MAKING THE INTERNET SAFER AND MORE SECURE

zveloCTI™

Meticulously Curated Data for Actionable Cyber Threat Intelligence

zveloCTI™

zveloCTI provides curated, high veracity, actionable data on phishing, malicious and suspicious new domains that Threat Intelligence Teams can ingest for analysis and enrichment.

When you need more than just malicious and phishing detections, zveloCTI curated feeds deliver the rich metadata and insights necessary for actionable Threat Intelligence. zvelo combines proprietary AI-based threat detection and categorization technologies with curated domains, threat and other data feeds, plus the clickstream traffic from its global partner network representing 600+ million users, to provide unmatched visibility, coverage, reach and accuracy.

zveloCTI | CURATED DATA FEEDS PLUS METADATA

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.

MALICIOUS DETAILED DETECTION FEED

zvelo's Malicious Intelligence identifies, confirms, and enriches malicious URLs for direct action by defenders and analysts. The data feed includes specific malicious URLs, as well as a range of metadata attributes such as date detected, malware family, and other significant intelligence data attributes.

SUSPICIOUS NEW REGISTRATIONS FEED

zvelo's Suspicious New Domain Intelligence combs the ProActiveWeb for new domain registrations and other signals which help identify potential threats early on — ***before*** they hit the ActiveWeb. This feed includes newly registered domains that are identified as being suspicious, along with comprehensive data attributes including DGA score, date registered, expiration date, ASN info, registrar info, active/offline, URL, and other key details.

zveloCTI™ AT A GLANCE

- Unique Detections of Malicious & Phishing Exploits
- Metadata Attributes for Context of Identified Threats
- Real-Time, Continuous Updates
- Massive Clickstream Traffic From 600+ Million Users and Endpoints
- Curated 3rd Party Feeds + zvelo Proprietary Data
- High Veracity and Low False Positives
- Flexible Deployment with Multiple Formats Available

METADATA ATTRIBUTES

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

zvelo

CTI PROCESS FEEDBACK LOOP

ACTIONABLE INTELLIGENCE

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.

02 | 99.9% ACTIVEWEB COVERAGE

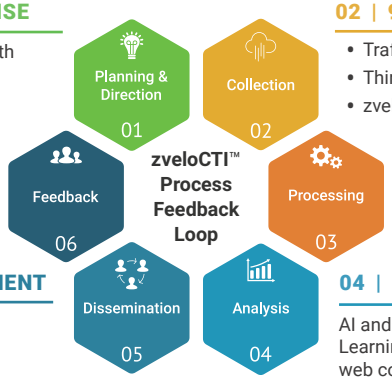
- Traffic from 600+ million end users
- Third party data sources
- zvelo proprietary data

06 | FEEDBACK

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

03 | DATA CURATION

- Extensive verification
- High accuracy
- Low false positive rate



05 | FLEXIBLE DEPLOYMENT

- API
- SDK
- Data Feeds (STIX, MISP)

04 | 99.9%+ ACCURACY

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

zvelo's VIEW OF THE WEB

ACTIVEWEB

The ActiveWeb is how zvelo refers to the publicly-accessible and indexable Surface Web. zvelo classifies these sites into topic-based content, malware, phishing, objectionable, and sensitive content categories. The 600+ million users represented by zvelo's partners provide a continuous stream of new ActiveWeb domains for classification, resulting in zvelo having over 99.9% coverage of the ActiveWeb on an ongoing basis.

PROACTIVEWEB

The ProActiveWeb is a precursor to sites becoming part of the ActiveWeb. zveloCTI monitors and analyzes signals from the ProActiveWeb, like TLD registrations and a range of other indicators, to produce predictive Threat Intelligence insights. These predictive insights are crucial to detecting threats ***before*** they become part of the ActiveWeb, arming zvelo's partners with highly unique threat intelligence data to sharpen their competitive edge.

INACTIVEWEB

The InActiveWeb is made up of all the websites which have expired or have an unreachable status — including legitimate sites that are no longer being used, as well as malicious or phishing sites that were flagged and taken down. While the InActiveWeb is rather innocuous and doesn't host active threats, it does harbor suspicious activity as this is where the Malicious Cyber Actors (MCAs) carve a path into the ActiveWeb. zvelo continues to track domains after they have moved from the ActiveWeb to the InActiveWeb, in case they become active again.

THREAT INTELLIGENCE REPORTING

zvelo delivers meticulously curated, actionable Threat Intelligence data with industry leading accuracy and low false positive rates for maximum precision, efficacy and protection against evolving and emerging threats.

- Malicious Intelligence Reporting
- Phishing Intelligence Reporting
- Suspicious New Domain Intelligence Reporting
- Brand Threat Intelligence Reporting
- Exposed/Exploited Assets Reporting
- Domain Squat Reporting
- Additional Intelligence Reporting Available

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

zvelo