THREATQUOTIENT™

zvelo

THREATQ™ AND ZVELO

Technology Segment: Intel Feeds

Get the actionable threat intelligence required to block adversaries for comprehensive protection against phishing and malicious IOCs. zveloCTI is intended for defenders, threat analysts, and SaaS security vendors seeking to integrate premium cyber threat intelligence data into their solutions or services.

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.

ZVELOCTI CURATED THREAT INTELLIGENCE FEEDS

zvelo CTI™ delivers Actionable Threat Intelligence via curated phishing and malicious datasets intended for Cybersecurity and Threat Intelligence teams to use for enrichment and analytics.

PhishBlocklist (PBL) supplies curated phishing cyber threat intelligence for comprehensive protection against active phishing threats in the wild. PBL provides detections and rich metadata attributes like date detected, targeted brand, and other crucial data points. Available as a data feed as standard, as well as an optional traffic submission & processing capability.

Malicious Detailed Detection Feed (MDDF) delivers curated malicious cyber threat intelligence data which identifies, confirms, and enriches malicious IoCs with a range of metadata attributes such as date detected, malware family, and many key intelligence attributes which can be used for further analysis and enrichment.

INTEGRATION HIGHLIGHTS

Eliminate blind spots in coverage by detecting threats other feeds miss

Reduce false positives to accelerate security outcomes

Enrich and automate SASE, SIEM, SOAR, and other security tools

Manage costs by streamlining threat sources with zvelo's multi-sourced, curated cyber threat intelligence

Focus on threat prioritization and mitigation tasks instead of data collection and curation

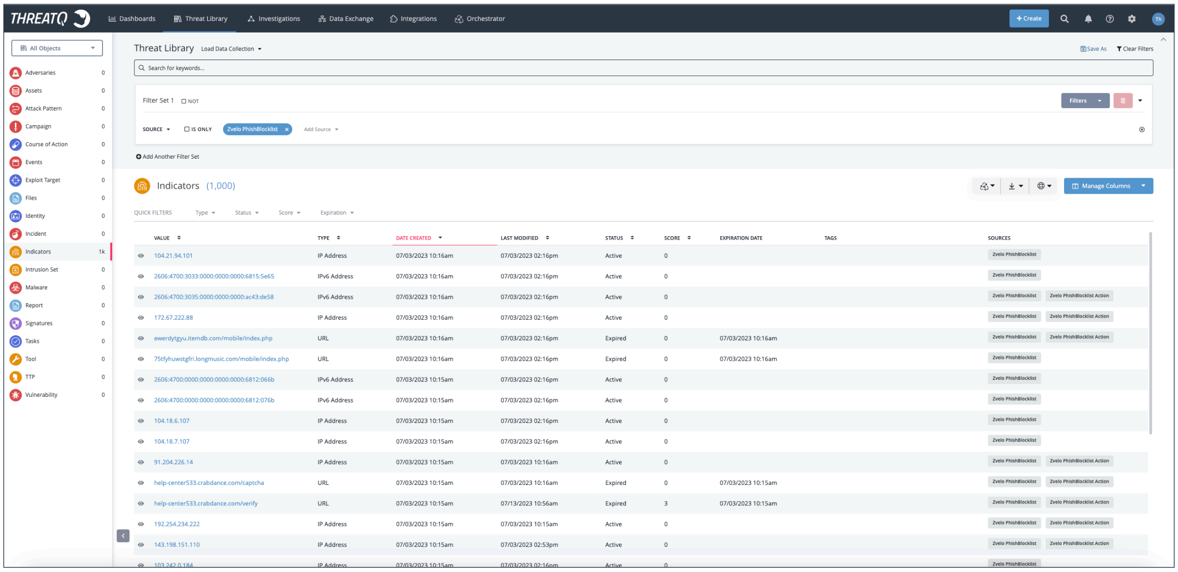
Leverage zvelo's 24/7 staffing of malware analysts to respond to customer requests within minutes

The primary use case for zveloCTI threat data via the ThreatQ platform is for threat detection and response, allowing clients to block active and emerging threats with the highest degree of accuracy before those threats can cause damage.

