**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across the Internet, using the Farsight DNS Database (DNSDB), SOC and Incident Response teams gain context and historical reference to attacks, threat actors and their networks.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.

---

**Corporate Overview**

- **Real-time streaming data**: 1Gb/sec
- **DNS Observations/second**: 200k+
- **Unique DNS records**: 100+ Billion
- **DNS data collected daily**: 5TB+
Security Information Exchange (SIE)

Plan ahead and prevent attacks: The Security Information Exchange (SIE) is a highly scalable, data-sharing platform where data is collected, aggregated, processed and streamed in real-time. It is delivered with multiple solutions in common formats and enables security professionals to accurately identify, map and protect their networks by providing worldwide Internet visibility on a turnkey basis; without the need to develop or deploy data collection infrastructures.

SOC, Incident Response, Threat Intelligence and Network teams consume SIE data into existing workflows using common formats including real-time telemetry, historical, indexed databases, RPZs and RBL feeds to DNS servers, firewalls, routers and switches for real-time threat mitigation. The Security Information Exchange is available with a variety of feeds and solutions:

- Raw and processed Passive DNS data
- Darknet/darkspace telescope data
- Full-text spam trap "spamples"
- Phishing URLs
- Malware-related metadata
- Intrusion detection system (IDS)/firewall blocking log data

SIE Solutions:

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 including:

- Malware obstruction
- Brand protection
- Spam filtering

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
- DNSSEC records
- Hostnames - also known as fully qualified domain names (FQDNs)

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
- Brand and Phishing Protection
- Domain 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 are:

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

Brand Sentry enables an organization to monitor and receive alerts for uncharacteristic usage of its brands across the Internet. Delivered in real-time, Brand Sentry provides actionable intelligence to empower an organization to quickly identify illegal, infringing or threatening online incidents against their brand in order to stop and prevent such breaches in the future.

Many of these new domain names are used in phishing attacks against users, customers and partners. They are also used for brand counterfeiting, brand abuse, identity theft and intellectual property abuse.

Through SIE, Brand Sentry looks at DNS label(s) in real-time and performs transformations and computations to determine “how similar” a DNS label or fully qualified domain name (“FQDN”) is to a specified set of brands. Brand Sentry immediately issues an alert when those brands or lookalikes are detected in DNS.

Domain Sentry

Domain Sentry monitors and alerts when domains and IP addresses under an organization’s stewardship don’t resolve to their intended endpoints. It enables organizations to monitor domains and IP addresses in real-time and provides actionable intelligence to prevent future breaches in domain and IP space resolutions.

- Reporting instances when your domains resolve outside of a predefined IP address space. This behavior indicates domain hijacking or hacking.
- Reporting any unidentified domain that resolves inside your IP address space - compromised servers or hosts, including intentionally installed hardware onto your organization’s network.

DNS Database (DNSDB)

Research and Pursue: The Farsight Security DNSDB is a passive DNS historical database providing a unique, fact-based, multifaceted view of global Internet. DNSDB leverages the richness of Farsight’s Security Information Exchange (SIE) platform and is engineered and operated by leading DNS experts.

Farsight collects passive DNS data from its global and diverse sensor array. It then filters and verifies the DNS transactions and ICANN-sponsored zone file download data before inserting them into the DNSDB. The end result is the highest-quality and most comprehensive passive DNS data service of its kind - with more than 100 billion domain resolutions since 2010.

Farsight’s DNSDB transforms threat feeds into actionable, relevant threat intelligence in real time to increase the value of an organization’s existing threat intelligence. Our high-performance, indexed, time-series DNS data ultimately improves visibility for an organization’s security program and protects its infrastructure from current and future threats. For simple integration, DNSDB queries can be automated into existing workflows.

- Accelerate incident research and post-breach analysis.
- Discover associations among threat actors and track and block their activity.
- Perform fact-based risk assessment of domain names and IP addresses.
- Uncover all domains using the same name server infrastructure used by a “known bad” domain.
- Reveal the IPs an adversary is using to conceal malicious activity and avoid takedowns.
- Conduct third-party audits of DNS configurations.
About Farsight Security

Farsight Security is the world’s largest provider of historic and real-time DNS intelligence 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. Learn more about how we can empower your threat platform and security team with Farsight Security DNS intelligence solutions.