EclecticIQ

EclecticIQ Platform

Enricher - Recorded Future

Last generated 05/12/2020

Table of contents

This article describes the specific configuration options to set up the enricher.
To configure the general options for the enricher, see Configure the general options[1].

	Specifications
Enricher name	Recorded Future
Input	Domain, hashes (sha1, md5, sha512, sha256), ipv4, and uri.
Output	The enricher returns additional data such as IPs, domains, email addresses, and hashes related to the submitted observables types, as well as maliciousness confidence levels based on the retrieved risk scores.
API endpoint	• `/api/v2/ip/{Ipv4}` • `/api/v2/domain/{Domain}` • `/api/v2/hash/{Hash}` • `/api/v2/url/{Uri}`
Description	The Recorded Future integration provides both a feed and enricher capabilities. With the feed, users have access to the Recorded Future Risk List which includes IP and file hashes, for example. The results are provided in standard STIX/TAXII protocols including TTPs and Indicators. The enricher allows users to query Domains, hashes, URLs and IP addresses.

Requirements

The Recorded Future enricher is compatible with EclecticIQ Platform release 2.3 and later. Users need an API key for their own configuration. Sign up and subscribe to the service to obtain the required API key credentials to access the API endpoint exposing the service.

1 https://docs.eclecticiq.com/display/LAT/Configure+enrichers

Configure the enricher parameters

1. In the top navigation bar, click **Data configuration > Enrichers > PyDat > Edit**.
2. From the **Observable types** drop-down menu, select one or more observable types you want to enrich with data retrieved through the enricher.
3. The **API URL** field is automatically filled in with the default domain for the endpoint.
   You can add a proxy or set up ports according to your needs.
   Default value: `https://api.recordedfuture.com`.
4. In the **API key** field, enter your API key to access the intelligence provider API and to consume the available services through their API endpoints.
5. In the **Maliciousness threshold (low)** field, enter a value between *0* and *99*.
   Analyzed observables with a higher risk score than the value defined here are flagged as **Malicious – Low confidence**.
   After completing the analysis, enrichment observables with a *higher* risk score than the *low maliciousness threshold,* and lower than the medium and high maliciousness thresholds, are flagged as **Malicious – Low confidence**.
   - Default value: *5*.
6. In the **Maliciousness threshold (medium)** field, enter a value between *0* and *99*.
   Analyzed observables with a higher risk score than the value defined here are flagged as **Malicious – Medium confidence**.
   After completing the analysis, enrichment observables with a *higher* risk score than the *medium maliciousness threshold,* and lower than the high maliciousness threshold, are flagged as **Malicious – Medium confidence**.
   - Default value: *24*.
7. In the **Maliciousness threshold (high)** field, enter a value between *0* and *99*.
   Analyzed observables with a higher risk score than the value defined here are flagged as **Malicious – High confidence**.
   After completing the analysis, enrichment observables with a *higher* risk score than the *high maliciousness threshold* are flagged as **Malicious – High confidence**.
   - Default value: *65*.

   To store your changes, click **Save**; to discard them, click **Cancel**.

Additional information

Polling the Recorded Future API through the Recorded Future can consume Recorded Future credits.
API access depends on a daily quota of API credits. API requests consume API credits:

API request	Credits per request
Risk list download	5
Lookup or search that returns results	1
Lookup or search that returns only a count	0

When your user account exceeds the daily credit quota, API access is disabled until the beginning of the next calendar day.

See also

- About enrichers[2]
- Configure enrichers[3]
- Enable and disable enrichers[4]
- Run enrichers[5]
- About enrichment rules[6]
- List of enrichers[7]

2 https://docs.eclecticiq.com/display/PINT/About+enrichers
3 https://docs.eclecticiq.com/display/PINT/Configure+enrichers
4 https://docs.eclecticiq.com/display/PINT/Enable+and+disable+enrichers
5 https://docs.eclecticiq.com/display/PINT/Run+enrichers
6 https://docs.eclecticiq.com/display/PINT/About+enrichment+rules
7 https://docs.eclecticiq.com/display/PINT/List+of+enrichers