# RiskIQ PassiveTotal App for Anomali

Last Edit: December 14th, 2020


**Summary** 1

**Requirements** 1

**Integration Details** 1

Enrichment Tab 2

Graph Enrichment 4

**Support** 8


---

## Summary


RiskIQ PassiveTotal App for Anomali enables security teams to accelerate their investigations, eliminate threats and better protect their enterprise. The PassiveTotal App for Anomali allows you to aggregate, correlate and enrich Anomali data with RiskIQ's Internet Intelligence Graph, providing unparalleled context and intelligence to detect, investigate and remediate IOCs and security events.


## Requirements

In order to make use of the RiskIQ PassiveTotal App for Anomali, users must be a customer of both Anomali and RiskIQ PassiveTotal. Customers of RiskIQ will need their API credentials, located within their account settings page, in order to complete the setup of the application.

## Integration Details

The RiskIQ PassiveTotal App for Anomali integrates enrichment in two key ways—via the context tabs and through the graph interface. Regardless of the access method, customers can gain access to rich contextual information about an indicator within a single click, accelerating their investigations and understanding of a threat.

# Enrichment Tab

Anomali displays an “Enrichments” section within their interface when viewing an indicator within their system. After installing and configuring the RiskIQ PassiveTotal App for Anomali, customers will see a “RiskIQ” tab appear within the enrichments section.


Figure 1-1: Enrichments section showing the RiskIQ tab.

Upon clicking this tab, a series of sub-tabs will be displayed, showing the various data sets that RiskIQ provides. Each one of these tabs will reveal deeper contextual information about the indicator.

The RiskIQ PassiveTotal App for Anomali currently supports the following data sets.

| Data Set | Description |
|---|---|
| Resolutions (Passive DNS) | Passive DNS is a system of record that stores DNS resolution data for a given location, record and time period. This historical resolution data set allows analysts to view which domains resolved to an IP address and vice versa. This data set allows for time based correlation based on domain or IP overlap. |
| WHOIS | A protocol that lets anyone query for information about a domain, IP address, or subnet. One of the most common functions for WHOIS in threat infrastructure research is to identify or connect disparate entities based on unique data shared within the WHOIS record content. |
| Subdomains | An internet domain which is part of a primary domain. Subdomains are also referred to as “hosts.” As an example, “play.google.com” is a subdomain of “google.com”. For every subdomain, there could be a new set of IP addresses of which the domain resolves to and thus can be a great data source for finding related infrastructure. |
| DNS | The DNS Tab provides analysts with insight into MX (mail exchanger), NS (nameserver), TXT (text), SOA (start of authority), and CNAME (canonical name) records. |
| Trackers | Trackers are unique codes or values found within web pages and often used to track user interaction. These codes can be used to correlate a disparate group of websites to a central entity. |

| | |
|---|---|
| Components | Web components are details describing a web page or server infrastructure gleaned from RiskIQ performing a web crawl or scan. These components allow an analyst to understand the makeup of a webpage or the technology and services driving a specific piece of infrastructure. |
| Host Pairs | Host pairs are two domains (a parent and a child) that share a connection observed from a RiskIQ crawl. The connection could range from a top-level redirect (HTTP 302) to something more complex like an iframe or script source reference. |
| OSINT | Long and short form reporting developed by individuals and companies combined with data feeds of known bad infrastructure. This data set provides context to the actors, campaign or malicious infrastructure. |
| Hashes | Malicious software used in attacks or found on the Internet. Outlines capabilities, intent and motives of an attacker. Aids in connecting back to infrastructure. |
| SSL Certificates | SSL certificates are files that digitally bind a cryptographic key to a set of user-provided details. Using internet-scanning techniques, PassiveTotal collects SSL certificate associations from IP addresses on various ports. These certificates are stored inside of a local database and allow us to create a timeline for where a given SSL certificate appeared on the Internet. |


Figure 1-2: RiskIQ enrichments showing the sub-tabs.

Each data set tab will result in a search action performed against the RiskIQ PassiveTotal API in order to retrieve matching results. Results will be displayed in a table format and when applicable, will also provide a direct link back to the RiskIQ PassiveTotal platform.

