked with a for sale notice? |
| spamming | boolean | Is the domain of this URL associated with email SPAM or abusive email addresses? |
| adult | boolean | Is this URL or domain hosting dating or adult content? |
| domain\_age | object | This object contains human, timestamp, iso values |
| message | string | A generic status message, either success or some form of an error notice. |
| success | boolean | Was the request successful? |
| Errors | array of strings | Array of errors which occurred while attempting to process this request. |

**ipqs.urlreputation.results.data** , this output variable contains the JSON object containing the Processed Malicious URL data, that can be extracted using JMESPath App.

|  |  |  |
| --- | --- | --- |
| **Attribute Name** | **Attribute Type** | **Attribute Description** |
| IPQS\_Reputation | string | This value provides the IP reputation based on Fraud Score.  Possible Values are:   1. Critical 2. High Risk 3. Moderate Risk 4. Low Risk 5. Suspicious 6. Clean |
| TC\_Threat\_Rating | String | This Value provides Threat Connect Threat Rating Information  Possible Values are:   1. Critical Threat 2. High Threat 3. Moderate Threat 4. Low Threat 5. Suspicious |
| unsafe | boolean | Is this domain suspected of being unsafe due to phishing, malware, spamming, or abusive behavior? View the confidence level by analyzing the "risk\_score" |
| domain | boolean | Domain name of the final destination URL of the scanned link, after following all redirects. |
| ip\_address | string | The IP address corresponding to the server of the domain name. |
| server | string | The server banner of the domain's IP address. For example: "nginx/1.16.0". Value will be "N/A" if unavailable. |
| content\_type | string | MIME type of URL's content. For example "text/html; charset=UTF-8". Value will be "N/A" if unavailable. |
| risk\_score | integer | The IPQS risk score which estimates the confidence level for malicious URL detection. Risk Scores 85+ are high risk, while Risk Scores = 100 are confirmed as accurate |
| status\_code | integer | HTTP Status Code of the URL's response. This value should be "200" for a valid website. Value is "0" if URL is unreachable. |
| page\_size | integer | Total number of bytes to download the URL's content. Value is "0" if URL is unreachable. |
| domain\_rank | integer | Estimated popularity rank of website globally. Value is "0" if the domain is unranked or has low traffic. |
| dns\_valid | boolean | The domain of the URL has valid DNS records. |
| suspicious | boolean | Is this URL suspected of being malicious or used for phishing or abuse? Use in conjunction with the "risk\_score" as a confidence level. |
| phishing | boolean | Is this URL associated with malicious phishing behavior? |
| malware | boolean | Is this URL associated with malware or viruses? |
| parking | boolean | Is the domain of this URL currently parked with a for sale notice? |
| spamming | boolean | Is the domain of this URL associated with email SPAM or abusive email addresses? |
| adult | boolean | Is this URL or domain hosting dating or adult content? |
| domain\_age | object | This object contains human, timestamp, iso values |
| message | string | A generic status message, either success or some form of an error notice. |
| success | boolean | Was the request successful? |
| Errors | array of strings | Array of errors which occurred while attempting to process this request. |

# **4. IPQualityScore Playbook Templates**

## **4.1. IPQualityScore Playbook Templates Installation**

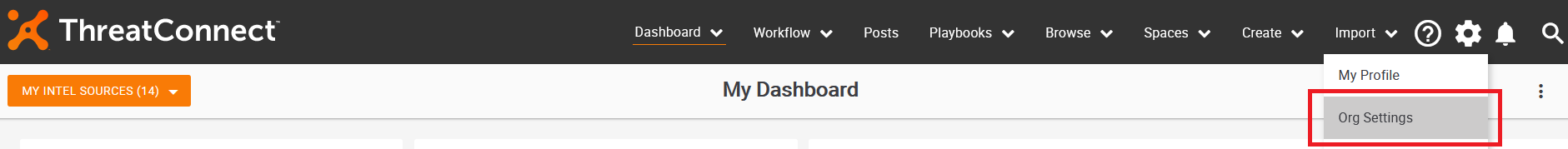
**IPQualityScore** provides three Playbook Templates **IPQualityScore IP Address Reputation Playbook Template.pbx**, **IPQualityScore Email Reputation Playbook Template.pbx** and **IPQualityScore URL Reputation Playbook Template.pbx** which are available on GitHub at: [GitHub Link](https://github.com/ThreatConnect-Inc/threatconnect-playbooks/blob/master/apps/IPQualityScore%20Enrichment/IPQualityScore_Enrichment_v1.0.tcx). These templates provide a basic understanding on how to use the IPQualityScore Enrichment App in the playbooks.

