Use Case Sheet

WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

# Security Intelligence (SI) Suite: How to Use and Combine Our Cyber Threat Intelligence Feeds

Every product included in the Security Intelligence (SI) Suite offers easy-to-consume and integrable data that enables security teams to counter domain, subdomain, and IP-related threats with weekly, daily, or even near-real-time updates. The following use cases are just some of the many ways commercial security platform (SIEM and SOAR systems and TIPs) developers, SOCs, MSSPs, and Fortune 1000 companies have integrated our cyber threat intelligence sources into their security solutions or operations.

1

# Attack Surface and Third-Party Risk Management

Gathering every possible attack vector is crucial to getting a comprehensive look at and effectively determining an organization’s attack surface and managing third-party risks. The SI Suite can provide intelligence on domains, subdomains, and IP addresses that could be used to attack your network, employees, partners, and clients.

| | |
|---|---|
| **WHOIS Data Feed** | • What domain names contain your company or brand name?<br>• Who owns the typosquatting domains?<br>• What other domains share the typosquatting domains’ registrant email address? |
| **WHOIS + IP Geolocation Database** | • Where are the IP addresses connected to the domains that comprise your attack surface geographically located?<br>• Who are the Internet service providers (ISPs) responsible for the IP addresses so they can begin taking down the malicious entities? |
| **WHOIS + IP Netblocks Database** | • What IP netblocks are associated with the suspicious domains?<br>• Who owns these IP netblocks? Are there reports of malicious activities associated with them? |
| **WHOIS + Passive DNS Database (Reverse IP)** | • What other domains share the same IP address?<br>• Do these domains widen your attack surface? |
| **WHOIS + Subdomains Data Feed** | • Are there new subdomain additions to your site infrastructure? What are these?<br>• What subdomains of other domains contain your brand or company name? |
| **WHOIS + Contacts and Categorization Data** | • How are the domains in your attack surface categorized?<br>• What top categories do the domains fall under? |
| **WHOIS + Typosquatting / Bulk Domain Detection** | • What look-alike domains were bulk-registered in a single day?<br>• Who owns these typosquatting domains? |

# 2 Platform Enrichment (TIP/SIEM/SOAR)

Do you develop security products and want to integrate as many relevant data sources as possible into them? Boost your products' intelligence with possibly the largest domain and IP intelligence data feeds. When your platform identifies a suspicious Internet entity, the SI Suite can help gather context with dozens of data points available to answer these questions:

| | |
|---|---|
| **WHOIS Data Feed** | • When was the suspicious domain created?<br>• Who owned it before WHOIS redaction?<br>• Are there other domains that share the same registrant email address or other registrant details? |
| **WHOIS + IP Geolocation Database** | • What is the host IP address of the suspicious domain?<br>• Where is the IP address geographically located? Is it located in a fraud or cybercrime hotspot? |
| **WHOIS + IP Netblocks Database** | • What IP ranges do the IP addresses belong to?<br>• Who owns or manages the IP ranges so you can facilitate related domain takedowns? |
| **WHOIS + Passive DNS Database (Reverse IP)** | • Are there other domains hosted on the same IP address?<br>• Are the domains flagged by the security platform? |
| **WHOIS + Subdomains Data Feed** | • How many subdomains does the suspicious domain have?<br>• When were the subdomains first and last seen? Does the data coincide with other cyber incidents? |
| **WHOIS + Contacts and Categorization Data** | • Does the website have contact information? Not publicizing contact details could signal illegitimacy.<br>• Does the domain belong to restricted or blacklisted categories of Internet sites? |
| **WHOIS + Typosquatting / Bulk Domain Detection** | • Was the domain bulk-registered?<br>• If so, what other domains were registered along with it? |

3

## Phishing and Brand Protection

Protect employees, clients, and other stakeholders from phishing emails or copycat websites that imitate your domain name by strengthening your brand protection strategies. Ensure your reputation remains untarnished by keeping track of look-alike domains using SI Suite products to answer these questions:

