THREATQUOTIENT

DATA SHEET

MISP Solution Brief

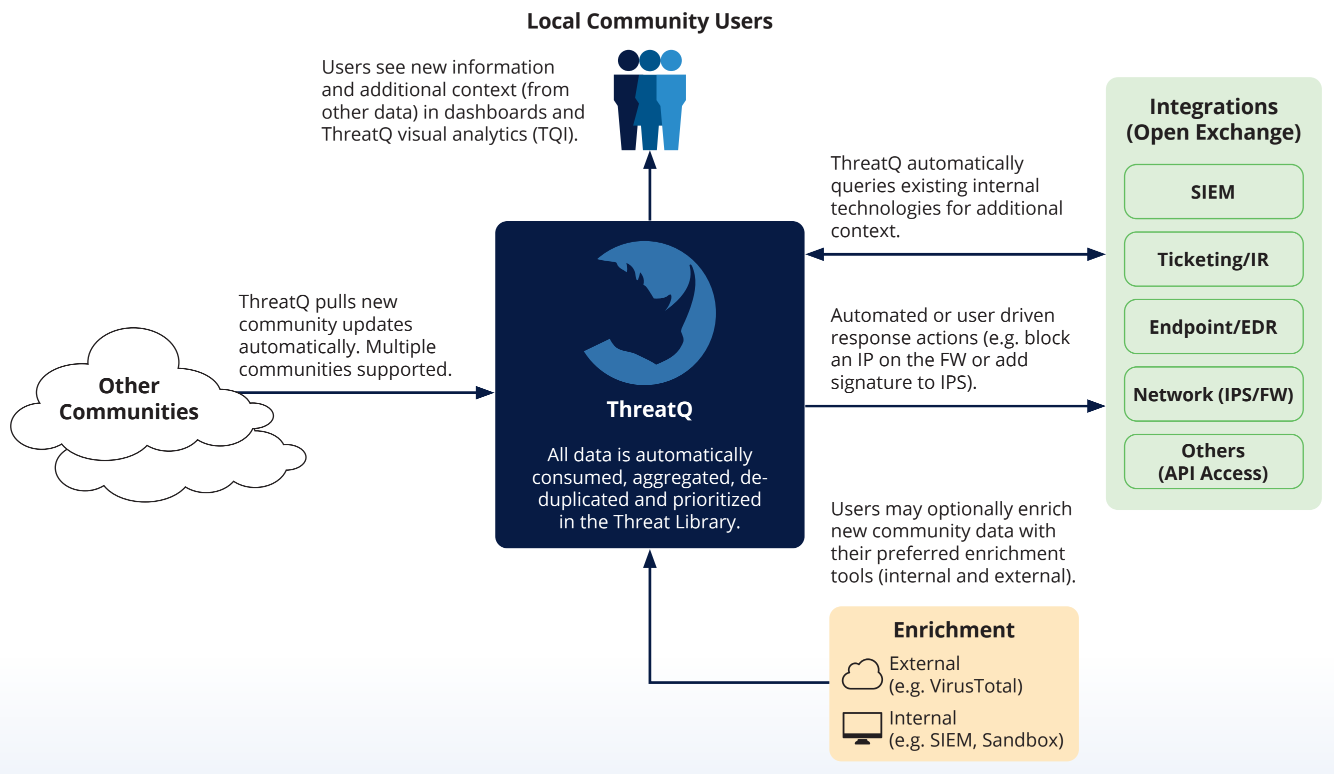
ThreatQ and MISP together allow our users to gain valuable information about emerging threats while correlating that information to additional sources. Utilizing our various MISP integrations, organizations are able to obtain threat intel from MISP, analyze that data and create investigations, as well as publishing that data back to MISP. Organizations are not only able to create their own MISP instance, but are also able to leverage existing MISP based communities as well.

HIGHLIGHTS

Importing Threat Intel from MISP

Using our MISP Import connector, organizations can pull MISP events into the ThreatQ platform. Indicators that are associated with these events will be related to any existing data within the Threat Library. The MISP Import connector will also incorporate any MITRE ATT&CK data that has been tagged against the source MISP event (e.g. adversaries, ATT&CK techniques, and malware information).

IMPORTING THREAT INTELLIGENCE FROM A MISP COMMUNITY



Users see new information and additional context (from other data) in dashboards and ThreatQ visual analytics (TQI).

