USER GUIDE

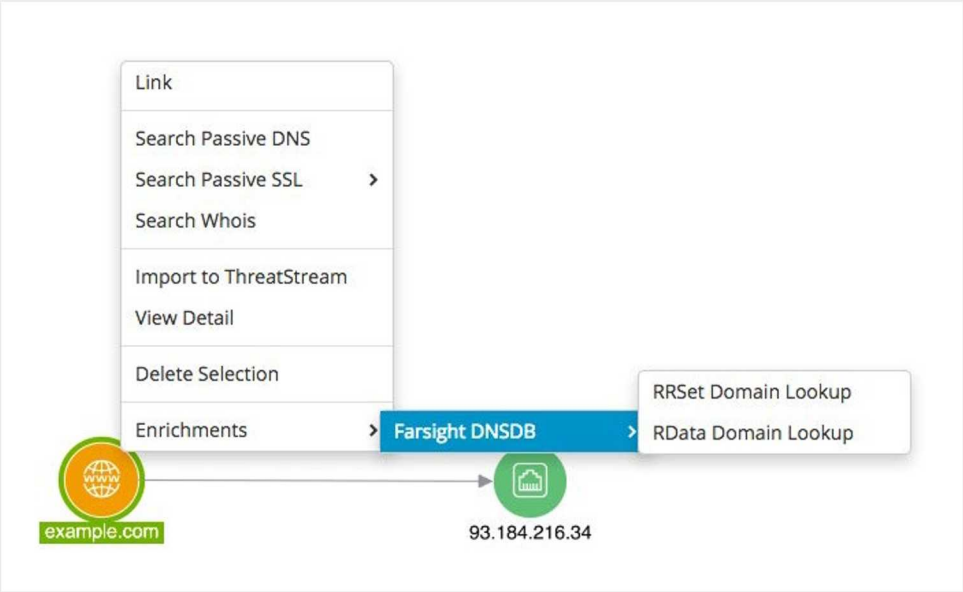
ANOMALI

FARSIGHT SECURITY

Enriching Anomali Data with Farsight Security's DNSDB®

When activated this enrichment allows you to review and pivot on domain names and IP addresses using the most recent data from Farsight Security's® passive DNS database, DNSDB®.

DNSDB pivoting options can be found when using the Explore tool context menu – right-click a domain or IP address node to get started, and then select how you want to pivot off of that node using the available RRSet and RData lookup options under the Farsight DNSDB option. Depending on how many results are found more nodes on the graph will appear.



More detailed data can be reviewed for a given Observable in the details page using DNSDB. When reviewing an Observable scroll down to the Enrichments heading and then select the 'Farsight DNSDB' enrichment to view information about a given domain or IP address in a table format. Both an RRSet and RData lookup will be performed and displayed for domains, and only a RData lookup will be performed for IP addresses. The most recent 2,000 results from each DNSDB lookup will displayed in the tables.

Enrichments

PASSIVE DNS (0) | WHOIS | FARSIGHT DNSDB | SUGGESTED ENRICHMENTS...

DNSDB RRSet Lookup Results

25 | 1 - 25 of 2,000 items

Time First (UTC)	Time Last (UTC)	Count	Bailiwick	RRName	RRType	RData
2021-07-05 16:23	2021-07-07 16:23	3025811	example.com.	example.com.	SOA	ns.icann.org. noc.dns.icann.org. 2021052033 7200 ...
2010-06-24 03:12	2021-07-07 13:29	158817867	com.	example.com.	NS	a.iana-servers.net., b.iana-servers.net.
2010-06-24 03:12	2021-07-07 13:17	162053842	example.com.	example.com.	NS	a.iana-servers.net., b.iana-servers.net.
2014-12-10 00:17	2021-07-07 12:59	27695230	example.com.	example.com.	AAAA	2606:2800:220:1:248:1893:25c8:1946
2020-11-17 17:48	2021-07-07 12:12	33701	example.com.	example.com.	TXT	"v=spf1 -all", "8j5nfqld20zpcyr8xjw0ydcfq9rk8hgm"
2019-09-05 17:28	2021-07-07 10:58	352105	example.com.	example.com.	MX	0 .
2014-12-10 00:31	2021-07-07 10:16	127940990	example.com.	example.com.	A	93.184.216.34
2021-06-29 10:23	2021-07-05 16:23	10242124	example.com.	example.com.	SOA	ns.icann.org. noc.dns.icann.org. 2021052032 7200 ...

For more information about Farsight Security and DNSDB, please visit: https://www.farsightsecurity.com/solutions/dnsdb/

The Farsight DNSDB enrichment enables the following data transformations on domain and IP address entities:

- **RRSet Domain Lookup:** returns DNS RRSet results for a given domain.
- **RData Domain Lookup:** returns DNS RRSet results for a given domain using a 'reverse' RData lookup.
- **RData IP Lookup:** returns DNS RRSet for a given IP address using a 'reverse' RData lookup.

