FARSIGHT SECURITY

Enriching Anomali Data

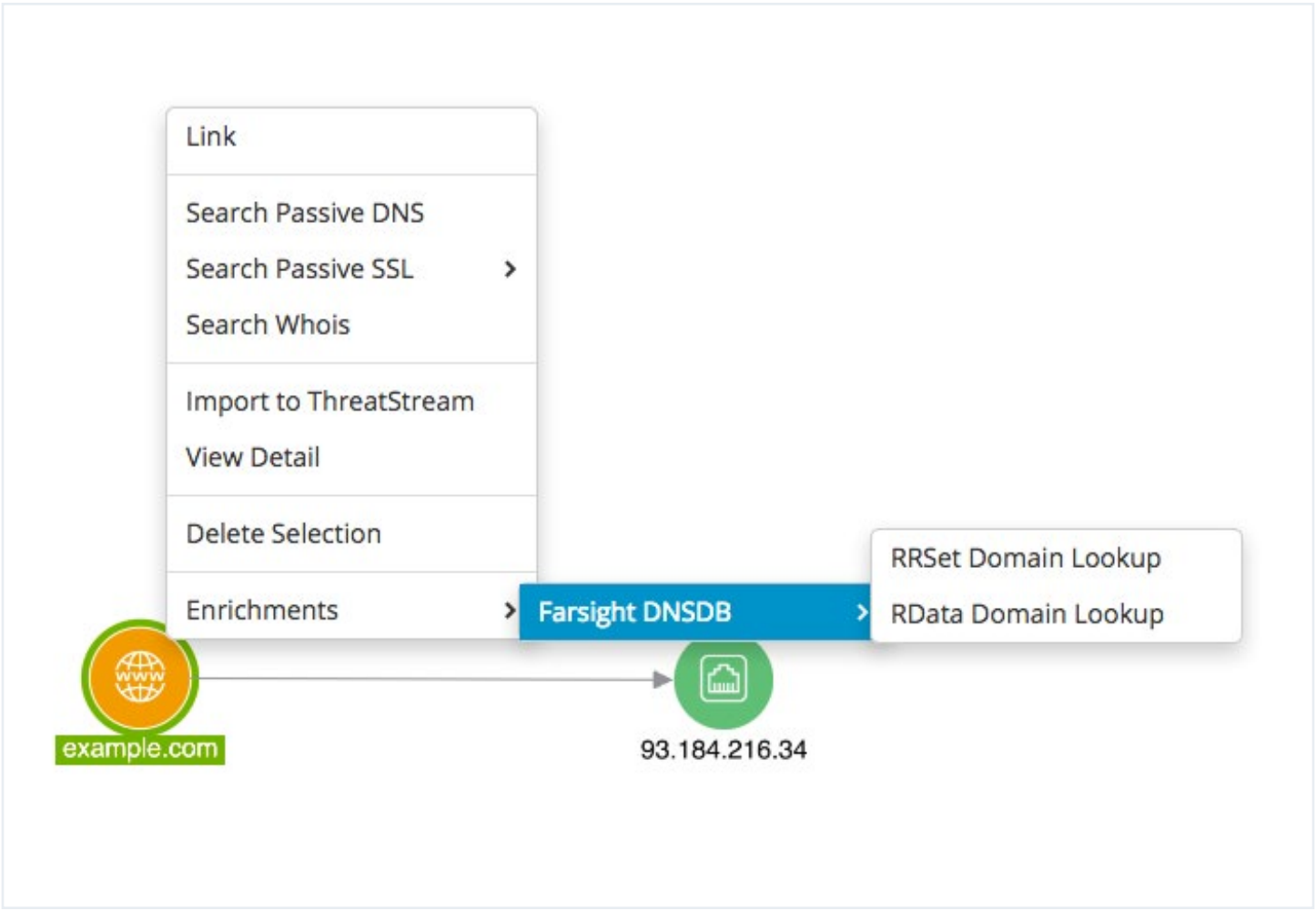
with Farsight Security's DNSDB®

ANOMALI

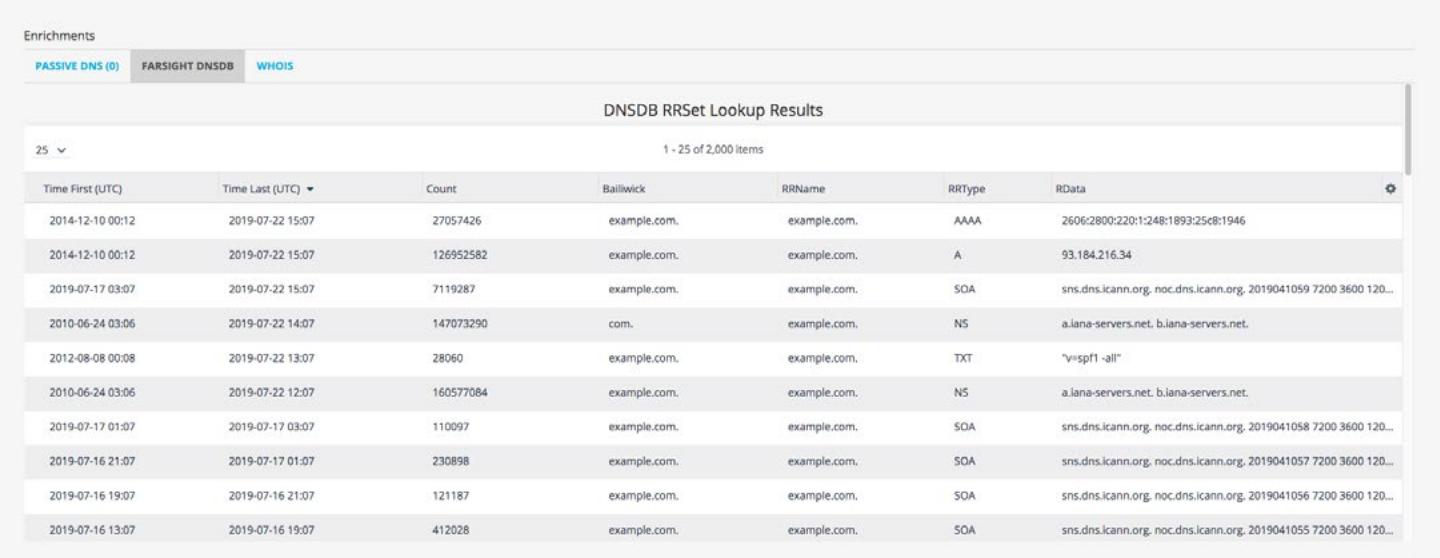
Last Updated: June 17, 2019

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.



Time First (UTC)	Time Last (UTC)	Count	Bailiwick	RRName	RRType	RData
2014-12-10 00:12	2019-07-22 15:07	27057426	example.com.	example.com.	AAAA	2606:2800:220:1:248:1893:25c8:1946
2014-12-10 00:12	2019-07-22 15:07	126952582	example.com.	example.com.	A	93.184.216.34
2019-07-17 03:07	2019-07-22 15:07	7119287	example.com.	example.com.	SOA	sns.dns.icann.org. noc.dns.icann.org. 2019041059 7200 3600 120...
2010-06-24 03:06	2019-07-22 14:07	147073290	com.	example.com.	NS	a.iana-servers.net. b.iana-servers.net.
2012-08-08 00:08	2019-07-22 13:07	28060	example.com.	example.com.	TXT	"v=spf1 -all"
2010-06-24 03:06	2019-07-22 12:07	160577084	example.com.	example.com.	NS	a.iana-servers.net. b.iana-servers.net.
2019-07-17 01:07	2019-07-17 03:07	110097	example.com.	example.com.	SOA	sns.dns.icann.org. noc.dns.icann.org. 2019041058 7200 3600 120...
2019-07-16 21:07	2019-07-17 01:07	230898	example.com.	example.com.	SOA	sns.dns.icann.org. noc.dns.icann.org. 2019041057 7200 3600 120...
2019-07-16 19:07	2019-07-16 21:07	121187	example.com.	example.com.	SOA	sns.dns.icann.org. noc.dns.icann.org. 2019041056 7200 3600 120...
2019-07-16 13:07	2019-07-16 19:07	412028	example.com.	example.com.	SOA	sns.dns.icann.org. noc.dns.icann.org. 2019041055 7200 3600 120...

