Product Sheet

First Watch Malicious Domains Data Feed

Why Businesses Choose First Watch Malicious Domains Data Feed?

Predictive threat intelligence is the only way to identify and block soon-to-become malicious domains at registration.

Key Industry Challenges

- Traditional threat feeds are reactive and identify harmful domains only after attacks have occurred, leaving organizations vulnerable during the initial stages.
- Many threat feeds provide incomplete visibility into attack infrastructures, creating blind spots that increase an organization's exposure to emerging threats.
- High false positive rates in traditional threat feeds burden SOCs with excessive noise, leading to alert fatigue and reduced operational efficiency.

First Watch Malicious Domains
Data Feed

So Why FWMD Data Feed?

- Proactively detects phishing, malware, and C2 domains soon after registration, before activation.
- Provides full visibility to eliminate attack infrastructure blind spots.
- Boosts SOC efficiency by drastically cutting false positives and alert fatigue.
- Minimizes the risk of overblocking legitimate services.

FWMD Data Feed Key Benefits

Neutralize threats at registration to stay one step ahead of attackers and prevent potential breaches.

TRADITIONAL SOLUTIONS	FIRST WATCH
✗ Reactive detection after attacks begin	✓ **Proactive identification at domain registration**
✗ High false positive rates	✓ **97% precision with near-zero false positives**
✗ Usage-based pricing that scales with threats	✓ **Predictable flat-rate pricing**
✗ Generic threat feeds	✓ **White-label capability for MSSPs**

BENEFITS

- **Near-zero MTTD** – Catch threats before they become active.
- **No alert fatigue** – High-precision AI filters out noise from traditional feeds.
- **No surprises** – Predictable, flat-rate pricing ensures security budgets remain stable.
- **Instant deployment** – One-day integration, seamless fit into existing product data lake.

97%
Precision in detecting malicious domains at registration

< 3%
False positive rate guarantee

12x
More attack infrastructure detected

3 months
Faster detection

FWMD Data Feed Details

DATA POINT	DESCRIPTION
Domain name	Associated domain name
Reason	Domain has just been added or discovered
Relevant dates	Creation, expiration, update, and audit dates applicable to the domain
Name and WHOIS servers	Name and WHOIS server/s hosting the domain
Registrar information	Name and ID of the domain registrar
Registrant information	Name, address, email, and contact details of the entity that registered the domain
Domain status	Status of the domain assigned by its registrar or registry
Administrative, billing, and technical contact details	Name, address, and contact details of the person in charge of the domain's billing, technical, and administrative aspects

UPDATE TIME & DELIVERY FORMAT

- The daily update is ready for download at 12:00 UTC.
- **Delivery format:** CSV

DOWNLOADING FILES

- Downloading via HTTPS
- Downloading via FTP
- Downloading via FTPS

DATA INTEGRATION

- Importing and indexing First Watch Malicious Domains Data Feed into MySQL

FWMD Data Feed Plans & Features

Starter

Coverage: newly registered domains without WHOIS records. No historical data.

Delivery format: CSV

--

Starter features:

- Predictive Domain Classification
- Recursive Deep Learning Neural Network
- Download Access
- Past 24 Hours

Pro

Coverage: newly registered domains with WHOIS records and 365 days of historical data.

Delivery format: CSV

--

Everything in Starter, plus:

- Infrastructure Details
- Past 365 Days
- Private Threat Intel Workshop Access

Enterprise

Coverage: newly registered domains with WHOIS records and all available historical data.

Delivery format: CSV

--

Everything in Pro, plus:

- Unlimited deployments
- Enterprise SLA & Support Tea
- False-Positive Guarantee

FWMD Data CSV File Preview

FWMD data feed offers three types of subscription plans which have different data features.

The presented Enterprise sample provides access to the newly registered domains with WHOIS records and all available historical data.

It includes the following output fields:

- reason
- domainName
- registrarName
- registrarIANAID
- whoisServer
- nameServers
- createdDateRaw
- updatedDateRaw
- expiresDateRaw
- createdDateParsed
- updatedDateParsed
- expiresDateParsed
- status
- registryDataRawText
- whoisRecordRawText
- auditUpdatedDate
- contactEmail
- registrant_rawText
- registrant_email
- registrant_name
- registrant_organization
- registrant_street1
- registrant_street2
- registrant_street3
- registrant_street4
- registrant_city
- registrant_state
- registrant_postalCode
- registrant_country
- registrant_fax
- registrant_faxExt
- registrant_telephone
- registrant_telephoneExt
- administrativeContact
- technicalContact
- billingContact
- zoneContact

