MAKING THE INTERNET SAFER AND MORE SECURE

zveloCTI™

Malicious Detailed Detection Feed™

Real-Time Malicious Threat Detection with Enriched Intelligence Data

IDENTIFY, CONFIRM, AND ENRICH INTELLIGENCE ON MALICIOUS URLS AND FILES WITH ZVELO'S MALICIOUS DETAILED DETECTION FEED™.

Part of the zveloCTI™ family of Cyber Threat Intelligence feeds, the Malicious Detailed Detection Feed™ (MDDF) delivers curated malicious intelligence data which identifies, confirms, and enriches malicious URLs with a range of metadata attributes pertaining to both the malicious URLs as well as malicious files associated with those URLs. The rich metadata reveals Indicators Of Compromise (IOC) which can be used for further analysis and enrichment.

MDDF is segmented into two components based on the type of metadata included — malicious URL metadata and malicious file metadata. You may opt to have the feed include metadata from either segment, or both. Below are examples of some of the metadata fields which may be found.

MALICIOUS URL METADATA

- Creation Date
- Expiration Date
- Age
- Domain History

MALICIOUS FILE METADATA

- File Hashes
- Malware Family
- Packing/Encoding
- Verdict Score

zvelo's proprietary AI-based threat detection and categorization technologies, combined with curated domains, threat and other data feeds, plus clickstream traffic from its partners' 600+ million users, provide unmatched visibility, coverage, reach and accuracy for powering applications which protect users and devices from malicious threats.

Unmatched Quality and Veracity

UNIQUE MALICIOUS URL DETECTIONS

Advanced AI-based, proprietary technology detects unique malicious URLs earlier and more accurately than other providers, to neutralize emerging threats when they are most dangerous.

MASSIVE CLICKSTREAM TRAFFIC

URLs from text, SMS, email, and surfing traffic of more than 600 million users supplies continuous and comprehensive visibility into the global clickstream.

MDDF™ AT A GLANCE

- Unique Malicious URL Detections
- Metadata Attributes for Context of Identified Threats
- Observe Malicious Trends Over Time
- 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
- Part of zveloCTI's Family of Cyber Threat Intelligence Feeds

METADATA ATTRIBUTES

- Full-Path URL
- Date Created and/or Expired
- Domain History
- Malware Family
- File Hashes
- Numerous Other Intelligence Attributes

zvelo

METADATA ATTRIBUTES FOR THREAT CONTEXT

Rich metadata accompanies full-path malicious URLs, plus the associated malicious files, so you can communicate the context of malicious threats like created date, domain history, malware family, and file hashes.

REAL-TIME MALICIOUS DETECTION

Newly identified malicious threats immediately propagate to global database deployments to maximize protection against emerging threats.

CURATED MALICIOUS INTELLIGENCE

The Malicious Detailed Detection Feed leverages massive clickstream traffic, along with other sensor-based data streams and proprietary data sources to identify, validate and enrich intelligence collected on malicious threats.

REAL-TIME, CONTINUOUS UPDATES

zvelo's global AI-based network continuously monitors and analyzes ActiveWeb traffic and proprietary data sources to identify new malicious threats as they mutate and change.

Extend Your Threat Protection with zveloCTI™

The Malicious Detailed Detection Feed is one of several Cyber Threat Intelligence feeds in the zveloCTI product family, and is uniquely positioned to identify, confirm, and enrich the intelligence collected on malicious URLs for direct action by defenders and analysts. For comprehensive protection against a broader range of other threats and exploits, zveloCTI offers additional Threat Intelligence feeds for further enrichment and analysis.

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.

SUSPICIOUS NEW REGISTRATIONS FEED™

Identify Indicators Of Compromise (IOC) and potential threats before they can impact victims. zvelo's Suspicious New Registrations Feed enriches new domain registration data with highly valuable metadata like DGA score, registration and/or expiration dates, ASN info, and more.

USE CASES

- Web Filtering & Parental Controls
- DNS Filtering & DNS RPZ
- Malicious Threat Analysis
- Malicious Intelligence Reporting
- Antivirus Software
- Next-Generation Firewalls
- Endpoint Security
- Enterprise Network Administration
- Ideal for ISPs, Telcos, CASBs, MSSPs, SIEM, IPS, UTM Vendors, and Many Others

zveloCTI™

Curated Threat Intelligence data that is unmatched in visibility, coverage, reach, and accuracy.

- PhishBlockList™
- Malicious Detailed Detection Feed™
- Suspicious New Registrations Feed™

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 MDDF or to request an evaluation, please contact us at **sales@zvelo.com** or visit **www.zvelo.com**.

LEARN MORE

zvelo