To install these Playbook Templates, go to the Playbooks tab within the ThreatConnect Platform. Select New > Import and locate the .pbx file you wish to add to your ThreatConnect Platform. Follow the on-screen instructions to complete the Playbook Template import.

## **4.2. IPQualityScore API Key Variable Set Up**

**Note**: This step is required, if not Playbook Templates will not work as expected. If you want to skip this step, you need to provide IPQualityScore API Key in each of the Playbook Template.

* Click on the settings (gear icon) in the top right corner in the ThreatConnect platform to select Org Settings and then Variables.



* Go to Variables.

1. Click on New Variable
2. Type = KEYCHAIN
3. Name = IPQualityScore API Key
4. Value = API Key provided by IPQualityScore
5. Click on Save.



Graphical user interface, application, Teams

Description automatically generated

## **4.3. IPQualityScore Custom Attributes Set Up**

**Note**: This step is required, if not Playbook Templates will not work as expected.

You can find the **IPQualityScore\_Attributes.json** file available on GitHub at: [GitHub Link](https://github.com/ThreatConnect-Inc/threatconnect-playbooks/blob/master/apps/IPQualityScore%20Enrichment/IPQualityScore_Enrichment_v1.0.tcx)., please download it.

**Step 1:** Click on the settings (gear icon) in the top right to get to your Org Config page as shown below.

A screenshot of a cell phone

Description automatically generated

**Step 2**: Click on the Upload button as shown below.

A screenshot of a cell phone

Description automatically generated

**Step 3**: Click on the Select File button and navigate to the **IPQualityScore\_Attributes.json** file, which was downloaded previously.

A screenshot of a social media post

Description automatically generated

**Step 4**: Click on Save to create the IPQualityScore Custom Attributes.

Graphical user interface, table

Description automatically generated

**Step 5**: After saving the IPQualityScore custom attributes will be created as shown below.

Table

Description automatically generated

Table

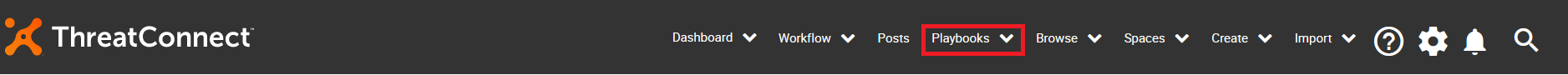
Description automatically generated

Graphical user interface, application, Teams

Description automatically generated

## **4.4. IPQualityScore Playbook Templates Activation**

**Step1**: Go to the playbook menu in the top banner area to select the IPQualityScore playbook Templates as shown below.



**Step2**: Click and open each of the IPQualityScore playbook Templates.



**Step3**: Toggle the switch to mark the playbook as active.







# **5.** **Running IP Address Reputation Playbook Template**

This Playbook Template provides the Reputation (Critical, High Risk, Moderate Risk, Suspicious, Clean) and Threat Rating (Critical Threat, High Threat, Moderate Threat, Suspicious) for the provided IP Address based on recent reputation and risk analysis across the IPQS threat network. The Playbook also enriches the IP address with reputation details such as Fraud Score, Abuse Velocity, Connection Type, ISP, Recent Abuse, and Proxy/VPN & TOR status as custom attributes and other important data points such as location and organization in the description attribute.

**Step1:** Browse to the existing Address Indicator (or) Create a new Address Indicator as shown below.

**Graphical user interface, application

Description automatically generated**

**Graphical user interface

Description automatically generated**

**Step2:** You can see the “IPQualityScore IP Address Reputation” Playbook Action in the Address Indicator details page.

Graphical user interface, application, Teams

Description automatically generated

**Step3:** Run the playbook by clicking on the Play button. The Status for the playbook Action will change to Completed when done.

Graphical user interface, application, Teams

Description automatically generated

**Step4:** Now, refresh the Indicator Details page. You will see the following Custom attributes are created.

Graphical user interface, text, application, Teams

Description automatically generated

Graphical user interface, text, application, Teams

Description automatically generated

Graphical user interface, application

Description automatically generated

**Step5:** You will see IPQualityScore Tag and Threat Rating will be updated based on API Response. For detailed Mapping, please refer [Threat Rating Metrics Table](#ThreatMappingTable).

