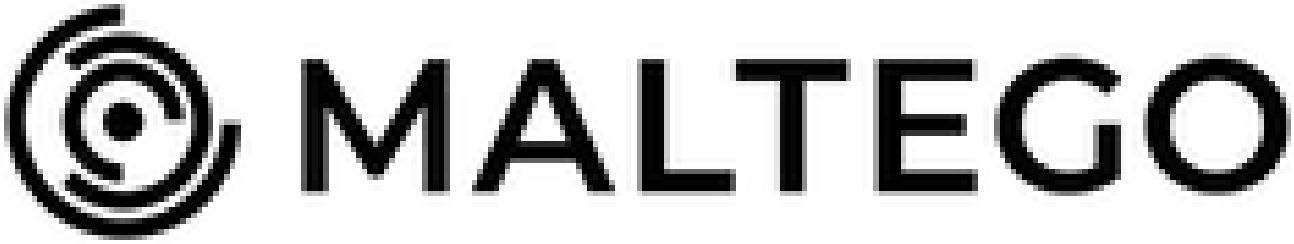
WhoisXML API Transforms Now Available on Maltego

Posted on March 20, 2022



Among the first obstacles in the way of cybercrime investigations is evidence gathering. Questions like “Where can we find the correct data for investigation?” and “Is the data we gathered enough to identify a cybercriminal?” often bug investigators and forensic teams. Without accurate and sufficient evidence, diagnoses would mostly remain assumptions and theories.

Maltego addresses this issue by employing various threat intelligence sources, which now include WhoisXML API, one of the largest domain and IP intelligence providers. With WhoisXML API transforms, Maltego enables investigators and researchers to include current and historical WHOIS and Domain Name System (DNS) records of IP addresses and domains in their investigations.

With WhoisXML API transforms in Maltego, investigators can now visually map out ownership timelines and network infrastructure, uncover hidden domain associations, and gain more insight to enhance their investigations.

What Is Maltego?

Maltego is an open-source intelligence tool (OSINT) security investigators use to gather data relevant to their investigations. It extracts data from various sources via transforms. Maltego’s Transform Hub allows investigators to collect data from over 30 data partners under diverse categories, such as blockchain, social media, web content, and threat intelligence. Furthermore, users can also integrate their own data into Maltego.

More than evidence gathering, however, Maltego stands out by allowing security investigators to create visual representations of the data they gather. They can include relevant information and entities from different sources into a chart that shows their relationships. This way, investigators can see the bigger picture.

How WhoisXML API Transforms Expand Maltego Functionality

As a leader in domain and IP intelligence provision, WhoisXML API has augmented the

capabilities of various cybersecurity solutions, such as security information and event management (SIEM) systems and threat intelligence platforms (TIPs). In the same way, the availability of WhoisXML API transforms in Maltego expands the list of threat intelligence sources of the cybercrime investigation software to include domain, IP, and DNS footprints.

In particular, WhoisXML API transforms give Maltego the following functionality:

- **WHOIS Lookup:** Users can identify the current owner of a particular domain name by extracting registration details from the WHOIS Records Transform set. That allows investigators to see who is responsible for a suspicious or malicious domain.

- **Historical WHOIS Lookup:** In most instances, current WHOIS records are redacted or privacy-protected. However, with the To Historical WHOIS Records [WhoisXML] Transform, investigators can trace past ownership records and see website owners' real identities. A domain name or an IP address can serve as a starting point for a historical WHOIS lookup, making it handy for cybercrime and person of interest investigations.

- **Reverse WHOIS Search:** With a single keyword, investigators can look up domain names that contain the text string in their WHOIS records. Users can thus see domain names that have that particular email address, company name, nameserver, mail server, registrant country, or any other WHOIS data point.

All of these domain, IP, and DNS data can be visually represented in Maltego, allowing investigators to establish relationships between entities. Learn more about WhoisXML domain and IP intelligence here:

- WHOIS History Lookup

- Reverse WHOIS Search

- WHOIS Lookup

Are you a security researcher, architect, or product developer working on the world's biggest security issues? Contact us for more information on potentially suspicious domains and other assets mentioned in this post, security research initiatives, and any other ideas for collaboration.