FARSIGHT SECURITY

Security Information Exchange (SIE)

The Security Challenge

Cybercriminals create and tear down their Internet infrastructures at ever-faster rates. As they refine and evolve their attack methods, data must be collected and shared in real-time so that security teams can detect and respond to threats with equal speed.

Security professionals have a wealth of data but much of it is data from the past — the equivalent of looking in the rearview mirror while trying to drive forward. They need real-time insights into global Internet activity to increase the actionable value of threat data and understand their impact.

The Farsight Solution

Farsight's Security Information Exchange (SIE) is a highly scalable data-sharing platform in which data is collected, aggregated, processed, and rebroadcast in real-time.

SIE data enables security professionals to accurately identify, map, and protect their networks from cybercrime activity by providing global visibility on a turnkey basis. It provides immediate access to worldwide real-time data without the need to develop or deploy your own data collection infrastructure.

Using data collected from Farsight's global sensor array, SIE streams more than 200,000 observations per second, including:

- 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

> "Farsight's SIE platform is the most complete real-time security telemetry of its kind."
>
> **Alex Pinto**
> Chief Data Scientist
> MLSec Project

Data flowing through the SIE platform is available as "channels" in Farsight subscription packages:

- **Raw Passive DNS**
  Real-time views of DNS cache-miss traffic from Internet recursive resolvers. The data includes DNS configuration and content records that authoritative name servers provide to those recursive name servers.
- **Value-Added Passive DNS**
  Real-time de-duplicated, filtered and verified Passive DNS data when observed on the Internet.
- **Newly Observed Domains and Hostnames**
  Real-time, actionable insights on domains and hostnames when they are first resolved on the Internet.
- **Base Channels**
  A collection of threat-oriented feeds including honeypot data (darknet and spam), botnet (e.g., Conficker) sinkhole data. It also includes other data feeds such as phishing data, IDS and firewall log data.
- **Premium Channels**
  A range of premium security-related feeds including malware metadata, IOCs and other telemetry. Subscribers consume the intelligence as real-time event flows rather than traditional batch transfers - which are inherently behind.

Farsight's Passive DNS sensors are designed with privacy in mind, avoiding the collection of Personally Identifiable Information (PII) from stub resolvers by intentionally collecting above the recursive resolver.

Delivery Options

SIE Local Access

Subscribers that need to receive a large volume of content can co-locate a Linux host in one of Farsight's two Equinix production data centers in Palo Alto, California or Ashburn, Virginia and cross-connect to our network infrastructure.

SIE Remote Access

Content can also be delivered through a TCP stream over the Internet, which allows subscribers to invoke a first-order filtering capability across a set of channels, selecting only the subset of records that match specific domain name/IP address search criteria.

How to Subscribe

For more information, contact **sales@farsightsecurity.com** or call +1-650-489-7919.

About Farsight Security

Farsight Security provides the world's largest real-time actionable threat intelligence on changes to the Internet. Leveraging proprietary technology with more than 200,000 observations/second, Farsight provides security teams with the Internet's view of an organization's presence and how it is changing - whether purposely, inadvertently or maliciously. The world's most security-conscious organizations use Farsight threat intelligence to protect their users and infrastructure.