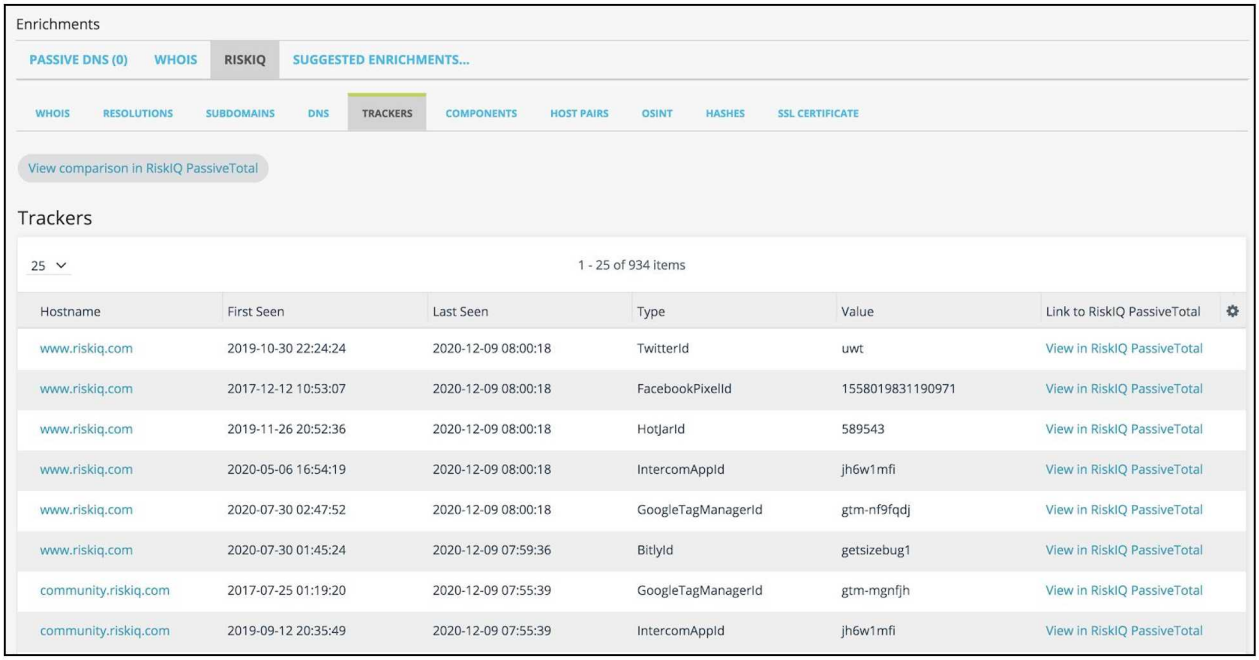


Figure 1-3: Example Tracker data set results formatted inside of a table.

It's worth noting, when a domain or IP address are part of the RiskIQ PassiveTotal results, these indicators will be linked within the Anomali platform in order to support an investigative pivot. For example, in Figure 1-3 above, the "Hostname" portion of the table has several hostname results with the first being "www.riskiq.com". Clicking on that hyperlinked indicator will perform a search within the Anomali platform, giving an analyst the opportunity to find more details and perform the same enrichments against the indicator.

# Graph Enrichment


Figure 2-1: Graph view of an indicator.

When viewing an indicator within the Anomali platform, details about the indicator will be shown alongside a graphical representation. This graphical representation is interactive and gives

analysts the ability to enrich the displayed indicator in order to build a link-graph chart of its relationships.

