PARTNER BRIEF

# Cortex XSOAR and Farsight Security DNSDB

## Increase Incident Response Speed and Accuracy

## Benefits

Together, Cortex XSOAR and Farsight Security DNSDB enable you to:

- Discover associations among threat actors and track / block their activity
- Uncover all domains using the same name server infrastructure
- Reveal the IPs an adversary is using to conceal malicious activity and avoid takedowns

## Compatibility

Cortex XSOAR, Farsight Security DNSDB

## Overview

Farsight Security DNSDB® is the world's largest DNS intelligence database that provides a unique, fact-based, multifaceted view of the configuration of the global internet infrastructure. DNSDB leverages the richness of Farsight's Security Information Exchange (SIE) data-sharing platform and is engineered and operated by leading DNS experts. Farsight collects passive DNS data from its global sensor array. It then filters and verifies the DNS transactions before inserting them into the DNSDB, along with ICANN-sponsored zone file access download data.

## Integration Features

The integration between Cortex XSOAR and Farsight DNSDB lets analysts:

- **Perform IP enrichment:** Enable the retrieval of hostnames that resolve to IP addresses to infer the reason the victim connected to a given IP address.
- **Perform hostname enrichment:** Find all IPs that a hostname has been observed resolving to around the time of observationtoidentify flows tocommand-and-control (C2) systems that change their IP addresses to avoid detection.
- **Find related hostnames:** Find other hostnames that have resolved to the same IP address as the target hostname to expand on threat intelligence by identifying alternative C2 hostnames that may be using common infrastructure.
- **Conduct interactive investigations:** Use the DNSDB API via DBot to automatically add the findings to an investigation. Perform advanced, interactive searches to aid investigations beyond the scope of provided playbooks.
- **Leverage hundreds of third-party integrations:** Coordinate response across security functions based on insights from Farsight DNSDB, taking advantage of Cortex XSOAR integration with hundreds of different third-party products.
- **Run hundreds of commands interactively:** Run commands (including for DNSDB) via a ChatOps interface while collaborating with other analysts and the Cortex XSOAR chatbot.

To measurably improve the speed and accuracy of incident response (IR), security analysts need to be able to uncover and gain context for all connected DNS-related digital artifacts in seconds, using a comprehensive, intelligent search process. Leveraging the integration of Cortex™ XSOAR and Farsight DNSDB, security practitioners can automate critical tasks to gain actionable insights into existing threat indicators and avoid dead time by coordinating actions across security projects on a single console. You can add to existing Cortex XSOAR workflows to auto-generate the query and populate the contextual information for all IPs and domain names.

## **Use Case No. 1:** Automated Enrichment

### Challenge

IR teams have visibility into DNS as it currently sits and can only resolve DNS from name to record. They need a reliable reverse-resolution and DNS history, as well as the ability to pivot from IP to name and vice versa, to retrieve the totality of logs related to an incident (e.g.,net flows related to a hostname).

### Solution

Farsight provides playbooks that integrate into your IR process. Employing Farsight's "Hostname from IP," "IPs from Hostname," and "Related Hostnames" playbooks in Cortex XSOAR automates the search. Teams can retrieve all hostnames seen for a given IP, all IPs for a given hostname, or a limited number of other hostnames seen on the same IPs as the target hostname. You can incorporate these playbooks into your IR pipeline for automated retrieval of relevant log data.

### Benefit

Automated IP-to-hostname queries reduce the time needed to respond to incursions and get a comprehensive view of the attacker's infrastructure. Automatic expansion and enrichment of the search base saves time because all the data is assembled.

## **Use Case No. 2:** Automated Enhancement of Interactive Forensic Investigations

### Challenge

Time is of the essence when responding to an incident. Threat teams need to be able to expand investigations to move beyond the scope of standard playbooks to perform advanced searches.

### Solution

Using the DNSDB API via DBot automatically adds the search findings to an investigation. This allows analysts to perform advanced, interactive searches that will aid their investigation beyond the scope of provided playbooks.

### Benefit

Automated enhancement increases the efficacy of other playbooks by enriching the findings with real-time and historical DNS data.

