DOMAINTOOLS

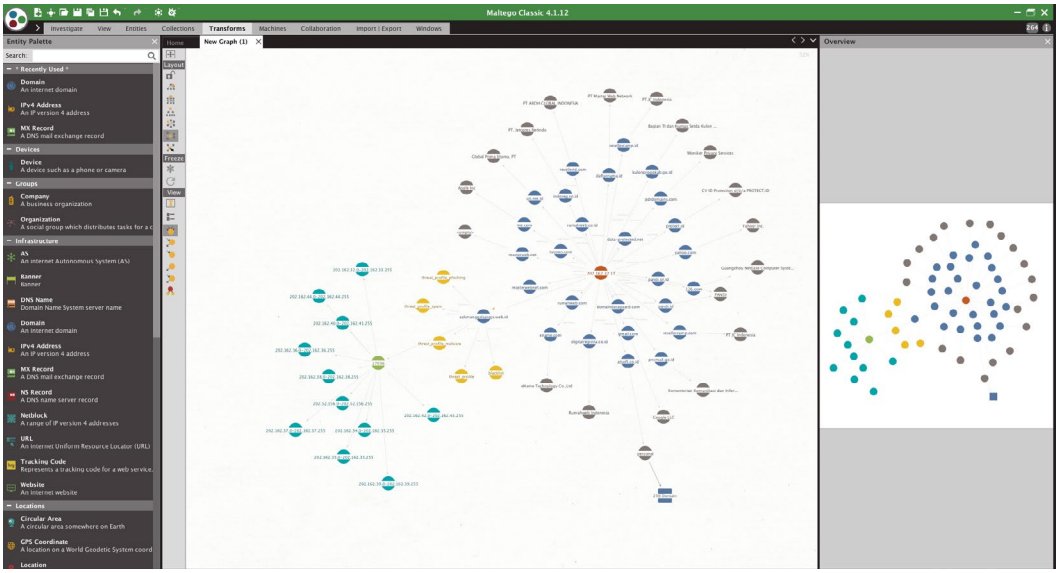
Streamlined Incident Response with Maltego

Empower Your Analysts with DomainTools Enrichment & Investigation Inside Maltego

DomainTools Iris Transforms for Maltego

Together, DomainTools and Maltego have simplified cyber investigations to provide actionable insights and expedite the investigation process. Extending the rich DNS, Whois, and beyond Whois datasets, DomainTools Iris integrates with Maltego to provide seamless workflows from the DomainTools Iris user interface directly to the Maltego graph.

The DomainTools solution for Maltego extends the rich domain name dataset and powerful pivot capabilities of DomainTools to the Maltego graph, enabling investigators and analysts to map connected infrastructure, run correlations, look at attribution, highlight risky domains, etc. to surfacing meaningful insights.



Investigators can transform a domain name from any source into a comprehensive set of entities, connections, and dynamic properties to reveal actors, surface infrastructure, and highlight risk. These new entities greatly increase the chance of intersection with existing graph data from other sources, and open up new investigative pathways.

Analysts can quickly identify which graph node to pivot on by consulting the Guided Pivot count present on nearly every entity these transforms act on. Counts appear in the properties section of any entity created by the DomainTools transforms. These counts indicate the number of domain records present in the Iris database that contain that same data point and can therefore be used to pivot and infer connection between one domain and another, assisting with mapping out a potential threat actor or group's TTPs (tactics, techniques, and procedures).

Besides the enrichment of domain entities, the transform set also offers over twenty different transforms that act on identities, infrastructure, tracking codes, and even SSL certificates. For example, a researcher may begin with an IP address and quickly discover other domains hosting a mail server or nameserver on that IP. Or, they may pivot from the SSL hash of a known-bad domain to uncover other sites using the same SSL certificate.

 | sales@domaintools.com | (206) 838-9020 | www.domaintools.com

DOMAINTOOLS

Domain Enrichment Transforms

These transforms operate on domain names and deliver Maltego entities or generic phrases that are ideally suited for follow-on enrichment with DomainTools transforms or those from other sources.

Domain to ASN	Domain to SOA Email Addresses
Domain to Contact Email Address	Domain to SSL Email Addresses
Domain to Google Adsense	Domain to SSL Hash
Domain to Google Analytics	Domain to SSL Org
Domain to IP Addresses	Domain to SSL Subjects
Domain to ISPs	Get Domain Contracts
Domain to MX Records	Get Domain Profile
Domain to NS Records	Get Risk Components
Domain to Organizations	Get Redirect Domain
Domain to Registrant	Get Email Domains
Domain to Registrar	

Investigate & Pivot Transforms

These transforms query the DomainTools Iris dataset and return domain names that share the same attributes as the value of the entity.

Google Adsense to Domain	NS Record to Domains (via IP Address)
Google Analytics to Domain	Organization to Domain (Registrant Org)
IP Address to Domain	Organization to Domain (SSL Org)
IP Address to Email Domains	Redirect Domain to Domain
IP Address to Nameserver Domains	Registrant to Domains
Iris Search Hash to Domain	Registrar to Domains
MX Record to Domains	SSL Hash to Domains
MX Record to Domains (via IP Address)	SSL Subject to Domains
NS Record to Domains	

Try it Out

If you would like to improve the ability to connect and pivot from DomainTools data to other Maltego datasets, please email **sales@domaintools.com** or call 206-838-9020.