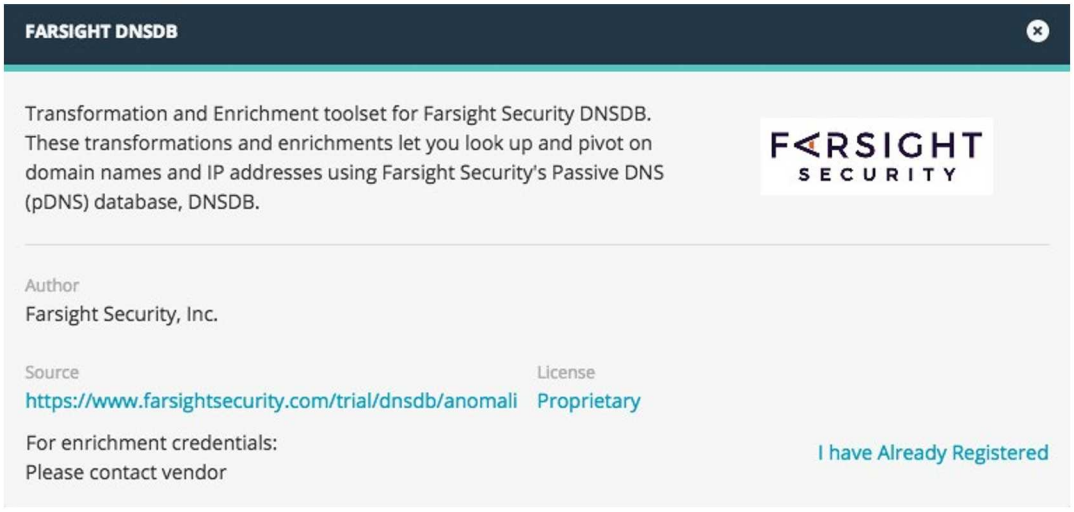
Each of these transformations have pivot variants for the interactive graph and context-based variant for displaying results in a table.

Note: Farsight's DNSDB provides enrichment data using a truncated results set for performance reasons. For more information about this, please contact support@anomali.com

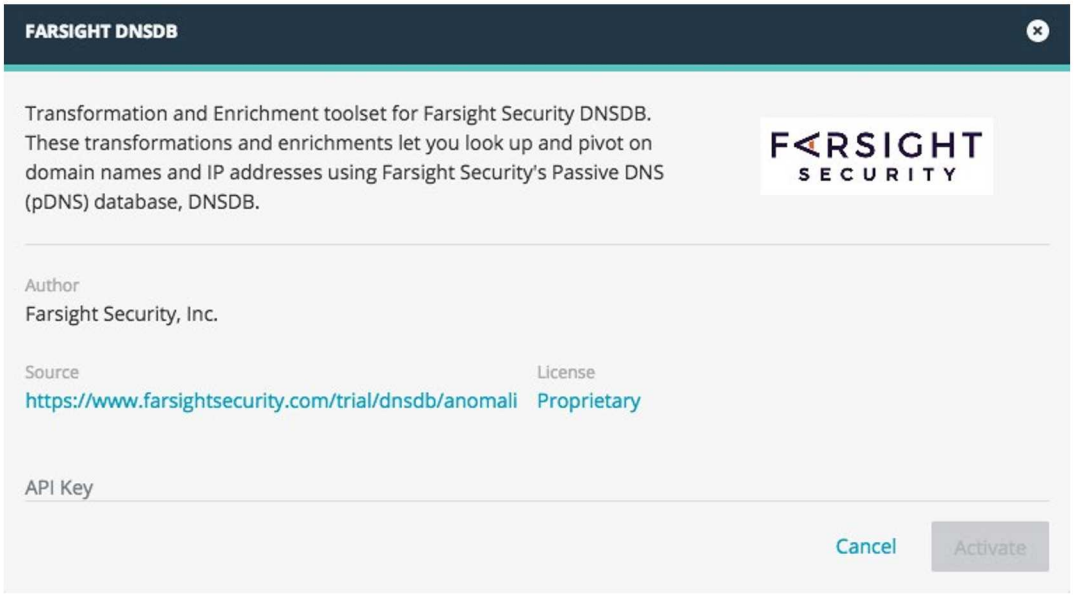
How to activate the Farsight DNSDB enrichment

1. Log into the Threatstream user interface.
2. Navigate to the Settings page by clicking the gear icon in the top-right corner.
3. Navigate to the Integrations page by clicking the Integrations header.
4. Click the Set Up button in the Farsight DNSDB Enrichment box:

