SIE CHANNEL GUIDE

FARSIGHT SECURITY

Real-Time Data Channels

The Data

The Security Information Exchange (SIE), from Farsight Security® Inc., is a highly scalable security information sharing platform. Farsight collects and redistributes more than 200,000 new raw observations per second from its global network of sensors. Farsight also applies unique proprietary methods to improve the usability of that data, sharing refined intelligence with SIE customers directly and via DNSDB®, the world's largest passive DNS database.

SIE distributes a variety of data types that are useful to the security professional, including:

- Raw and processed passive DNS data
- Darknet/darkspace telescope data
- SPAM sources and URLs
- Phishing URLs
- Connections from malware-infected systems (as seen by a sinkhole)
- Intrusion detection system (IDS) and firewall connection block data

SIE transports these diferent data sets as feeds, known as channels. These data sets can be tailored to meet the needs of each individual user, allowing them to subscribe to and access just the channels needed to solve their problem.

The Channels

SIE data is distributed via a series of channels. The Channel Guide is Farsight's summary of available channels and what they each contain.

SIE channels are available either through SIE Direct Connect or through SIE Remote Access (SRA) which are described later in the SIE Technical Reference document. Some SIE channels are not available through SIE Remote Access due to technical and bandwidth limitations. Whether or not a channel is available is noted in the table definitions for the channel.

For each channel we show the average and max bitrates (in bits per second) to indicate how much network bandwidth ingesting the channel will require, and the average and max payloads (per second) as an indication of the number of records that need to be handled when ingesting the channel in real time. These numbers are accurate as of September, 2019.

When you set up your Farsight SIE subscription, you can subscribe to individual channels or one of the bundles of commonly used data. Your Farsight sales representative can help you select the channels that will best meet your needs.

SIE Channel	Name	Bitrate (Max)	Payloads (Max)	SRA	Description
14	Darknet	N/A	N/A	Yes	Captured packets destined for unused network space. Can be used to monitor scanning activity and back-scatter from large spoofing attacks
24	Spam-Full	N/A	N/A	Yes	Full copies of emails sent to spam trap email addresses
25	Spam-Select	5k/sec (50)	2 (10)	Yes	Selected fields from the emails sent to **Spam-Full**
27	Phishing URLs	4K/sec (20)	1 (5)	Yes	PhishLabs data for malicious sites involved in phishing campaigns
42	IDS and Firewall Log Data	4Mb/sec (10)	400 (1500)	Yes	ThreatStop data of blocking action from IDS and Firewall devices
80	Conficker Sinkhole	N/A	N/A	Yes	Connection attempts from sinkholes that monitor activity from Conficker infected clients
115	DDos Events	N/A	N/A	Yes	Evidence of DDoS and DRDoS attacks gathered from Darknet data
204	Processed DNS Data	40Mb/ sec (60)	30K/sec (50)	Yes	Data from Farsight's global sensor array that has been deduplicated, filtered and verified
206	DNSDB Rejected Records	20Mb/ sec (25)	10K/sec (15)	Yes	Passive DNS observations from the sensor network that were malformed, not successful queries, or otherwise fail our validation process
207	DNSDB De-duplicated data	35Mb/ sec (50)	35K/sec (50)	No	Passive DNS observations from the sensor network after the de-duplication processing phase, immediately prior to the validation phase

SIE Channel	Name	Bitrate (Max)	Payloads (Max)	SRA	Description
208	DNSDB Verified data	50Mb/ sec (80)	5K/sec (15)	No	Passive DNS observations from the sensor network after the verification processing phase but prior to filtering
211	Newly Active Domains (NAD)	60k/sec (160)	2 (12)	Yes	Domains that have been observed after having not been seen for at least 10 days
212	Newly Observed Domains (NOD)	5k/sec (15)	2 (12)	Yes	Passive DNS observations of base domains not previously seen when compared to the DNSDB historical database
213	Newly Observed Hostnames (NOH)	400k/sec (610)	310 (500)	Yes	Fully Qualified Domains not previously seen when compared to the DNSDB historical database
214	DNS Changes	1.5m/ sec (2)	825 (1150)	Yes	Passive DNS observations where some aspect of the query or response was not found when compared to the DNSDB historical database
220	DNS Errors	160m/ sec	40k/sec (50)	No	Domain names where authoritative servers answered with an error code
221	NX Domains	25m/sec	30k/sec (45)	Yes	Passive DNS observations where the responding server returned the NXDOMAIN error
255	Heartbeat	1k/sec	1 (1)	Yes	Repeating data used for SIE health monitoring

Access Methods

SIE data can be accessed through these access methods:

- **SIE Batch:** This delivery mechanism batches SIE data on a per-channel basis, providing asynchronous access to SIE data on demand. You can select the datasets and time periods of interest to you and collect them either via the API or web-based dashboard
- **Direct Connect:** Connect a system directly to the SIE network. This is done by installing a server in one of the data centers where Farsight has a point of presence and then ordering a network cross connect between your server and SIE network switch. Many users prefer to lease a blade server from Farsight
- **SIE Remote Access (SRA):** Remotely connect to Farsight's servers using an encrypted tunnel from your workstation or a server in your local data center

For more information on SIE connection options, please see SIE Technical Overview document.

Additional Information

- For more information about SIE and how it can be delivered to you, please see the SIE Technical Overview
- For more information on our Passive DNS channels and to learn more about the Waterfall processing that generates them, please see the SIE Passive Channels Technical Overview
- For more information on our Base SIE channels, please see the SIE Base Channels Technical Overview
- For more information on the NOD/NOH channels please see SIE Newly Observed Domain and Hostname Channels Technical Overview
- For more information on the NXDOMAIN channels please see SIE DNS Error and NXDOMAIN Channels Technical Overview

For more technical information, please contact the Farisght Sales team at sales@farsightsecurity.com

About Farsight Security

Farsight Security, Inc. is the world's largest provider of historical and real-time DNS intelligence solutions. 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 www.farsightsecurity.com or follow us on Twitter: @FarsightSecInc.
Quoted bitrates are representative of SIE trafic as of September, 2019.