ThreatQ automatically queries existing internal technologies for additional context.

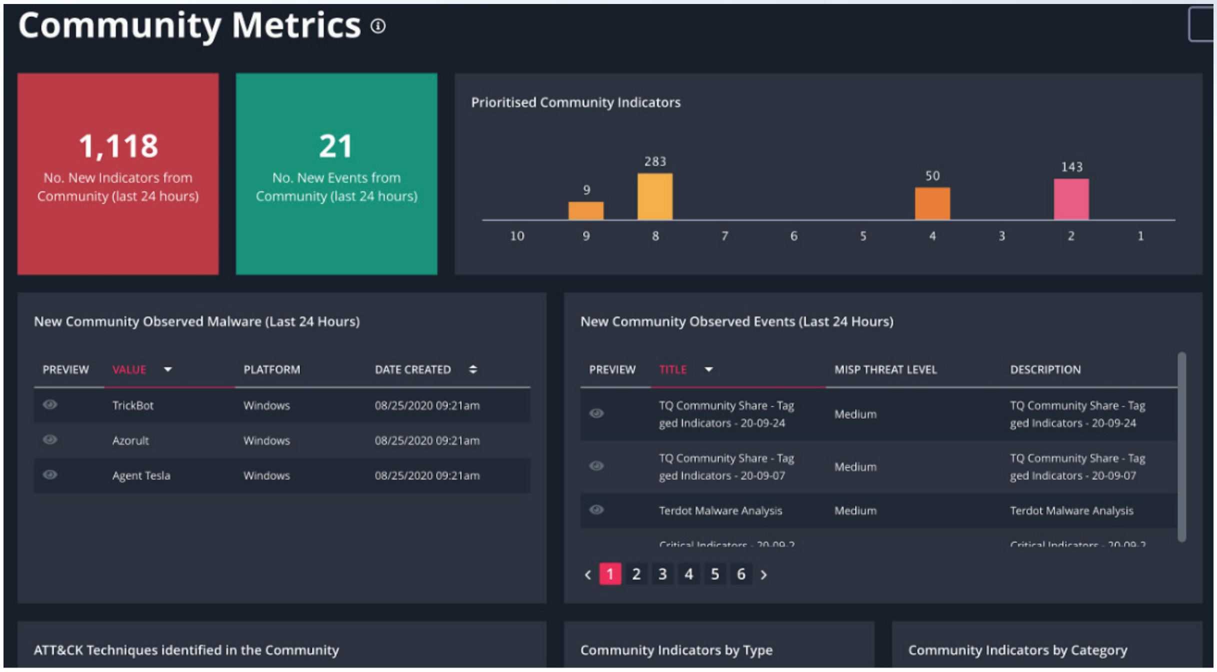
ThreatQ pulls new community updates automatically. Multiple communities supported.

Automated or user driven response actions (e.g. block an IP on the FW or add signature to IPS).

All data is automatically consumed, aggregated, de-duplicated and prioritized in the Threat Library.

Users may optionally enrich new community data with their preferred enrichment tools (internal and external).

ThreatQ dashboards offer users the option to visualize any data that has been imported from MISP using a single view. This may then be utilized for tracking and if necessary, investigation purposes. This is particularly useful when looking for high-level metrics or highlighting specific trends.



Community Metrics

1,118
No. New Indicators from Community (last 24 hours)

21
No. New Events from Community (last 24 hours)

Prioritised Community Indicators

New Community Observed Malware (Last 24 Hours)

PREVIEW	VALUE	PLATFORM	DATE CREATED
👁	TrickBot	Windows	08/25/2020 09:21am
👁	Azorult	Windows	08/25/2020 09:21am
👁	Agent Tesla	Windows	08/25/2020 09:21am

New Community Observed Events (Last 24 Hours)