5. In the popup that appears, click the 'I Have Already Registered' link:



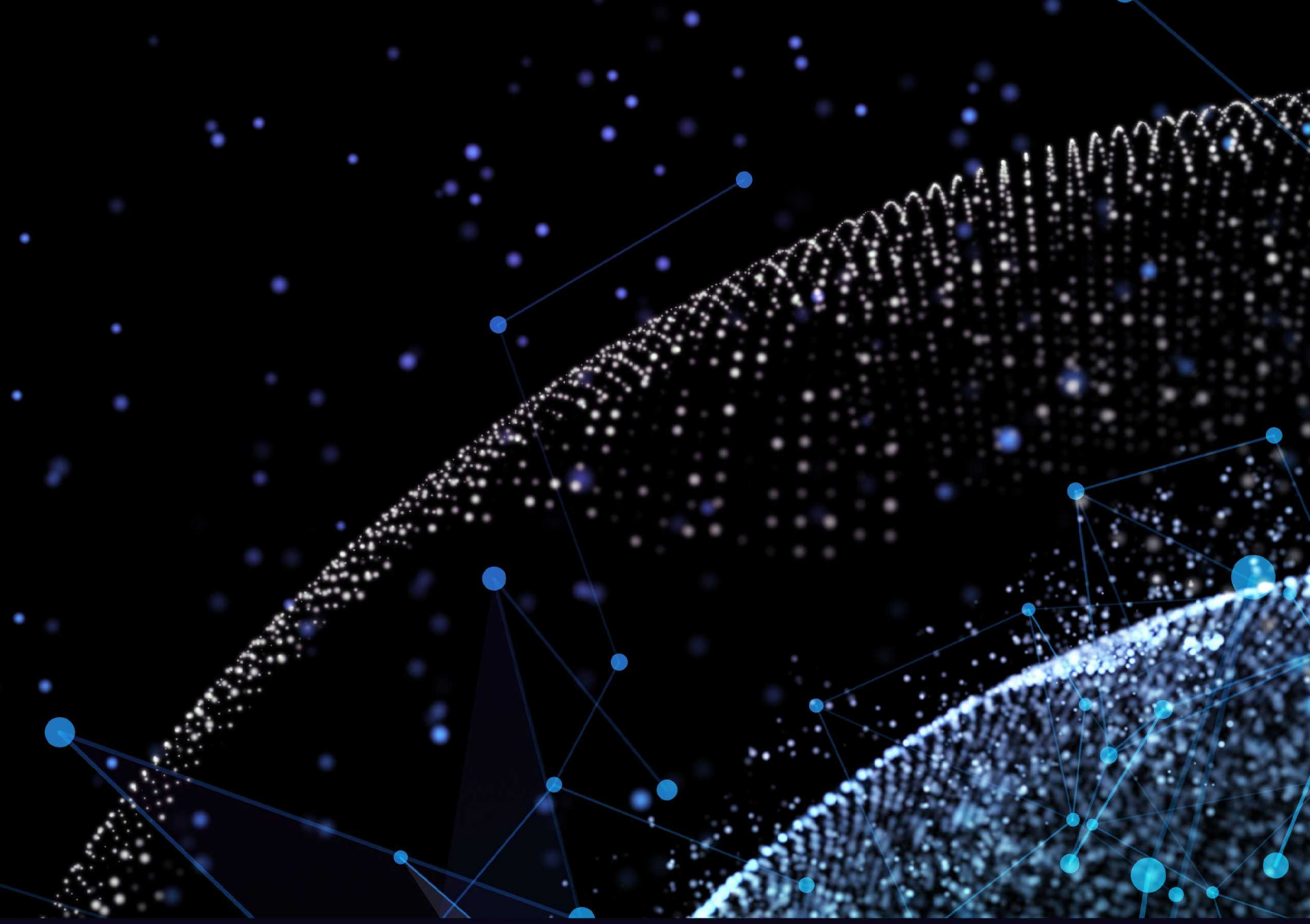
6. Enter your Farsight DNSDB API Key into the API Key field:



7. Finally, click the 'Activate' button. The Farsight DNSDB enrichment is now active.

Note: You must have a valid/active Farsight DNSDB API Key independently acquired from Anomali Threatstream or through an Anomali channel in order to use the Farsight DNSDB enrichment. For a free trial or sales inquiries, please visit: https://www.farsightsecurity.com/trial/dnsdb/anomali

If you see any errors while activating or using the Farsight DNSDB enrichment please contact support@anomali.com for assistance.



About Farsight Security, Inc.

Farsight Security®, Inc. is the world's largest provider of historical and real-time DNS intelligence solutions. We enable security teams to qualify, enrich and correlate all sources of threat data and ultimately save time when it is most critical - during an attack or investigation. Our solutions provide enterprise, government and security industry personnel and platforms with unmatched global visibility, context and response. Farsight Security is headquartered in San Mateo, California, USA.

Learn more about how we can empower your threat platform and security team with Farsight Security passive DNS solutions at https://www.farsightsecurity.com or follow us on Twitter: @FarsightSecInc.

To schedule a demo and obtain a free trial, contact: sales@farsightsecurity.com

+1-650-489-7919

Farsight Security®, Inc.177 Bovet Rd Ste 180 San Mateo, CA 94402 USA
info@farsightsecurity.com www.farsightsecurity.com