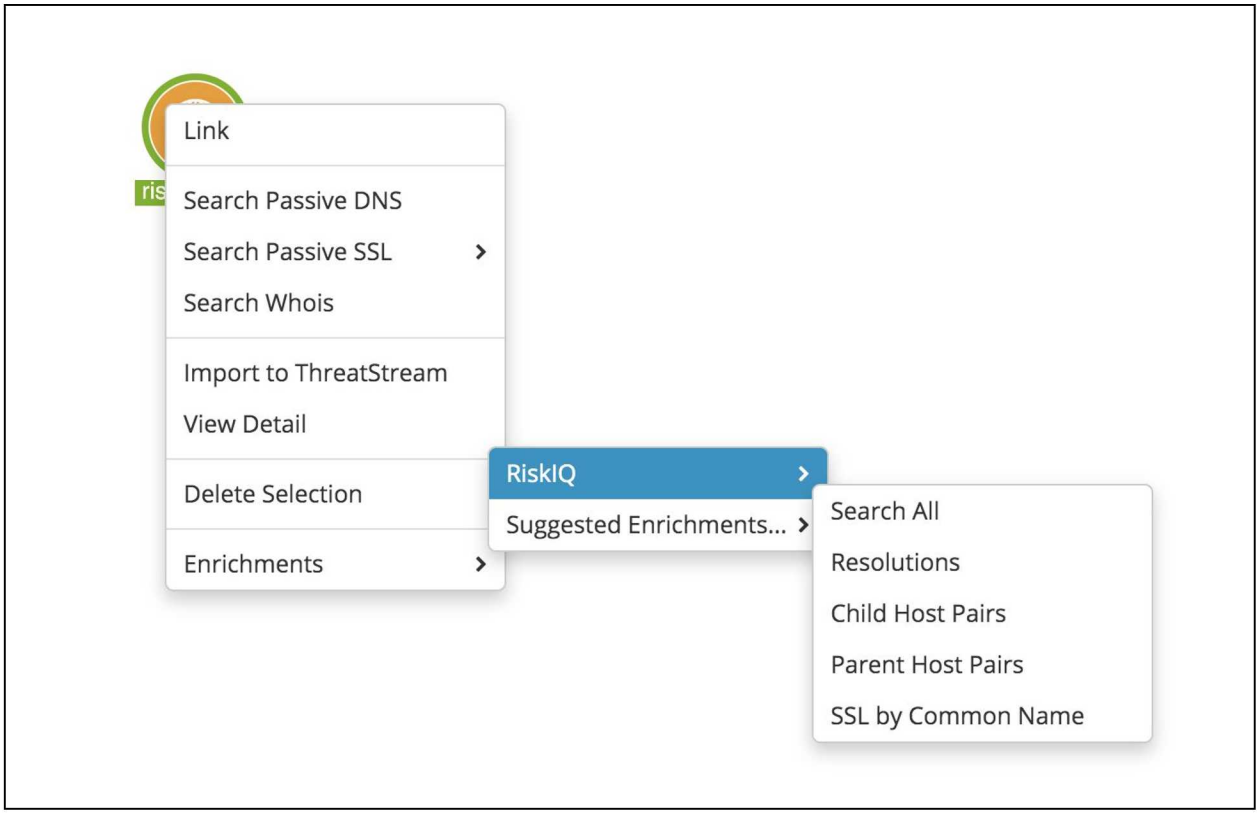


Figure 2-1: Context menu showing available enrichments within the Anomali Graph.

The RiskIQ PassiveTotal App for Anomali extends the graph to include enrichments for domains, IP addresses and email addresses using the following data sets: Passive DNS, SSL Certificates, and Host Pairs. Figure 2-1 shows the context menu available to users when right-clicking on an indicator within the graph. Upon selecting an enrichment within the graph, data will be retrieved from RiskIQ PassiveTotal and displayed as a connection to the original indicator.

The RiskIQ PassiveTotal App for Anomali currently supports the following transforms.

| **Transform** | **Entity** | **Description** |
|---|---|---|
| domainToIP | anomali.Domain | Find all IPs which the domain can be resolved to. |
| domainToChildHostPairs | anomali.Domain | Find Child Host Pairs linked to the Domain. |
| domainToParentHostPairs | anomali.Domain | Find Parent Host Pairs linked to the Domain. |

| | | |
|---|---|---|
| domainToSSL | anomali.Domain | Find SSL Certificates linked to the Domain. |
| ipToDomain | anomali.IPv4Address | Find all domains which the IP addresses can be resolved to. |
| ipToSSL | anomali.IPv4Address | Find SSL Certificates linked to the IP Address. |
| emailToDomain | anomali.Email | Find Domains linked to the email. |

