FARSIGHT SECURITY

Corporate Overview

Everything Starts with DNS

As early as 2007, Internet pioneer, Dr. Paul Vixie recognized that real-time observations of global Internet activity could significantly help security teams improve their risk posture against cyber attacks. He focused on the Domain Name System (DNS) which maps domain names to IP addresses and other Internet resources - the basis for everything on the Internet.

Today, at Farsight Security®, we leverage our global and diverse sensor array to collect, aggregate and process over 200,000 DNS resolution observations per second. This real-time data is made available through our Security Information Exchange (SIE) platform, where it is offered in a variety of real-time solutions and specific data alerts (Sentry).

We also create over five terabytes of DNS records information daily. This data includes over 100 billion domain resolutions. Since every threat or attack leaves broad fingerprints across the Internet, using the Farsight DNS Database (DNSDB®), SOC and Incident Response teams gain context and historical reference to attacks, threat actors and their networks.

SOC, Incident Response, Threat Intelligence and Network teams consume data from SIE, Sentries and DNSDB® into existing workflows. They use common formats such as real-time telemetry, historical, indexed databases, RPZs and RBL feeds to DNS servers, firewalls, routers and switches for real-time threat mitigation.

5TB
DNS data collected daily

100+
Billion DNS Records

200K+
Observations/second

1Gb/sec
Real-time streaming data

DNSDB® 2.0

Now search using
Regular Expressions (REGEX)
and Globbing

Data at Rest - Historical DNS Intelligence

Cybercriminals Rely on DNS

Cybercriminals quickly switch between domains, IPs and hosting infrastructure to avoid detection; all of these changes have a DNS record associated with them - thereby leaving footprints. Security teams need to analyse historic DNS records to gain a global picture of how domains and IPs were used - or are currently in use - by cybercriminals. With this added visibility, security teams will detect global patterns of malicious activity, understand cybercriminal strategy and take a proactive role in blocking future attacks.

DNSDB Uncovers DNS Footprints

Farsight Security's DNSDB is the world's largest database of DNS resolution and change data. Started in 2010 and updated in real-time, DNSDB provides the most comprehensive history of domains and IP addresses worldwide.

This DNS data is observed and collected through our global sensor array. We verify the DNS transactions before updating them into DNSDB, along with ICANN-sponsored zone file access download data. This results in the highest-quality and most comprehensive DNS intelligence data service of its kind.

Access Method	Description
DNSDB 2.0 API	Farsight Security's API Key portability program lets you unlock the power of DNS intelligence across dozens of SIEM, Orchestration, Automation and Threat Intelligence Platforms that already support Farsight's DNSDB RESTful API
DNSDB 2.0 API - Enterprise Block Query	Delivers DNSDB API with a more flexible block quota and enterprise account management features. Designed to accommodate intermittent and bursting usage patterns typical for investigations. Includes Enterprise management such as the ability to assign additional user contacts, each receiving their own API key and allocate a split of the quota to each user and reallocate as necessary
DNSDB 2.0 Export	An on-premises installation of DNSDB in your own environment

Correlation, Contextualization and more

- Perform fact-based risk assessments of domain names and IP addresses associated with known bad actors.
- Search using natural language keywords or wildcards. (REGEX/GLOB)
- Discover associations among threat actors and track / block their activity.
- Reveal the IPs an adversary is using to conceal malicious activity and avoid takedowns.
- Conduct third-party audits of DNS configurations.

Farsight's DNSDB is built for ease of use. Chain and pivot capabilities allow security teams to easily swing from one query to another. Time fencing, output tailoring and limiting of record types are among the capabilities that enable investigators to access the exact results they need. DNSDB queries can be automated into existing workflows through a RESTful API, web-enabled UI and integrations with security incident and event management solutions, security automation solutions and threat intelligence platforms.

Security Information Exchange

Plan ahead and prevent attacks: SIE is the backbone of how Farsight collects, aggregates, processes and delivers DNS intelligence in real-time. This data is delivered in a variety of common formats and provides up to the minute information about how the Internet is changing as seen through the DNS.

Delivery Methods

SIE Batch - Batch download via API or UI

Direct Connect - Connect directly to the SIE network

SIE Remote Access (SRA) - Remote connection with encrypted tunnel

Real-Time DNS Intelligence Channels

Newly Active Domains (NAD)

The industry's first real-time data feed that reports domains that have become active on the Internet after a brief period of inactivity (10 days or more). This data is very useful to detect, and block domains used by threat actors who are patient enough to establish a harmless reputation for domain-name assets before use or reusing expired domains that may have previously good reputations.

- Malware obstruction
- Phishing protection
- Risk Management

Newly Observed Domains (NOD)

The Newly Observed Domains (NOD) solution provides real- time actionable insights based on the newness of a domain. This enables immediate user protection until new domains are better understood by the rest of the security industry. It provides a holistic view of all DNS changes.

- Malware obstruction
- Brand protection

Newly Observed Hostnames (NOH)

The Newly Observed Hostnames (NOH) solution provides visibility of Fully Qualified Domain Names (FQDNs) – when they are first active. Using NOH, security teams can leverage real-time, actionable insights based on new hostnames that target their domains as well as their partners; thus ensuring end-to-end security.

- Name servers
- Hostnames - also known as fully qualified domain names (FQDNs)
- DNS SEC records

DNS Errors and NXDOMAINS

The DNS Errors and NXDOMAINS solution helps identify the cause of certain types of errors that prevent successful resolution of domain names.

- Operational Monitoring
- Domain Protection
- Brand and Phishing Protection
- Detection of Botnets and Domain Generation Algorithms (DGAs)

DNS Changes

The DNS Changes solution reports on global changes when existing domains have changed purposely, inadvertently or maliciously. Some examples:

- Unexpected DNS additions
- Situational awareness for sensitive environments
- Move to a new IP address
- Use of different name servers

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