INTEGRATION USE CASES:

Additional use cases for zvelo solutions include:

- DNS Filtering to block high risk or potentially dangerous connections to phishing or malicious domains.
- SWG & CASB to secure native cloud environments and protect users, endpoints & networks.
- Endpoint Security to stop threats from compromising endpoints and IoT devices.
- RBI & Secure Browser to enable safe browsing for users.
- Email & SMS Security to block end users from accessing phishing or malicious links in emails and text messages.
- Supplement Threat Research with zvelo's high veracity, actionable threat data for greater enrichment and analysis.



Threat Library Load Data Collection

Search for keywords...

Filter Set 1 □ NOT

SOURCE □ IS ONLY Zvelo PhishBlocklist Add Source

Indicators (1,000)

VALUE	TYPE	DATE CREATED	LAST MODIFIED	STATUS	SCORE	EXPIRATION DATE	TAGS	SOURCES
104.21.94.101	IP Address	07/03/2023 10:16am	07/03/2023 02:16pm	Active	0			Zvelo PhishBlocklist
2606:4700:3033:0000:0000:0000:6815:5e65	IPv6 Address	07/03/2023 10:16am	07/03/2023 02:16pm	Active	0			Zvelo PhishBlocklist
2606:4700:3035:0000:0000:0000:ac43:de58	IPv6 Address	07/03/2023 10:16am	07/03/2023 02:16pm	Active	0			Zvelo PhishBlocklist Zvelo PhishBlocklist Action
172.67.222.88	IP Address	07/03/2023 10:16am	07/03/2023 02:16pm	Active	0			Zvelo PhishBlocklist Zvelo PhishBlocklist Action
ewerdytgyu.itemdb.com/mobile/index.php	URL	07/03/2023 10:16am	07/03/2023 02:16pm	Expired	0	07/03/2023 10:16am		Zvelo PhishBlocklist Zvelo PhishBlocklist Action
75tfyhuwstgfri.longmusic.com/mobile/index.php	URL	07/03/2023 10:16am	07/03/2023 02:16pm	Expired	0	07/03/2023 10:16am		Zvelo PhishBlocklist
2606:4700:0000:0000:0000:0000:6812:066b	IPv6 Address	07/03/2023 10:15am	07/03/2023 02:16pm	Active	0			Zvelo PhishBlocklist
2606:4700:0000:0000:0000:0000:6812:076b	IPv6 Address	07/03/2023 10:15am	07/03/2023 02:16pm	Active	0			Zvelo PhishBlocklist
104.18.6.107	IP Address	07/03/2023 10:15am	07/03/2023 02:16pm	Active	0			Zvelo PhishBlocklist
104.18.7.107	IP Address	07/03/2023 10:15am	07/03/2023 02:16pm	Active	0			Zvelo PhishBlocklist
91.204.226.14	IP Address	07/03/2023 10:15am	07/03/2023 10:16am	Active	0			Zvelo PhishBlocklist Zvelo PhishBlocklist Action
help-center533.crabdance.com/captcha	URL	07/03/2023 10:15am	07/03/2023 10:16am	Expired	0	07/03/2023 10:15am		Zvelo PhishBlocklist Zvelo PhishBlocklist Action
help-center533.crabdance.com/verify	URL	07/03/2023 10:15am	07/13/2023 10:56am	Expired	3	07/03/2023 10:15am		Zvelo PhishBlocklist Zvelo PhishBlocklist Action
192.254.234.222	IP Address	07/03/2023 10:15am	07/03/2023 10:15am	Active	0			Zvelo PhishBlocklist Zvelo PhishBlocklist Action
143.198.151.110	IP Address	07/03/2023 10:15am	07/03/2023 02:53pm	Active	0			Zvelo PhishBlocklist Zvelo PhishBlocklist Action
103.242.0.184	IP Address	07/03/2023 10:15am	07/03/2023 02:16pm	Active	0			Zvelo PhishBlocklist

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 ZVELO

zvelo provides industry-leading cyber threat intelligence and URL classification data services. zvelo's proprietary AI-based threat detection and categorization technologies, combines curated domains, threat and other data feeds, with the clickstream traffic from its global partner network of 1 billion users and endpoints to provide unmatched visibility, coverage, reach and accuracy. zvelo powers applications and solutions for the world's leading providers of web filtering, endpoint detection and response (EDR), extended detection and response (XDR), Secure Access Service Edge (SASE), brand safety and contextual targeting, cyber threat intelligence platforms, threat analysis, and more.

For more information, visit www.zvelo.com.