Graphical user interface, application, Teams

Description automatically generated

# **6. Running Email Address Reputation Playbook Template**

This Playbook Template provides the Reputation (Critical, High Risk, Moderate Risk, Low Risk, Invalid, Clean) and Threat Rating (Critical Threat, High Threat, Moderate Threat, Low Threat, Suspicious) for the provided Email Address based on the status of email’s inbox (validation check) and recent reputation across the IPQS threat network. It also adds First Seen information as a custom attribute and other important information such as Fraud Score, Recent Abuse, Deliverability, and more in the description attribute for the provided Email Address.

**Step1:** Browse to the existing Email Address Indicator (or) Create a new Email Address Indicator as shown below.

**Graphical user interface, application

Description automatically generated**

**Graphical user interface, text, application

Description automatically generated**

**Step2:** You can see the “IPQualityScore Email Address Reputation” Playbook Action in the Address Indicator details page.

Graphical user interface, application

Description automatically generated

**Step3:** Run the playbook by clicking on the Play button. The Status for the playbook Action will change to Completed when done.

Graphical user interface, application

Description automatically generated

**Step4:** Now, refresh the Email Address Indicator Details page. You will see the following Custom attributes are created.

Graphical user interface, text, application, email

Description automatically generated

**Step5:** You will see IPQualityScore Tag and Threat Rating will be updated based on API Response. For detailed Mapping, please refer [Threat Rating Metrics Table](#ThreatMappingTable).

Graphical user interface, application, Teams

Description automatically generated

.

# **7. Running URL/Domain Reputation Playbook Template**

This Playbook Template provides the Reputation (Critical, High Risk, Moderate Risk, Low Risk, Suspicious, Clean) and Threat Rating (Critical Threat, High Threat, Moderate Threat, Low Threat, Suspicious) for the provided URL/Domain based on Risk Score. It also adds Domain Rank, IP Address, and Status for Malware, Parking, Phishing, Spamming, and Suspicious or Unsafe behavior as custom attributes, and other important information in the description attribute for the provided URL/Domain.

**Step1:** Browse to the existing URL or Host Indicator (or) Create a new URL or Host Indicator as shown below.

**Graphical user interface, application

Description automatically generated**

**Graphical user interface, application

Description automatically generated**

**Step2:** You can see the “IPQualityScore URL Reputation” Playbook Action in the Address Indicator details page.

Graphical user interface, application, Teams

Description automatically generated

**Step3:** Run the playbook by clicking on the Play button. The Status for the playbook Action will change to Completed when done.

Graphical user interface, application

Description automatically generated

**Step4:** Now, refresh the Indicator Details page. You will see the following Custom attributes are created.

Graphical user interface, text, application

Description automatically generated

Graphical user interface, application, Teams

Description automatically generated

Graphical user interface, text, application

Description automatically generated

**Step5:** You will see IPQualityScore Tag and Threat Rating will be updated based on API Response. For detailed Mapping, please refer [Threat Rating Metrics Table](#ThreatMappingTable).

Graphical user interface, application

Description automatically generated

# **8. Threat Rating Metrics Table**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Fraud Score** | **Risk Score** | **Other Data Point** | **IPQS Reputation Tag** | **THREAT RATING** |
| **IP Address** | **== 100** |  |  | **Critical** | **Critical Threat** |
|  | **>= 85 & <=99** |  |  | **High Risk** | **High Threat** |
|  | **>=75 & <=84** |  |  | **Moderate Risk** | **Moderate Threat** |
|  | **>=60 & <=74** |  |  | **Suspicious** | **Suspicious** |
|  | **<=59** |  |  | **Clean** | **N/A** |
|  |  |  |  |  |  |
| **Email Address** |  |  | **Disposable = true** | **Critical** | **Critical Threat** |
|  | **== 100** |  |  | **High Risk** | **High Threat** |
|  | **>=88 & <=99** |  |  | **Moderate Risk** | **Moderate Threat** |
|  | **>=80 & <=87** |  |  | **Low Risk** | **Low Threat** |
|  |  |  | **valid = false** | **Invalid** | **Suspicious** |
|  | **<=79** |  |  | **Clean** | **N/A** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| **URL** |  |  |  |  |  |
|  |  |  | **malware=true** | **Critical** | **Critical Threat** |
|  |  |  | **phishing=true** | **Critical** | **Critical Threat** |
|  |  | **>=90** |  | **High Risk** | **High Threat** |
|  |  | **>=80 & <=89** |  | **Moderate Risk** | **Moderate Threat** |
|  |  | **>=70 & <=79** |  | **Low Risk** | **Low Threat** |
|  |  | **>=55 & <= 69** |  | **Suspicious** | **Suspicious** |
|  |  | **<= 54** |  | **Clean** | **N/A** |