**THREATQUOTIENT** 

**feedly**

# THREATQ™ AND FEEDLY
## Technology Segment: Enrichment and Analysis

## FEEDLY OVERVIEW

The Feedly integration ingests threat intel from articles, blog posts, social media, and RSS feeds aggregated in Feedly. Feedly has a layer of NLP processing that filters out noise and provides a lot of great context about the articles being ingested. The integration parses through this information and builds out reports containing attributes, tags and related objects such as IOCs, CVEs, and malware. It then relates the objects together so that everything is easily viewable in the threat library.

## THREATQ BY THREATQUOTIENT™

ThreatQuotient's solutions make security operations more efficient and effective. The ThreatQ data-driven security operations platform is both open and extensible, supporting the integration of 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.

## FEEDLY FOR THREAT INTELLIGENCE

Feedly for Threat Intelligence helps security teams stay one step ahead of increasingly active cyber adversaries.

The Feedly AI Engine speeds up the discovery and research of emerging threats.

It includes a set of machine learning models that automatically gather and analyze intelligence from millions of sources, in real-time.

The ThreatQ+Feedly integration allows you to push that intel and it rich context (IoCs, TTPs, CVEs, and malware) as reports to ThreatQ.

### INTEGRATION HIGHLIGHTS

Agregate intel from articles, blog posts, and social media.
___

Automate context tagging using the Feedly AI Engine.
___

Rich reports with IoCs, CVEs, malware tags and objects.
___

## INTEGRATION USE CASES:

The Integration supports a variety of use cases such as:

- Track emerging critical CVEs and zero-days

- Collect IoCs from blogs, articles, and threat intelligence reports

- Link IoCs to threat actors, malware, TTPs, and CVEs
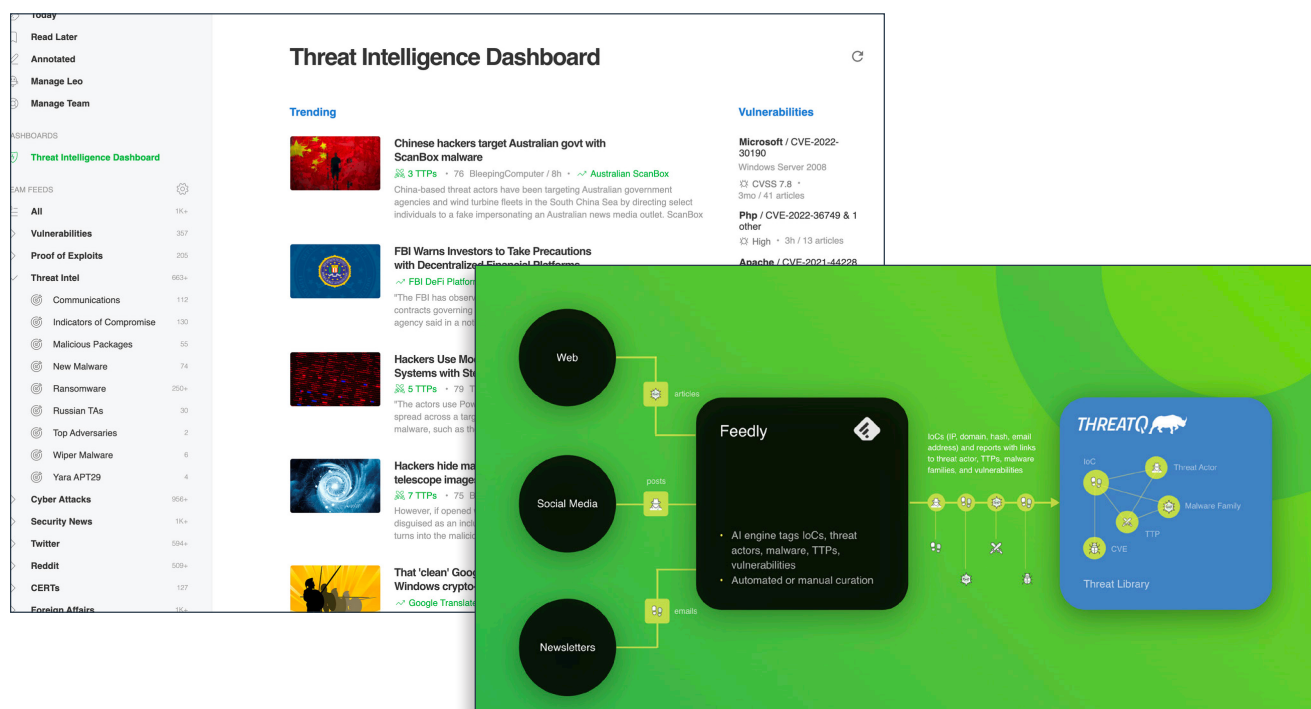


## ABOUT THREATQUOTIENT™

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, vulnerability prioritization and threat intelligence management. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe and APAC.
For more information, visit www.threatquotient.com.

## ABOUT FEEDLY

Feedly offers a set of machine learning models that help cybersecurity team automate the aggregation, analysis, and sharing of threat insights scatered across the Web.

Feedly is headquartered in California with international operations based out of Europe and APAC.

For more information, visit feedly.com/ai-threat-intelligence