DATASHEET

Making Sense of Unstructured Data

The volume of unstructured intelligence data can overwhelm an analyst. Manually sorting through vast quantities of information is not only time consuming but can result in errors and omissions. The ability of ThreatQ to parse unstructured data through automation or assist on-demand in revealing the relevance of the data to your environment allows security professionals to prioritize the steps needed to secure the enterprise.

THREATQ BY THREATQUOTIENT™

ThreatQuotient's solutions make security operations more efficient and effective. The ThreatQ open and extensible platform integrates disparate security technologies into a single security infrastructure, automating actions and workflows so that tools and people can work in unison. Empowered with continuous prioritization based on their organization's unique risk profile, security teams can focus resources on the most relevant threats, and collaboratively investigate and respond with the aim of taking the right actions faster.

THREATQ ACE

ThreatQ ACE automatically identifies and extracts Threat Intelligence such as Indicators of Compromise (IOCs), malware, adversaries and tags from unstructured data, using Natural Language Processing (NLP) & keyword matching. Customers can use ThreatQ ACE to extract meaning and context from unstructured text in data feed sources and finished intelligence reports; as well as parse any reports, events or PDFs that are already in the ThreatQ Threat Library.

ThreatQ TDR Orchestrator's automation with the ACE workflow saves analysts time by removing the manual steps they spend today reading and extracting data from reports manually, freeing them to be more proactive when addressing the risk within their environment.

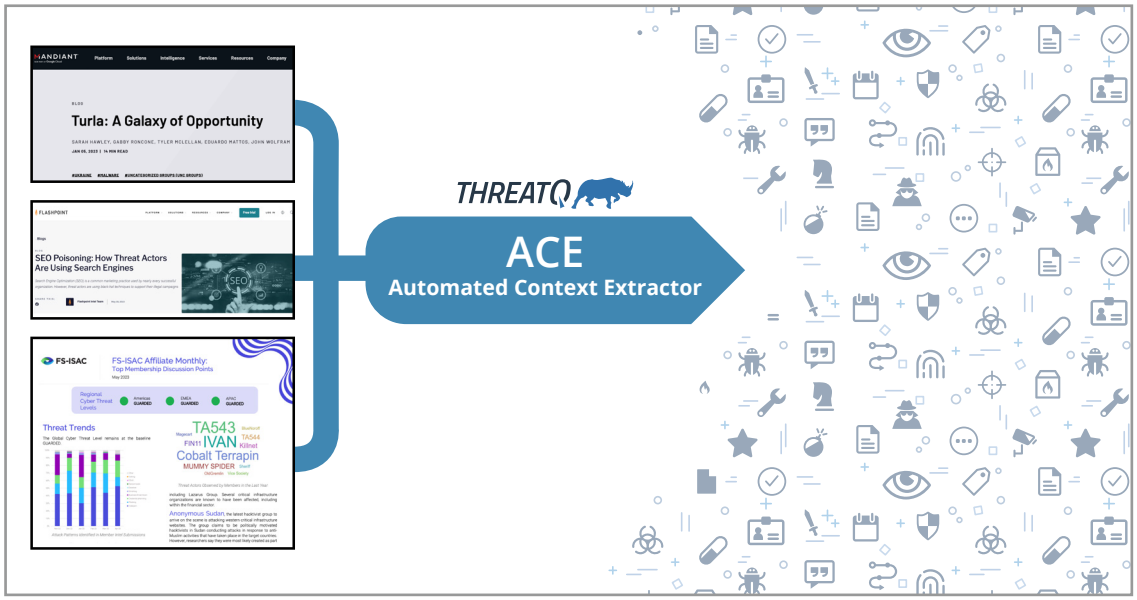
THREATQ KEYWORD TAGGER

The Report Keyword Tagger Workflow for ThreatQ TDR Orchestrator enables the automatic tagging of reports by a user-provided list of keywords. These keywords can either be applied as an attribute or a tag. This workflow facilitates the categorization of reports, based on the keywords that are valuable to your organization such as a specific product stack.

USE CASES:

- Data Ingestion - Reduce the time it takes to sort through mountains of data brought in automatically from intelligence feeds. Analysts will be presented with the context parsed from Open Source or commercial feeds. ThreatQ ACE removes the manual step that can be so time consuming.
- Internal Data - Analysts can leverage internal knowledge sources by automatically parsing the relevant context out of any PDF, CSV or TXT document that is uploaded into the ThreatQ Platform.
- Automated Workflows - Once the indicators have been parsed out from the unstructured source, customers can use the extracted indicators in an automated workflow to be enriched with the tools they already work with in their security stack.
- Curate the Data - Automatically parse and extract context from the data that is continually updated in the ThreatQ Threat Library. Always make sure that you have visibility into the most important IOCs by adding attributes, tags and relationship data to the existing and newly ingested data within your ThreatQ Threat Library.

The ACE and Keyword Tagger actions are available for use within ThreatQ for all users today at the ThreatQ Marketplace https://marketplace.threatq.com



ABOUT THREATQUOTIENT™

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection and response. ThreatQuotient's data-driven security operations platform helps teams prioritize, automate and collaborate on security incidents; enables more focused decision making; and maximizes limited resources by integrating existing processes and technologies into a unified workspace. The result is reduced noise, clear priority threats, and the ability to automate processes with high fidelity data. ThreatQuotient's industry leading data management, orchestration and automation capabilities support multiple use cases including incident response, threat hunting, spear phishing, alert triage and vulnerability prioritization, and can also serve as a threat intelligence platform. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, MENA and APAC. For more information, visit www.threatquotient.com.