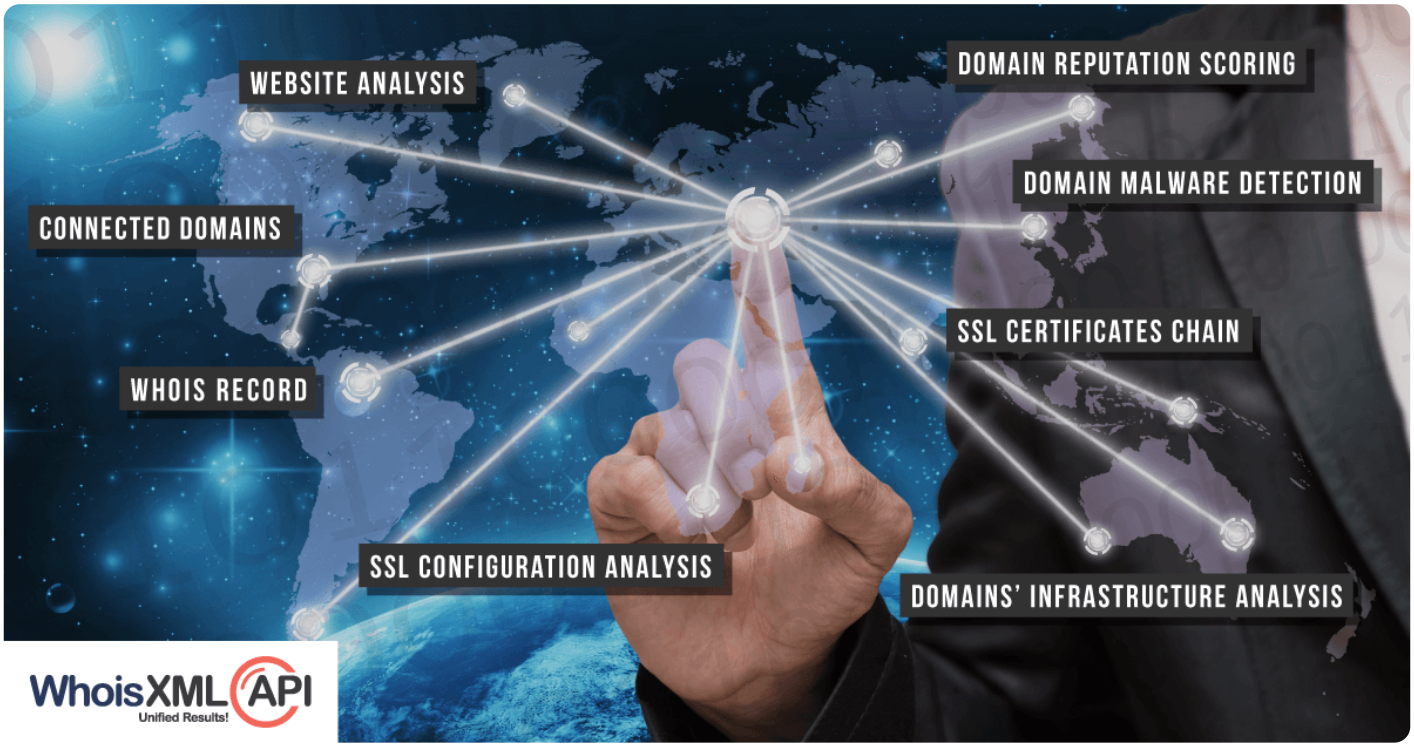
Approach Cyber Security the Smart Way!

Posted on December 19, 2018



With each passing year, the magnitude of cyber crime has increased steadfastly. Small & large companies alike are facing threats to their online infrastructure, customer data & reputation with these constantly evolving attacks. Whether it is an in-house IT team monitoring the safety of their company, MSSP providing security services, or security analyst detecting cyber crime at large, smart cybersecurity begins with knowing what you are really up against and having valuable data about hosts, domain owners, websites, servers, and configurations. But with the plethora of data points available to verify & analyze this task has only become more difficult. Professionals are now no longer looking for just data sets but Intel over various online entities to take timely action & make informed decisions on their security operations & strategy.

