PARTNER BRIEF

FARSIGHT SECURITY

Maltego and Farsight Security

MALTEGO

Maltego and Farsight Security together help Security and Intelligence teams and Law Enforcement to expedite their investigations by combining DNS intelligence with Maltego capabilities.

Technology Overviews

Maltego

Maltego is a comprehensive tool for graphical link analyses that offers real-time data mining and information gathering, as well as the representation of this information on a node-based graph, making patterns and multiple order connections between said information easily identifiable. With Maltego, you can easily mine data from dispersed sources, automatically merge matching information in one graph, and visually map it to explore your data landscape. Maltego offers the ability to easily connect data and functionalities from diverse sources using Transforms. Via the Transform Hub, you can connect data from over 30 data partners like Farsight, a variety of public sources (OSINT) as well as your own data. Our different Desktop Client versions, data sources and server solutions enable you to tailor Maltego to your specific needs in terms of data access, functionalities, and security requirements.

Farsight Security's Solution

Farsight Security DNSDB® is the world's largest DNS intelligence database that provides a unique, fact-based, multifaceted view of the configuration of the global Internet infrastructure. DNSDB leverages the richness of Farsight's Security Information Exchange (SIE) data-sharing platform and is engineered and operated by leading DNS experts. Farsight collects Passive DNS data from its global sensor array. It then filters and verifies the DNS transactions before inserting them into the DNSDB, along with ICANN-sponsored zone file access download data. The end-result is the highest-quality and most comprehensive DNS intelligence service of its kind — with more than 100 billion domain resolution records and updated in real-time at over 200,000 times/second.

Integration Highlights

Expand your investigations by retrieving and pivoting on passive DNS (pDNS) records for hostnames and IP addresses from Farsight with internal data and other exclusive third-party data sources such as threat intelligence feeds and infer connections between different entities.

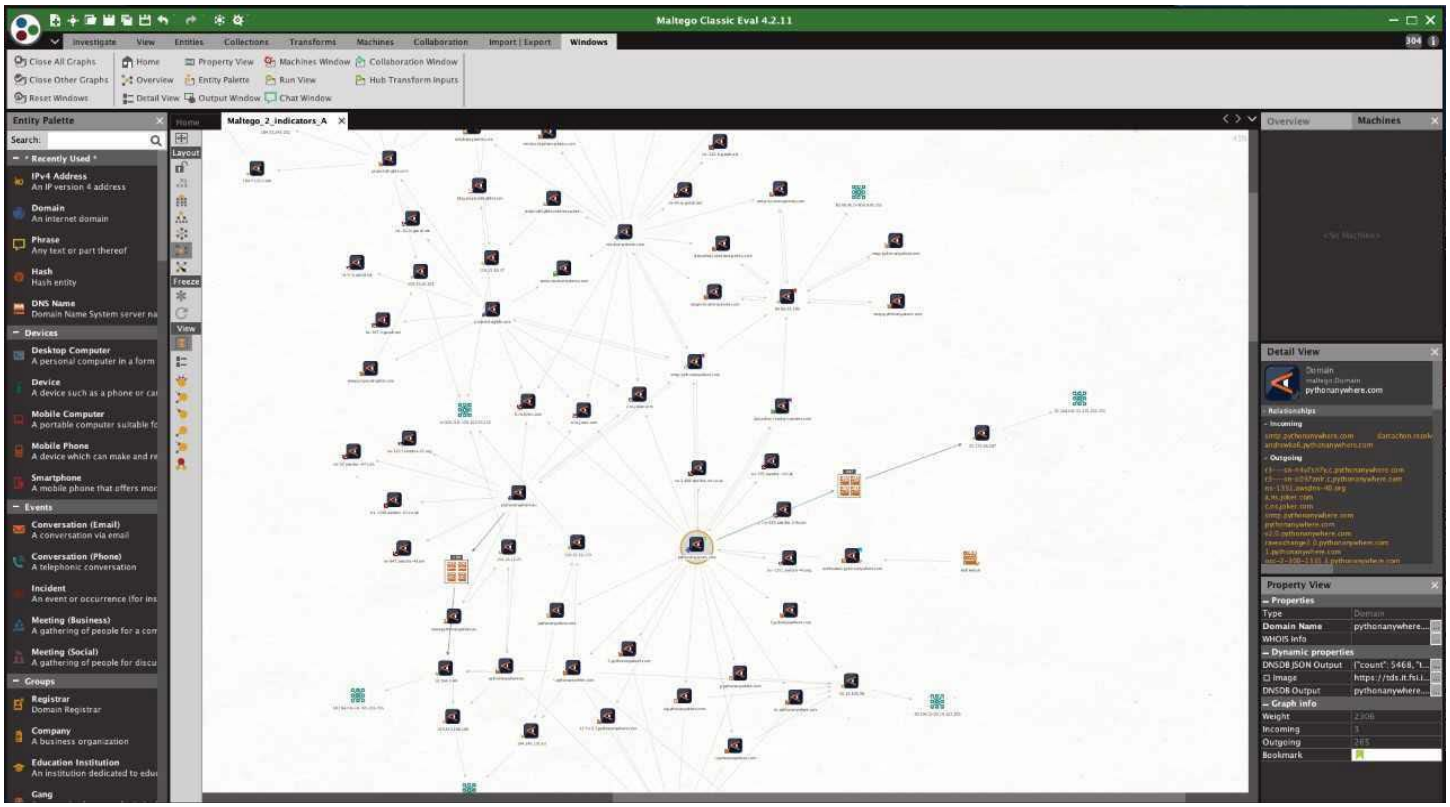
Visualize, correlate, and contextualize infrastructure relationships and quickly analyze data.

Automate repetitive steps of an investigation with the help of Maltego Machines and collaborate with teammates in real-time to share progress and insights.

Integration Use Cases

Enrich Domains and IP addresses	Infer Connections Between Different Indicators of Compromise (IOC)

- **Investigators** can expose entire networks, gain an outside-in view of their infrastructure to detect any suspicious or hostile activities and take measures to defend against malicious attacks on the systems.
- The **e-crime divisions** within Law Enforcement Agencies use historic DNS data to correlate internet and network traffic observations with other events, and gain insight into the source, ownership, and destination of internet traffic. Farsight's high-frequency updates mean officers can actively hunt for systems and people involved in cybercrime, such as hunting for the command server of an active malware campaign.



About Maltego

Maltego empowers investigators worldwide to speed up and increase the precision of their investigations through easy data integration in a single interface, aided by powerful visualization and collaborative capabilities to quickly zero in on relevant information. Maltego is a proven tool that has been downloaded by almost one million commercial and community users worldwide since its first launch in 2008. Due to its wide range of possible use cases ranging from threat intelligence to fraud investigations, Maltego is used by a broad audience, from security professionals and pen testers, to forensic investigators, investigative journalists, and market researchers.

Learn more about how we can empower your investigations at **www.maltego.com.**

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