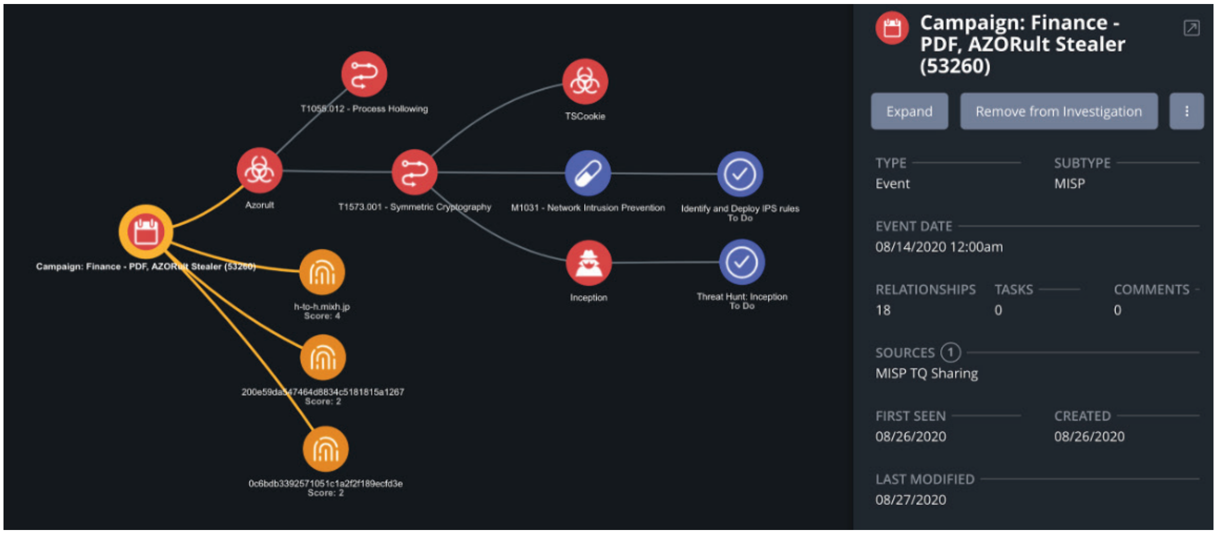
PREVIEW	TITLE	MISP THREAT LEVEL	DESCRIPTION
👁	TQ Community Share - Tagged Indicators - 20-09-24	Medium	TQ Community Share - Tagged Indicators - 20-09-24
👁	TQ Community Share - Tagged Indicators - 20-09-07	Medium	TQ Community Share - Tagged Indicators - 20-09-07
👁	Terdot Malware Analysis	Medium	Terdot Malware Analysis
	Critical Indicators - 20-09-2		Critical Indicators - 20-09-2

ATT&CK Techniques identified in the Community

Community Indicators by Type

Community Indicators by Category

ThreatQ Investigations may also be triggered from an ingested MISP event. Investigations support collaborative analysis and response in real-time. Investigations assist users such as threat hunters, incident responders, and intelligence analysts to leverage new community data quickly and identify its possible impact.



T1055.012 - Process Hollowing
TSCookie
Azorult
T1573.001 - Symmetric Cryptography
M1031 - Network Intrusion Prevention
Identify and Deploy IPS rules
To Do
Campaign: Finance - PDF, AZORult Stealer (53260)
h-to-h.mixh.jp
Score: 4
Inception
Threat Hunt: Inception
To Do
200e59da547464d8834c5181815a1267
Score: 2
0c6bdb3392571051c1a2f2f189ecfd3e
Score: 2
Expand
Remove from Investigation

Campaign: Finance - PDF, AZORult Stealer (53260)

