Enrich 24x7 Managed Security Operation Offerings with an In-Depth View of the World's DNS

Business Problem

As a managed detection and response (MDR) team or managed security service provider (MSSP), you know that there is no such thing as a uniform approach to protecting networks. Effectively managing your clients' security operations often means getting your hands dirty and diving deep into each environment's unique vulnerabilities, risk exposure, and security needs. This process involves enriching vast volumes of internal data with relevant external sources of intelligence to shed more light on one of the most common sources of threats—the Internet.

Data-Driven Solution

You can't afford to delay data processing while looking to make sense of ambiguous log events and endpoint connections, prioritizing remediation, and enabling critical defensive security operations 24x7. You need high-resolution and reliable Domain Name System (DNS) data points to provide context to client network data, and you need them to be easily readable and integrable to existing systems and algorithms. Efficient, tailor-made, and round-the-clock security operations and solutions can benefit from real-time and well-structured WHOIS, domain, IP, DNS, and other Internet-related data.

Notable Use Cases	Connected Data Points
MDR and extended detection and response (XDR)	Provide context-rich and correlated threat data for efficient MDR services and XDR solutions that help answer questions, such as: • What registrant organizations, names, email addresses, and other clues are currently and historically behind a suspicious or malicious domain? • What nameservers and IP resolutions did the malicious domain use at the time of the incident? When were these resolutions first and last seen? • Are any of these clues and indicators present in other clients' environments?
Managed endpoint detection and response (EDR)	Map and find out everything possible about endpoints in real-time: • Where is the endpoint's IP address located? • Is the IP address allowed or blocked in the client's network? Is it malicious? • To which IP range does the endpoint's IP address belong? What are its administrative details?
Managed digital forensics and incident response (DFIR)	Provide accurate and relevant threat contextualization to hasten incident responses and fuel cybercrime investigations: • Is the malicious domain or IP address currently or historically linked to known threat actors or advanced persistent threat (APT) groups? • What other domain names resolve to the malicious IP address? Do they indicate a dangerous network of domains? • What other domain names share the malicious domain's current and historical WHOIS record details? Have any of them been used in cyber attacks?
Vulnerability management	Determine the health of your clients' domain, IP, and DNS infrastructure: • Are there exploitable misconfigurations in the organization's Secure Sockets Layer (SSL) certificate? Are there inconsistencies in the complete SSL chain? • Are the client's DNS records configured correctly? Are there signs of dangling DNS records that could lead to subdomain takeovers? • Are the organization's domains adequately protected with the appropriate status codes? Is their infrastructure, including nameservers, mail servers, and subnetworks, configured correctly?

> WhoisXML API has one of the largest WHOIS *and DNS repositories I’ve* used in my career as a data scientist. Their data has helped us really dive into the unique digital surfaces of our clients. As a result, we understand vulnerabilities and risk exposures better to provide effective and specialized security services.

Data Scientist and Security Analyst
Managed Security Services 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