reason	domainName	registrarName	registrarIANAID	whoisServer	nameServers	createdDateRaw	updatedDateRaw	expiresDateRaw
discovered	ankaraefeturizm	Atak Domain	1601	whois.apiname.c	ns31.guzelhostir	2024-10-17T15:4	2024-10-17T15:4	2025-10-17T15:4
discovered	endometriosiskli	Atak Domain	1601	whois.apiname.c	ns1.guzelhosting	2024-10-18T14:3	2024-10-18T14:3	2025-10-18T14:3
added	raweat-sama-diyala.iq		0		ns1417.websitewelcome.com|ns1418.websitewelcome.com			
added	payas.com.mx	Key-Systems Gr	269	whois.mx	ns-cloud-b1.goo	2024-10-28	2024-10-28	2025-10-28
added	iwx2618.cn	阿里云计算有限公	0	whois.cnnic.net.c	aron.ns.cloudfla	2024-10-27 15:4		2025-10-27 15:4
added	casacosnorthfac	GMO INTERNET	49	whois.discount-c	shaz.ns.cloudfla	2024-10-29T01:3	2024-10-29T01:3	2025-10-29T01:3
added	dany-pool-servic	Squarespace Do	3827	whois.squarespa	ns-cloud-d2.goo	2024-10-29T00:0	2024-10-29T00:0	2025-10-29T00:0
added	access-ing-aktualisierung.de		0	whois.denic.de	brit.ns.cloudflare.com|eugene.ns.c	2024-10-29T02:11:38+01:00		
added	theworshipleade	GoDaddy.com, L	146	whois.godaddy.c	NS03.DOMAINC	2024-10-27T04:3	2024-10-27T04:3	2025-10-27T04:3
added	pimaprima.eu	GoDaddy.com, L	146	whois.eu	ns17.domaincontrol.com|ns18.domaincontrol.com			
added	teltonika-gps.mx	GoDaddy.com	146	whois.mx	ns63.domaincon	2024-10-28	2024-10-28	2025-10-28
added	dailydigitaldollars	GoDaddy.com, L	146	whois.godaddy.c	NS21.DOMAINC	2024-10-29T00:0	2024-10-29T00:0	2025-10-29T00:0
added	trumpsminuteme	IONOS SE	83	whois.ionos.com	ns1091.ui-dns.d	2024-10-29T00:3	2024-10-29T00:3	2025-10-29T00:3
added	ekg-eho-cardio.k	ua.ukraine	945	whois.com.ua	ns1.s-host.com.u	2024-10-27 15:2	2024-10-28 21:0	2025-10-27 15:2
added	vivririviv.com	GoDaddy.com, L	146	whois.godaddy.c	NS47.DOMAINC	2024-10-29T00:3	2024-10-29T00:3	2034-10-29T00:3
added	sweetsbybeckys	TUCOWS, INC.	69	whois.tucows.co	ns1.systemdns.c	2024-10-29T00:3	2024-10-29T00:3	2025-10-29T00:3
added	cvkbuvonf.cc	Gname.com Pte	1923	whois.gname.co	A.SHARE-DNS.(	2024-10-28T12:3	2024-10-28T12:3	2025-10-28T12:3
added	globalmeddx.cor	GoDaddy.com, L	146	whois.godaddy.c	NS47.DOMAINC	2024-10-29T00:3	2024-10-29T00:3	2025-10-29T00:3
added	norfolkprimecha	Namecheap, Inc	1068	whois.nic.uk	dns1.registrar-se	27-Oct-2024	27-Oct-2024	27-Oct-2025
added	thelondonclinica	GoDaddy.com, L	146	whois.nic.uk	ns19.domaincon	27-Oct-2024	27-Oct-2024	27-Oct-2025
added	bakixanovbelediyyesi.az		0		ns1.dns-parking.com|ns2.dns-parking.com			
added	bomberosbiblian.gob.ec		0		ns7.daganet.net|ns8.daganet.net			
added	brownscrapmeta	Synergy Wholes	1609	whois.auda.org.a	irma.ns.cloudflare.com|porter.ns.c	2024-10-28T22:49:56Z		
added	segurosdeimpagodealquiler.es		0		ns1.sedoparking.com|ns2.sedoparking.com			
added	chrisdoesgamed	GoDaddy.com, L	146	whois.godaddy.c	NS37.DOMAINC	2024-10-28T11:5	2024-10-28T11:5	2025-10-28T11:5
discovered	constanzaonetoj	NIC Chile	0	whois.nic.cl	marge.ns.cloudfl	2024-10-16 14:18:13 CLST		2025-10-16 14:1
added	bazarganilastikshayan.ir		0	whois.nic.ir	ns1.mxndns.com|ns2.mxndns.com			
discovered	khggyd.cn	阿里云计算有限公	0	whois.cnnic.net.c	dns7.hichina.cor	2024-10-19 16:2		2025-10-19 16:2
added	xn--hallsjgrd-c3a	Loopia AB	1625	whois.iis.se	ns2.loopia.se|ns	2024-10-28	2024-10-28	2025-10-28
added	gymkyptservices	Atak Domain	1601	whois.apiname.c	tr1.prodasunucu	2024-10-25T08:3	2024-10-25T08:3	2025-10-25T08:3

You can explore more samples here.

Thank you

www.whoisxmlapi.com

WhoisXMLAPI

The Who Behind Domain, IP & Cyber Threat Intelligence