Use Case Sheet

WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

Mapping the Attack Surface from a Vantage Point: Build DNS Data into Attack Surface Discovery

Business Problem

Whether you are an attack surface management (ASM) solutions provider, cyber risk manager, penetration tester, or blue team member, you need a comprehensive view of your or your clients' attack surface. But today's connectivity-reliant services, hybrid work environments, and use of Internet of Things (IoT) devices have added more blind spots to what were already obscure attack surfaces. You can't afford to focus only on portions of attack surfaces, leaving the rest unmapped or untested and, therefore, vulnerable.

Data-Driven Solution

Internet-wide visibility of cyber resources is required for extensive and accurate DNS asset discovery and monitoring, domain and subdomain enumeration and attribution, service discovery, and other critical attack surface mapping processes. To effectively manage your or clients' attack surface, get access to data relevant to the world's Domain Name System (DNS), including domain, WHOIS, IP, and other Internet records. Fusing DNS data into attack surface intelligence lessens the number of blind spots, improves attack surface visibility, and enables you to manage potential threats from a vantage point.

Notable Use Cases	Connected Data Points
Scan, enumerate, and map out your or your clients' digital infrastructure	• Which domain names have been registered using the attack surface owner's corporate email address or other registration details? What could they be potentially used for? • What subdomains were added to the organization's root domains? • How large are domain and subdomain footprints today compared to 6, 12, or 24 months ago? • What IP addresses do the domains resolve to? Which IP netblocks do they fall under?
Create an inventory of cloud/third-party services	• How many domain names, subdomains, and other assets owned by third parties can be connected to a given attack surface? • Were third-party services enabled as identified through DNS records or subdomains? • Does the organization's A records reveal network concentration or single points of failure (SPoFs)?
Discover dependencies relevant to cloud/tech stacks	• What information can be found in the attack surface owner's CNAME records? Are there hidden details about third parties? • Who are the organization's mail server providers according to its MX records? • Are the organization's subdomains associated with dangling DNS records?
Detect rogue assets in real-time	• Are there domain impersonation campaigns against the attack surface owner? • Are there domain generation algorithm (DGA)-enabled cyber resources that could be weaponized? • Are the organization's IP addresses being used in fraud or malicious events?

> *We have this great responsibility to effectively and efficiently manage our clients' attack surfaces, and we can't do that with blurred vision. We have to see everything that's going on, and WhoisXML API has been helping us see what's happening in the DNS without going through painstaking data aggregation and normalization.*

Solutions Engineer
Attack Surface Management (ASM) Company

> *We're constantly comparing the data. With subdomains, you guys again have more, better data. The one other company we were using for subdomains has fewer observations and they do not include dates. Your WHOIS history has more, and more accurate data. Also, your Reverse WHOIS is significantly better than the competition. Your data is pound for pound a much better value. By far.*

Thomas Derenthal, Penetration Tester & Founder - ***CyberIQ***

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 • Enterprise-grade IT infrastructure • Streaming of domain and DNS data in real-time	• Ongoing improvement of data coverage, freshness, and accessibility • New features, products 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