| | |
|---|---|
| **WHOIS Data Feed** | • How many domains resemble yours? What are they?<br>• Who owns them now? Who owned them in the past?<br>• What other domains share their current or historical registrant name, organization, or email address? |
| **WHOIS + IP Geolocation Database** | • Who are the ISPs of the potential phishing domains?<br>• Are the associated IP addresses located in cybercrime hotspots? |
| **WHOIS + IP Netblocks Database** | • What IP ranges do the IP addresses belong to?<br>• Are there other possible phishing domains using the IP ranges? |
| **WHOIS + Passive DNS Database (Reverse IP)** | • Are there other phishing domains hosted on the same IP address?<br>• When were the domains first and last seen? Do the dates coincide with publicized phishing incidents? |
| **WHOIS + Subdomains Data Feed** | • What are the subdomains of known phishing websites?<br>• Have any suspicious subdomains been added to your website? |
| **WHOIS + Contacts and Categorization Data** | • Do the contact details of a suspicious domain match that of the imitated brand? Mismatched or missing contact details could be signs of illegitimacy.<br>• What are the phishing domains and subdomains in a specific category?<br>• Are the categories consistent with how popular brands categorize their websites? |
| **WHOIS + Typosquatting / Bulk Domain Detection** | • Are the look-alike domains bulk-registered in groups with others?<br>• How many misspelled variations of your domain were bulk-registered on a given day? What are they? |

4

## Threat Hunting and Cybersecurity Investigations

The SI Suite enables security teams to regularly scan their networks for potential threats, whether they come in the form of old or newly registered domains (NRDs). Known indicators of compromise (IoCs) can also be investigated and expanded to include other artifacts. With the help of domain, DNS, and IP intelligence, you can discover the answers to these questions:

| | |
|---|---|
| **WHOIS Data Feed** | • What are the NRDs?<br>• Who are the NRDs' current and historical registrants? Are any of them known threat actors? Or are they related to known attacks?<br>• What are the current and historical WHOIS ownership details of known threat IoCs? |
| **WHOIS + IP Geolocation Database** | • What are the NRDs' host IP addresses? Are they publicized IoCs or suspicious entities?<br>• What are the threat IoCs' host IP addresses? Are they also tagged as IoCs? |
| **WHOIS + IP Netblocks Database** | • What IP ranges do the IP addresses publicized as IoCs belong to?<br>• Are the IP ranges associated with NRDs connected to known threats? |
| **WHOIS + Passive DNS Database (Reverse IP)** | • What other domains are hosted on the same IP addresses as the identified IoCs? These domains could be considered threat artifacts.<br>• When were the artifacts first and last seen? Are they related to recent threats? |
| **WHOIS + Subdomains Data Feed** | • What are the subdomains of the IoCs and artifacts?<br>• When were the subdomains first and last seen? Have they been used to carry out attacks? |
| **WHOIS + Contacts and Categorization Data** | • What are the contact details in the NRDs' WHOIS records? The presence of email addresses, social media profile links, and phone numbers could help prove that they are benign.<br>• What categories do the threat IoCs and artifacts belong to? |
| **WHOIS + Typosquatting / Bulk Domain Detection** | • Are the threat IoCs, artifacts, and NRDs bulk-registered with other domains?<br>• Which typosquatting groups do they belong to? |

# 5 Fraud Detection

WHOIS records, IP address associations, the presence of website contact details, and other domain and IP intelligence data points could hint at the legitimacy and trustworthiness of an entity. The SI Suite can help detect fraudulent clients, suppliers, partners, and other entities by providing answers to these questions:

| | |
|---|---|
| **WHOIS Data Feed** | • Does the given domain exist? If it does, what are its current and historical ownership details?<br>• What other domains share the same registrant name, organization, or email address? |
| **WHOIS + IP Geolocation Database** | • What are the host IP addresses of the domains?<br>• Where is the IP address geographically located? Is it located in a fraud or cybercrime hotspot? |
| **WHOIS + IP Netblocks Database** | • What IP ranges do the IP addresses belong to?<br>• Are the IP netblocks associated with known fraudulent activities or entities? |
| **WHOIS + Passive DNS Database (Reverse IP)** | • Are there fraudulent or suspicious domains that share the same IP address?<br>• When were the domains first and last seen? Do these coincide with known fraudulent and other cyber incidents? |
| **WHOIS + Subdomains Data Feed** | • What are the subdomains of the potential clients', suppliers', or partners' domains? Are there legitimate reasons for adding the subdomains?<br>• What are the subdomains of known fraud domains? |
| **WHOIS + Contacts and Categorization Data** | • Do the given domains' contact details match those of the potential client, partner, or supplier?<br>• Does the domain belong to any restricted category? |
| **WHOIS + Typosquatting / Bulk Domain Detection** | • Were the fraud-related or suspicious domains bulk-registered with others?<br>• Are there domains that use misspelled variations of the potential client's, supplier's, or partner's name? |

## Contact Us

We have gathered, processed, and aggregated domain, IP, and DNS intelligence for more than a decade now to make sure the Internet remains transparent and secure. Reach out to us at sales@whoisxmlapi.com to learn more about how the SI Suite can help you with your cybersecurity requirements.

WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence