THREATQUOTIENT™

PATERVA
A new train of thought

MALTEGO TRANSFORMS FOR THREATQ™

Maltego Transforms for ThreatQ™ enables users of Maltego to query ThreatQ for information on elements that could be part of an investigation. These transforms extend the visibility of Maltego to include threat intelligence stored within ThreatQ, including commercial, industry, private, OSINT (open source intelligence) and internal sources, so you can visualize and discover additional data relationships.

Since ThreatQ is commonly deployed in private networks that are not directly accessible over the Internet, Maltego Transforms for ThreatQ are delivered as 'local transforms' that can be installed locally on systems running the Maltego client software. This ensures that connectivity between the client and the ThreatQ instance is direct and does not risk sending data to public transform servers.

INTEGRATION BENEFITS:

- Query information from all Threat Library sources quickly to find additional context to support an investigation
- Correlate internal and external threat data to accelerate online investigations
- Find relationships between threats, adversaries, indicators and incidents
- Easily perform link analysis and visualization

SYSTEM REQUIREMENTS

- ThreatQ version 3.4.3 or later
- ThreatQ SDK version 1.6.7 or later
- Maltego client support
  - Maltego Classic: Yes
  - Maltego XL: Yes
  - Maltego CE: Yes
- Local Operating System Support
  - Apple OS X: Yes, available now
  - Microsoft Windows: Yes, available now
  - Linux: Coming soon; contact for more information

WHAT IS MALTEGO?

Maltego (by Paterva) is an interactive data mining tool that renders directed graphs for link analysis. The tool is used in online investigations for finding relationships between pieces of information from various sources located on the Internet.

WHAT IS THREATQ?

ThreatQ is a threat intelligence platform (TIP) that enables users to build a custom Threat Library™ of adversaries, indicators, and threat data that is most relevant to an organization. The platform provides customer-specific controls to prioritize the library contents based on context and risk, as well as integrations with ecosystem partner solutions to act upon and learn from those actions. This helps security operations become more effective and efficient in both responding to events/alerts and anticipating future threats.

DATA TRANSFORMS PROVIDED (IN BOTH DIRECTIONS)

ThreatQ Object	Transforms to	ThreatQ Object
Adversary	<->	Related Adversaries Related Events Related Indicators Related Files Related Signatures Attributes
Event	<->	Related Adversaries Related Events Related Indicators Related Files Related Signatures Attributes
Indicator	<->	Related Adversaries Related Events Related Indicators Related Files Related Signatures Attributes
File	<->	Related Adversaries Related Events Related Indicators Related Files Related Signatures Attributes
Signature	<->	Related Adversaries Related Events Related Indicators Related Files Related Signatures Attributes
Attributes	<->	Related Adversaries Related Events Related Indicators Related Files Related Signatures

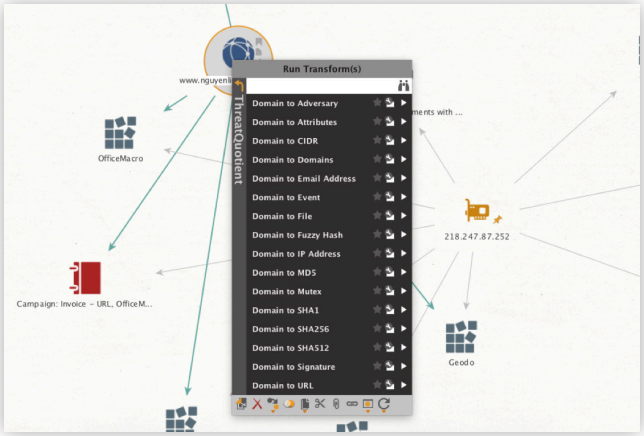

Figure 1: The ThreatQ transform list, which introduces related objects to the visualization.

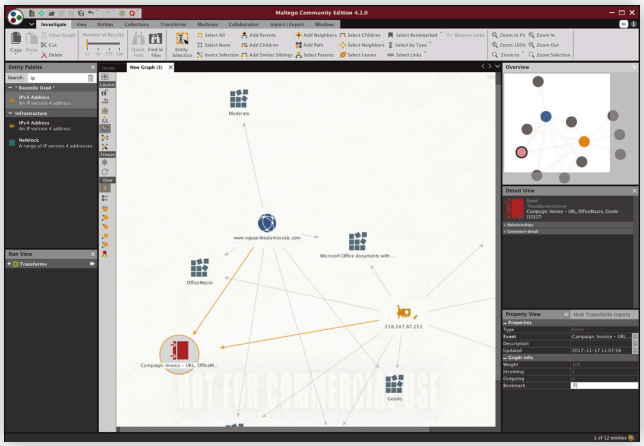

Figure 2: Maltego displaying ThreatQ data.

ABOUT THREATQUOTIENT™

ThreatQuotient understands that the foundation of intelligence-driven security is people. The company's open and extensible threat intelligence platform, ThreatQ™, empowers defenders to ensure the right threat intelligence is utilized within the right tools, at the right time. Leading global companies are using ThreatQ as the cornerstone of their threat intelligence operations and management system, increasing security effectiveness and efficiency.

For additional information, please visit threatq.com.

ABOUT PATERVA

Paterva designs, builds and supports "Maltego," a powerful suite of software tools used for data mining, link analysis and data visualization. In the modern digital age, these techniques are used to convert data into information and, thereby, extract concrete value from that data by identifying, analyzing and visualizing patterns within.

For more information, visit www.paterva.com.

THREATQUOTIENT™

11400 Commerce Park Drive, Suite 200, Reston, VA 20191 • ThreatQ.com
Sales@ThreatQ.com • Sales and General Inquiries: +1 703 574-9885