Use Case Sheet

WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

Empowering the Cyber Threat Intelligence Development Cycle: From Threat Data Collection to Adversary Disruption

Business Problem

As a cybersecurity expert managing security operations or developing security platforms, you know that the quality of protection you provide is tantamount to your cyber threat intelligence. Simply put, incomplete threat intelligence means lousy cybersecurity. Threat actors and attack vectors come from all directions and in all shapes and forms. Failing to account for even one source can weaken your cyber threat intelligence, exposing you and everyone relying on you to costly cyber attacks. A comprehensive and unhindered view of real-time and historical Internet events can help make your cyber threat intelligence more complete and powerful.

Data-Driven Solution

Assembling the most effective cyber threat intelligence—from threat discovery to analysis, expansion, and disruption—requires high-fidelity and high-quality raw data from every corner of the digital world. Every step of the cyber threat development process can hugely benefit from being all-informed of countless Internet events through complete and conveniently delivered WHOIS, domain, IP, DNS, and other data sources, enabling proactive threat detection, in-depth threat analysis, extensive threat expansion, and accelerated threat prevention and disruption.

Notable Use Cases	Connected Data Points
Real-time and early threat detection, prediction, and expansion	Discover possible threats before they get weaponized and predict the prospective badness of digital properties by mapping malicious domain, DNS, and IP connections: • What domains and subdomains added within the past hour share the same digital footprints (e.g., nameserver, registrant information, SSL certificates, and text strings) as indicators of compromise (IoCs)? What IP addresses do these properties resolve to? • Have typosquatting and domain generation algorithm (DGA)-created domains been added or updated within the past hour? • What newly registered or updated domains use self-signed Secure Sockets Layer (SSL) certificates or those issued by less reputable certificate authorities (CAs)? • Do some of the domains have expired or nearly expiring SSL certificates? • Do some domains belonging to unsafe categories, such as adult and gambling sites, try to communicate with a given corporate network? • What endpoints are geolocated in cybercrime hotspots or out-of-service areas? • Do the domain's WHOIS registrant records coincide with its website contact details, or are there significant inconsistencies? • What emails are sent using temporary or disposable email addresses?
Accelerated threat prevention	Enable in-depth threat investigation and analysis to inform threat prevention strategies: • Should security solutions block a given set of new domains registered or updated within the past hour? • Is domain-level blacklisting sufficient, or should your threat intelligence recommend IP-level blocking when several domains resolving to a specific IP address have the potential to go bad? • Should websites with self-signed SSL certificates be allowed network access? • What website categories should be considered as safe for work, and which ones should be blocked? • For security solutions implementing geoblocking, what cities or countries should be blacklisted? • Which disposable email addresses have communicated with corporate networks?

Adversary contextualization

Dig deeper into every detected threat to uncover tactics, techniques, and procedures (TTPs), indicating patterns and telltale bad actor characteristics:

- What are the malicious domains' and subdomains' WHOIS, website contact, IP geolocation, and DNS details?
- Does the malicious property belong to a typosquatting group of domains registered on the same day? If so, what are the other members of the group and are there text strings common to all of them?
- What registration and ownership changes have the malicious domains undergone in the past?
- How is the malicious domain categorized as a website? Is the categorization accurate or inconsistent?
- What are the malicious domain's SSL certificate chain details?
- What are the geolocation details of a malicious IP address? To which IP range does it belong and what entity owns or manages the range?
- What domain names resolve to the malicious IP address? Does the number of connected domains indicate that the IP address is publicly shared?

Adversary disruption and takedown

Take the first step toward disrupting threat actor activities and infrastructure connections:

- What organization owns the IP range to which the malicious IP address belongs? What are its contact details?
- What are the registrar, registrant, and administrative contact details of a malicious domain or the root domain of a malicious subdomain?
- Who issued the malicious websites' SSL certificates? What other clues can you obtain from its SSL certificate chain details?

> **"Through WhoisXML API, we can access DNS, WHOIS, and IP intelligence with real-time and passive coverage. The data works seamlessly with our other intelligence sources, allowing us to derive the most complete cyber threat intelligence so we can analyze and predict threat actor behaviors and provide timely insights to our users."**
>
> **CTO & Co-Founder**
> **Threat Intelligence Feed Provider**

> **"We found certain nameservers that were always used for a phishing campaign, having those in our rules enabled us to catch phishing sites before they affected our user base. WhoisXML API is a responsive and reliable provider of domain intelligence. Whenever there are issues, they are quick to respond and resolve them. Working with them is smooth and straightforward."**
>
> **Christine Bejerasco, Senior Analyst**
> **F-Secure Labs**

Finding Your Own DNS Data (FYODD) Doesn't Let You Scale

Delivering a real-time and uninterrupted satellite view of the world's DNS is our core business. The WhoisXML API data engine is built and frequently upgraded to offer you the most complete, updated, and unique Internet intelligence footprints. We aim to contribute to our clients' competitive edge at every step and give back months or years of development cycle time to your most pressing and mission-critical projects and deployments.

How the WXA Data Engine Is Ready to Add to Your Success Today:

1. Collection	2. Unification	3. Maintenance	4. Delivery	5. Innovation
• Internet-wide data sensing and crawling since 2010 • Legal agreements with major data aggregators • Large and growing network of data exchange partners	• Consistent data parsing of multiple data points across formats • Resolving incomplete, conflicting, and inaccurate records	• Addition of new and historical domains, subdomains, and IP and DNS records • Daily updating of millions of WHOIS, DNS, IP, and other records	• Batch feeds and APIs with complete documentation • Different support and customer success tiers • Streaming of domain and DNS data in real-time • Enterprise-grade IT infrastructure	• Ongoing improvement of data coverage, freshness, and accessibility • New features, product iterations, and solutions driven by market demand

Our Enterprise Value Proposition

Our intelligence is available through customized enterprise packages and product suites with multi-year contracts, flexible licensing models, nonrestrictive data access, and dedicated account and customer success teams. Contact us for more information.

Diamond: Includes all products listed below with Premium SLA
Gold: Pick 2 of each Tier, includes Gold SLA
Silver: Pick 1 of each Tier, includes Silver SLA
Starter: Pick 1 Tier-1 product, 1 Tier-2 product

Tier	Product	Update Frequency
P	Real-time & Historic Whois Streaming	Real-time Stream, Daily & Quarterly Feed, Real-time API Lookups
P	Real-time & Historic Passive DNS Coverage	Daily + Weekly Feed, Real-time API Lookups
P	Enterprise & Threat Intelligence APIs	Enterprise APIs T5 & Threat Intelligence APIs (1M CPM)
1	Real-time WHOIS Data Coverage	Daily & Quarterly Feed, Real-time API
1	Real-time DNS Coverage	Weekly Feeds, Real-time API
1	IP Geolocation & Netblocks Data Coverage	Daily Feeds
1	Website Contacts & Categorization Feed	Daily Feed
2	Subdomains Database Feed	Daily Feed
2	IP Netblocks (IPv4 + IPv6)	Daily Feed
2	IP Geolocation Database	Daily Feed
2	Typosquatting Data Feed (Enriched)	Daily Feed
2	Disposable Email Domains Feed	Daily Feed
2	MAC Address Database Feed	Daily Feed

About Us

WhoisXML API aggregates and delivers comprehensive domain, IP, DNS, and subdomain data repositories. WhoisXML API has more than 52,000 satisfied customers from various sectors and industries, such as cybersecurity, marketing, law enforcement, e-commerce, financial services, and more. Visit whoisxmlapi.com or contact us for more information about our products and capabilities.

WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence