Query.AI Anomali ThreatStream Enrichment v1.0.0

About Query.AI

Siloed data prevents organizations from gaining timely views into security risks. The Query.AI platform provides real-time, centralized insights from decentralized data so you can accelerate cybersecurity investigations and efficiently respond to threats.

About Query.AI Anomali ThreatStream Enrichment

The Query.AI Anomali ThreatStream Enrichment enables from Anomali, searching and accessing your cybersecurity data from across on-premises, multi-cloud, and SaaS applications, without duplicating data from its native locations.

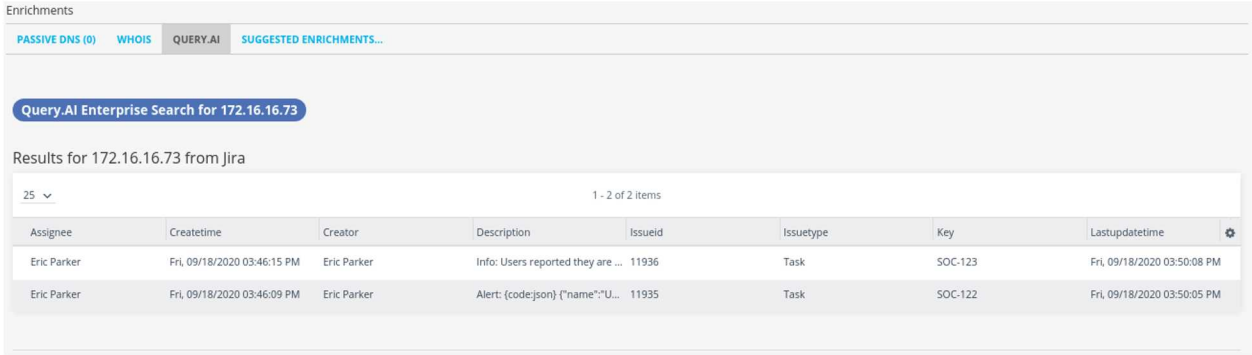
Supported Observable Type

IPAddress

Query.AI Anomali ThreatStream Enrichment widget

QueryAI Widget

Below widget shows enterprise search results for an IP Address on the Jira platform:



QueryAI Enrichment output

Enrichment displays information as a tabular result based on the Platform Connection(s) and may include custom fields configured by the user.

Steps to generate the API Key

1. Go to https://app.query.ai and click on the "**Create Account**" button. (skip to step #4 if you are already a Query.AI user)
2. Complete the registration form and validate your email. (Note: Registration is free.)
3. Configure connections to your desired data platforms
4. After successful login, from the app menu go to "**User Settings**" page
5. Look for "**API Token**" section and click on generate token
6. Copy the token and store it in a safe location

Enrichment Setup Fields

Below are the setup fields needed to activate the Query.AI Enrichment on the ThreatStream UI:

1. **API Key** (Mandatory) - Refer previous section.
2. **Platform Connections** (Mandatory) - List of Platform connection names active on Query.AI in CSV format such as "splunk_us".
3. **Search Duration** (Optional) - Search time range such as 1 hour or 1 day. If left blank, the default search duration of 1 hour is applied.

Activate Query.AI Anomali ThreatStream Enrichment

1. Log in to the ThreatStream user interface.
2. Locate the Query.AI enrichment in ThreatStream APP Store.
3. Click "***Get Access***".
4. Click the "***I have credentials***" link and enter your Query.AI API Key (refer section "Steps to generate the API Key").
5. Fill other setup fields as per need (refer section "Enrichment Setup Fields").
6. Click **Activate**.

Contact Us

Contact: support@query.ai
Website: https://query.ai