TYPE
Event

SUBTYPE
MISP

EVENT DATE
08/14/2020 12:00am

RELATIONSHIPS
18

TASKS
0

COMMENTS
0

SOURCES (1)
MISP TQ Sharing

FIRST SEEN
08/26/2020

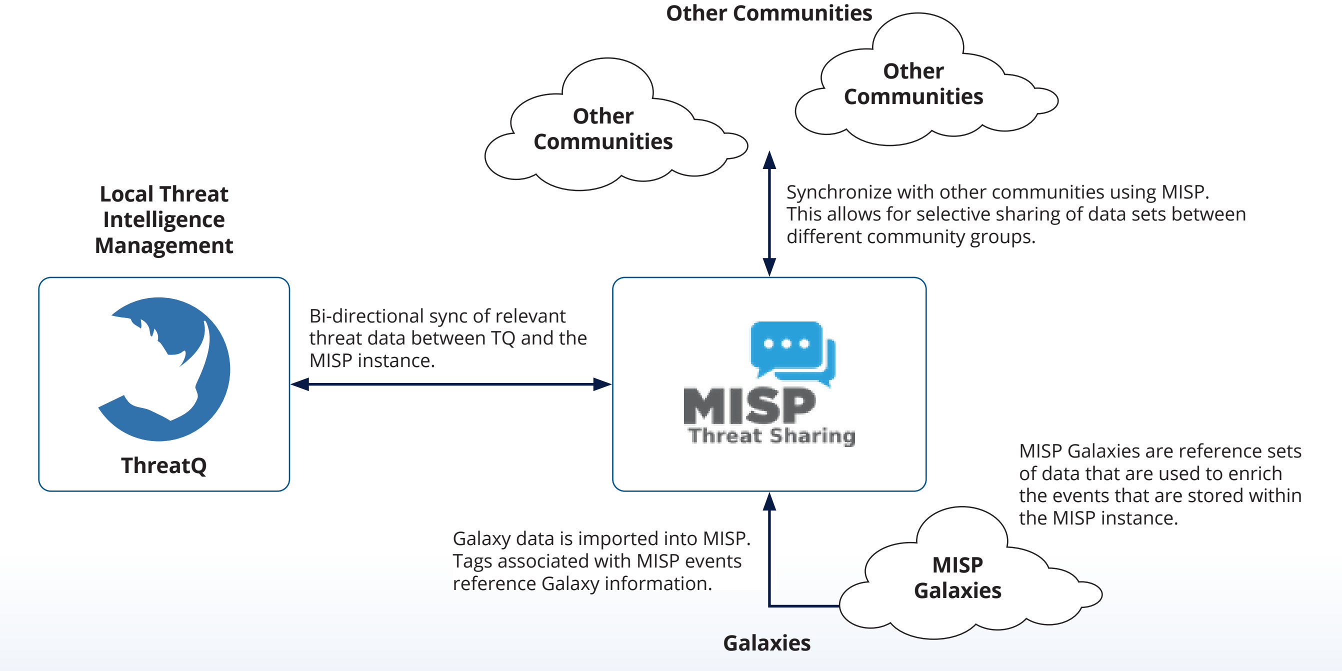
CREATED
08/26/2020

LAST MODIFIED
08/27/2020

Exporting Data from ThreatQ to MISP

ThreatQ ingests and prioritizes threat intelligence from sources that are external and internal and can assist with the identification of real threats to the business. Threats are identified and highlighted using the contextually rich data from the Threat Library, scoring, and ThreatQ Investigations. The MISP Export connector can automatically capture this important information and share it with the MISP community as a dedicated MISP Event. Any related data (such as adversaries, MITRE ATT&CK techniques, and malware) will be automatically associated with the MISP event in a format that can be utilized by MISP Galaxies (if used).

SENDING THREAT INTELLIGENCE TO A MISP COMMUNITY



Synchronize with other communities using MISP. This allows for selective sharing of data sets between different community groups.

Bi-directional sync of relevant threat data between TQ and the MISP instance.

MISP Galaxies are reference sets of data that are used to enrich the events that are stored within the MISP instance.

Galaxy data is imported into MISP. Tags associated with MISP events reference Galaxy information.

Intel Feeds

ThreatQ supports the direct ingestion of MISP Galaxy clusters as a source of enrichment for ThreatQ's Threat Library. The MISP Galaxy clusters that are supported include:

- Threat Actor
- Branded Vulnerabilities
- Ransomware
- Android malware
- RAT (Remote Access Tools)
- Banker (Banker malware)
- Countries
- Tools (used by Adversaries)

Along with the Galaxy intel data above, customers can leverage COVID-19 specific data to fight misinformation campaigns, medical information, and cyber threats related to or abusing COVID-19.

For more information visit the ThreatQ Marketplace

MISP Import | MISP Export | MISP Galaxies | MISP COVID-19

ThreatQuotient's mission is to improve the efficiency and effectiveness of security operations through a threat-centric platform. By integrating an organization's existing processes and technologies into a single security architecture, ThreatQuotient accelerates and simplifies investigations and collaboration within and across teams and tools. Through automation, prioritization and visualization, ThreatQuotient's solutions reduce noise and highlight top priority threats to provide greater focus and decision support for limited resources. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, APAC and MENA. For more information, visit **www.threatquotient.com**.