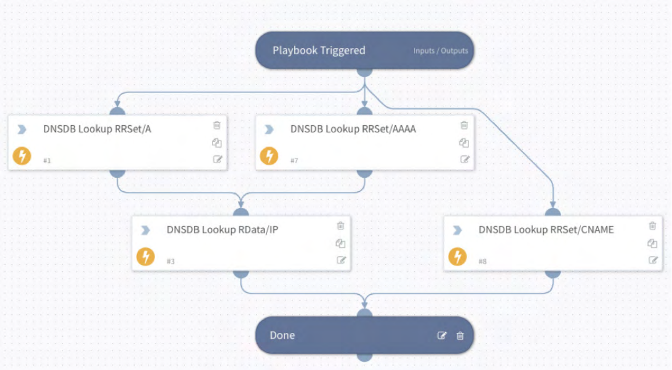
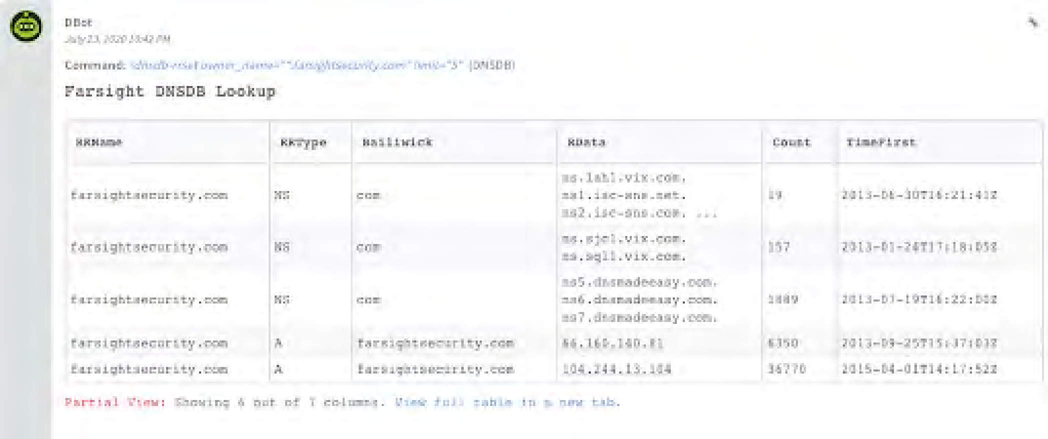


**Figure 1:** Condensed Co-Located Hostnames playbook



DBot
July 23, 2020 13:42 PM

Command: !dnsdb-rrset owner_name="*.farsightsecurity.com" limit="5" (DNSDB)

Farsight DNSDB Lookup

| RRName | RRType | Bailiwick | RData | Count | TimeFirst |
|---|---|---|---|---|---|
| farsightsecurity.com | NS | com | ns.lah1.vix.com.,<br>ns1.isc-sns.net.,<br>ns2.isc-sns.com., ... | 19 | 2013-06-30T16:21:41Z |
| farsightsecurity.com | NS | com | ns.sjc1.vix.com.,<br>ns.sql1.vix.com. | 157 | 2013-01-24T17:18:05Z |
| farsightsecurity.com | NS | com | ns5.dnsmadeeasy.com.,<br>ns6.dnsmadeeasy.com.,<br>ns7.dnsmadeeasy.com. | 1889 | 2013-07-19T16:22:00Z |
| farsightsecurity.com | A | farsightsecurity.com | 66.160.140.81 | 6350 | 2013-09-25T15:37:03Z |
| farsightsecurity.com | A | farsightsecurity.com | 104.244.13.104 | 36770 | 2015-04-01T14:17:52Z |

Partial View: Showing 6 out of 7 columns. View full table in a new tab.

**Figure 2:** Search results in the Cortex XSOAR War Room

## About Cortex XSOAR

Cortex™ XSOAR is the only security orchestration, automation, and response (SOAR) platform that combines security orchestration, incident management, and interactive investigation to serve security teams across the incident lifecycle. With Cortex XSOAR, security teams can standardize processes, automate repeatable tasks, and manage incidents across their security product stack to improve response time and analyst productivity.

For more information, visit paloaltonetworks.com/cortex/xsoar.

## About Farsight Security

Farsight Security® is the world's largest provider of historical and real-time Passive DNS data. 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 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