Domain Sentry

Criminals Easily Manipulate the DNS

Cybercriminals manipulate the Domain Name System (DNS) to leverage Advanced Persistent Threats (APT), and commit fraud on otherwise secure domains. Preventing cybercrime on domains is essential to safeguarding not only the people using them, but also the intellectual property at the core of every organization. With the Farsight Domain Sentry solution, organizations can easily make always-on DNS monitoring part of their security shield to protect and support their partners, customers and employees.

Actionable Intelligence

Domain Sentry monitors your organization’s domains and IP addresses in real-time to ensure appropriate usage. If there is a deviation from a specified domain-IP relationship, Domain Sentry will send an alert with enclosing context. The intelligence Domain Sentry makes available to a security team arms their activities and can prevent breaches to the domains and IP addresses under an organization’s stewardship.

Domain Sentry helps prevent breaches in domain security by:

- Reporting instances when your organization’s domains resolve outside of your predefined IP address space. This behavior can indicate domain hijacking or other criminal activity.

- Exposing any unidentified domains that resolve inside your predefined IP address space. This behavior can indicate compromised hosts or other criminal activity.

“Farsight’s SIE platform is the most complete real-time security telemetry of its kind.”
Alex Pinto
Chief Data Scientist
MLSec Project
The Technology Behind Domain Sentry

Domain Sentry monitors in real-time the Farsight Security Information Exchange (SIE) platform for your specified domains and IP addresses. Organizations set their pre-defined parameters in Domain Sentry to monitor the relationship between specific domains, IP addresses, and DNS record types. Domain Sentry reports on global changes when existing domains purposely, inadvertently, or maliciously deviate.

When such activities occur, an alert is triggered and the data surrounding the specific event is sent to an organization. If IP addresses resolve to the planned domains, no alert is sent.

The Muscle Behind Domain Sentry: Farsight SIE

Farsight observes millions of domains each day. Using the historical DNSDB database as a delta, Farsight detects that more than 100,000 of these are newly-configured domains daily. Leveraging more than 5 TB of daily real-time Passive DNS data, Farsight discovers when these domains are first used.

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 information on how the Internet is changing, with more than 200,000 observations per second. Farsight Security provides security solutions to leaders in the health care, consumer brands, banking, travel, and securities industries, as well as government law enforcement agencies.