

zveloCTI™

Meticulously Curated Data for Actionable Cyber Threat Intelligence

zveloCTI DELIVERS ACTIONABLE THREAT INTELLIGENCE ON PHISHING AND MALICIOUS IOCS WITH INDUSTRY-BEST DETECTION COVERAGE, SPEED, AND SAVINGS.

zveloCTI™ delivers a superior quality cyber threat intelligence feed with 30% better detection coverage, greater accuracy, and faster threat detections with an average cost savings of 70%.

- Eliminate blind spots by detecting threats other feeds miss with unrivaled global coverage.
- Accelerate security outcomes with richly contextualized IOCs and malicious threat signals.
- Enrich and automate SASE, SIEM, SOAR, and other security tools, to boost ROI from existing infrastructure.
- Streamline 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.
- Optionally, use zvelo's threat detection processing and threat hunting capabilities to get forward-looking threat intel and security guidance.

zveloCTI | CURATED DATA FEEDS PLUS METADATA

zvelo's proprietary AI-based threat detection and categorization technologies, combined with curated domains, threat and other data feeds, plus ActiveWeb traffic from its partners' 1 billion users and endpoints, provide unmatched visibility, coverage, reach and accuracy for powering applications which protect users and devices from malicious threats.



PHISHBLOCKLIST

zvelo's AI-powered Phishing Intelligence detects phishing threats within the ActiveWeb traffic and other sensor-based data streams to deliver a richly packaged feed of highly curated and validated phishing threats that are enriched with additional metadata attributes like date detected, targeted brand, and other crucial data points.

zveloCTI™ AT A GLANCE

- 30% Better Detection Coverage
- Less Than 0.1% False Positives
- 70%+ Cost Savings vs In-house Threat Intel
- Unique Detections of Malicious & Phishing Exploits
- Metadata Attributes for Contextual Relevance
- Real-Time, Continuous Updates
- 99.9%+ ActiveWeb Coverage — 1 Billion Users & Endpoints
- Curated 3rd Party Feeds + zvelo Proprietary Data
- Fast, Easy Deployment

METADATA ATTRIBUTES

- Date Detected
- Active/Offline Status
- Targeted Brand
- Threat Type
- Threat Family
- File Hashes
- Full-Path URL
- Confidence Score
- And Other Intelligence Attributes

zvelo



MALICIOUS DETAILED DETECTION FEED

zveloCTI's Malicious Detailed Detection Feed delivers curated malicious cyber threat intelligence data which identifies, confirms, and enriches malicious IOCs with a range of metadata attributes such as date detected, threat type, threat family, file, OS/subsystem targeted and many key intelligence attributes which can be used for further analysis and enrichment.

THE VALUE OF ZVELO CURATION

In addition to the typical aggregation of third party threat feeds, zvelo processes the ActiveWeb traffic from tens of millions of users and machines around the world. This visibility into the massive volumes of ActiveWeb traffic gives zvelo a clear advantage when it comes to identifying more unique phishing and malicious threats with a greater degree of accuracy than any other vendor. zvelo's in-house capabilities include a 3-tier team of dozens of data analysts and threat hunters who work 24x7 performing curation, investigation, and threat hunting activities related to suspicious activity or potential threats that get flagged for human review by our advanced AI/Deep-Learning models. The net result is a superior quality cyber threat feed with faster detections and lower false positives, plus 24x7 customer support.

CTI PROCESS FEEDBACK LOOP

zvelo collects billions of data points across the web and combines those with feedback from partners, and multiple proprietary data sources. The raw data is segmented by Topic-Based Content, Malicious, Phishing, and Suspicious Domain Intelligence where it undergoes an extensive validation process to produce highly curated data for deeper analysis using AI and Human Supervised Machine Learning. The end result is richly packaged Threat Intelligence data ready for dissemination in the desired schema, format, and timeline.

01 | INDUSTRY EXPERTISE

Internal experts collaborate with external sources for global cybersecurity strategies.

06 | FEEDBACK

Continuous feedback loop for real-time, dynamic updates of the ActiveWeb.

05 | FLEXIBLE DEPLOYMENT*

- API
- SDK
- Data Feeds

* **Note:** Deployment options vary by feed or URL classification solution.

02 | 99.9% ACTIVEWEB COVERAGE

- Traffic from 1 billion users & endpoints
- Third party data sources
- zvelo proprietary data

03 | DATA CURATION

- Extensive verification
- High accuracy
- Low false positive rate

04 | 99.9%+ ACCURACY

AI and Human Supervised Machine Learning assures maximum accuracy for web content classifications.



ABOUT ZVELO

zvelo's passion is to make the internet safer and more secure by providing the industry's premium Cyber Threat Intelligence and web classification data services.

LEARN MORE

To learn more about zveloCTI or to request an evaluation, please contact us at sales@zvelo.com or visit www.zvelo.com.

LEARN MORE

z v e l o