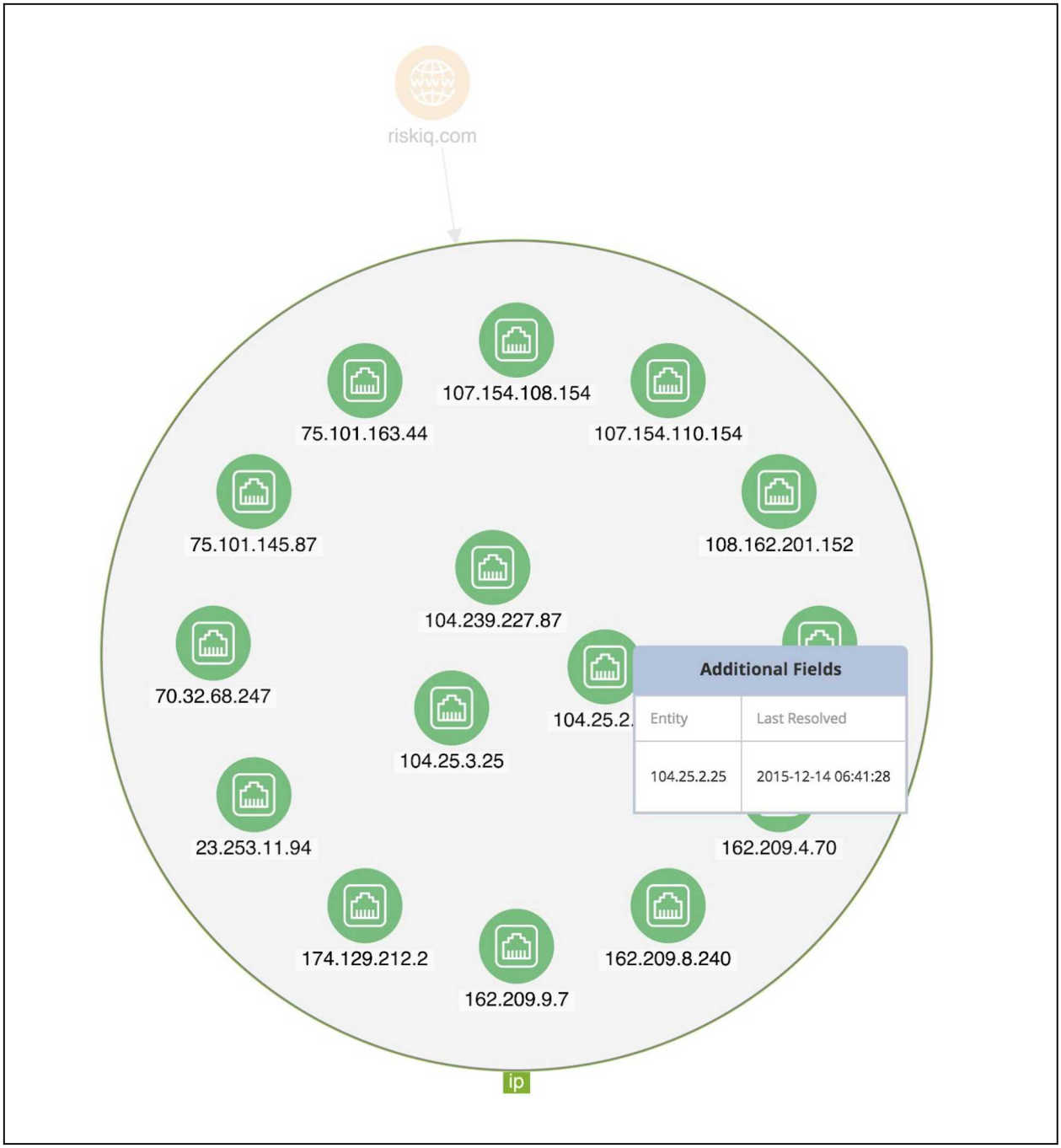


Figure 2-3: Results from enriching a domain with “Resolution” data.

When possible, entities displayed within the graph will include additional metadata information. Figure 2-3 shows an example of this data when hovering over a particular IP address. In this case, RiskIQ PassiveTotal shows the last date/time of when that indicator was associated with the enriched domain.

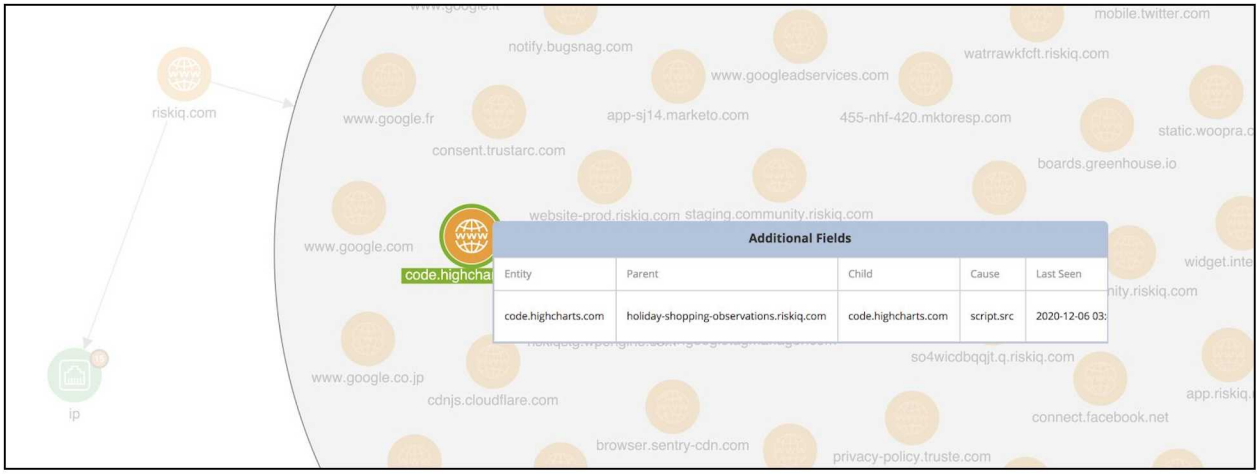


Figure 2-4: Additional metadata for an entity.

Figure 2-4 shows an additional example of metadata provided with entities from RiskIQ PassiveTotal enrichment.

# Support

RiskIQ is happy to provide support for our Anomali application. If you have questions, feedback or run into issues, please contact us using support@riskiq.com. Alternatively, existing enterprise clients can reach out directly to their support representative. Please do not contact Anomali support for issues related to the RiskIQ application.