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:

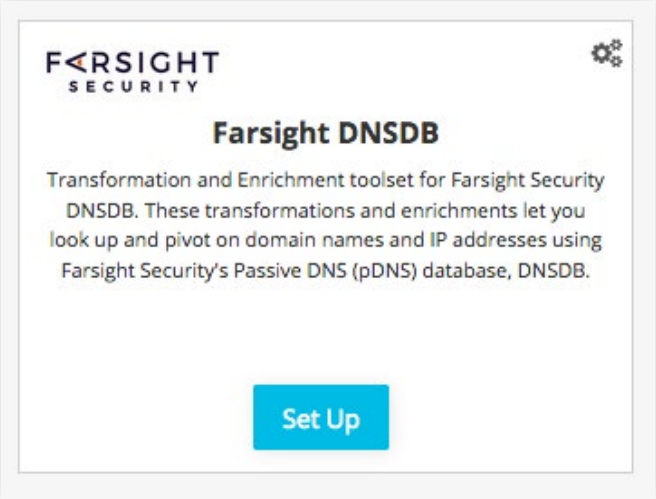
- RRSet Domain Lookup: returns DNS RRSet results for a given domain.
- RData Domain Lookup: returns DNS RRSet results for a given domain using a 'reverse' RData lookup.
- RData IP Lookup: returns DNS RRSet for a given IP address using a 'reverse' RData lookup.

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

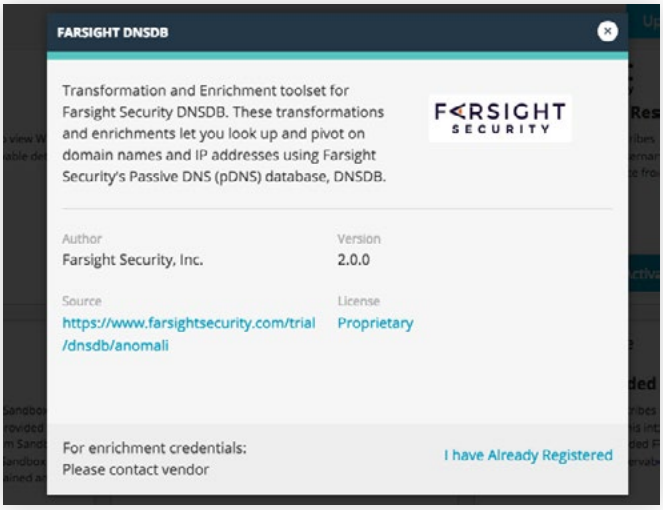
Note: Farsight's DNSDB provides enrichment data using a truncated results set for performance reasons. For more information about this, please contact support@anomali.com

How to activate the Farsight DNSDB enrichment

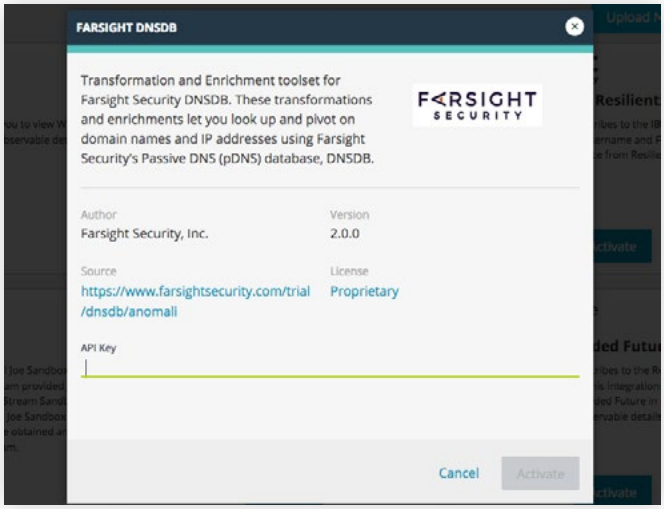
1. Log into the Threatstream user interface.
2. Navigate to the Settings page by clicking the gear icon in the top-right corner.
3. Navigate to the Integrations page by clicking the Integrations header.
4. Click the Set Up button in the Farsight DNSDB Enrichment box:



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.