Threat Intelligence (TI) can be a great building block in your toolkit for threat detection. It aggregates, correlates & analyses real-time threat data & provides an in-depth perspective on any hostname and the infrastructure behind them. When put into context, it provides a roadmap for tackling one's security vulnerabilities and assessing the trustworthiness of third parties which can help in anticipating where criminals are likely to strike. This can also be a valuable instrument to improve your security department's performance while also reducing organizational costs.

Whois API, Inc. provides this crucial Threat Intelligence to professionals in 2 forms:

1) Threat Intelligence API

You can directly integrate Threat Intelligence API with your pre-existing security systems and processes, incident response platforms or SIEMs. These APIs serve as shortcuts as there is no need to compile sources of data manually, allowing to move directly to the analysis of critical online assets & analyzing threats like intrusion detection and prevention, secure email gateways, firewalls, web application protection and more. Integrating TI feeds into your organization's systems and applications via APIs will complement your current systems seamlessly yielding more effective results, along with, providing fast and streamlined access to TI data across departments.

2) Threat Intelligence Platform

Threat Intelligence Platform provides a quick, visual overview of a domain & its infrastructure to analyze threats in real time. Our easy to use & advanced web interface does not require coding, software installation, back-end systems or any other complexity to access Intelligence. The online

platform analytics enables security analysts to quickly investigate and raise red flags on suspicious traffic.

The various exploitable vulnerabilities & threat data that security professionals can identify & analyze with Threat Intelligence from Whois API, Inc. are:

- **Domain's Infrastructure Analysis**

Get comprehensive Intel on the different elements that comprise a domain and know details about its web, mail & name servers along with its IP address, geolocation & subnetwork information. These aspects help determine the credibility & security of any domain.

Domain's Infrastructure Analysis provides a context in the investigation of malicious domains. It can shed deep insights on how cybercriminal networks are organized, where their servers are located, how they are dispersed, and what kinds of data they are distributing.

- **SSL Certificates Chains & Configuration Analysis**

Get a breakdown of a particular domain's SSL Certificate and the complete SSL Certificates chain starting with the end-user to the intermediate certificates and then to the root SSL Certificate to verify the sender's trustworthiness. It also helps Identify SSL connection to their hosts and analyze their configurations to detect any likely issues that might lead to vulnerabilities.

SLL Certificates Analysis helps security professionals to validate the identification & trustworthiness of a domain. It also confirms data encryption thereby protecting businesses that are conducting their interactions online from hackers or even economic losses.

- **Domain Malware Detection**

Get to know if a domain name is blacklisted or considered dangerous from multiple reputed & trusted security data sources. It saves professionals a lot of time because there is no need to perform searches manually, website by website, since our system run the domain through multiple databases that track malware.

Malware is one of the biggest cybersecurity threats today and with Domain Malware Detection, analysts can cut the legwork & take timely actions against bad actors.

- **Connected Domains**

Get a list of all the domain names resolving to an IP address, including subdomains & also get details of the infrastructure of these connected domains.

Connected Domains checks whether a domain is part of a malicious cluster of domains, allowing cybersecurity teams to warn employees about potentially dangerous websites, and promptly configure firewalls to block traffic from the cluster. It is also helpful in investigating fraudulent networks. Connecting the dots of similar domains and shared IP addresses trace the extent of malicious activities and can lead to other domains owned by a cybercriminal. Discovering the networks of dubious websites and their handlers might result in their subsequent prosecution and eventual shutdown. Also, legit online businesses sharing a host server or IP address with malicious actors can damage their reputation. So by checking their neighborhood, they can proactively opt to transfer their website to another hosting service.

- **Domain Reputation Scoring**

Get real-time risk analysis of a domain. Our detection system examines the domain's website content, Whois records, IP infrastructure, DNS records, and network data, along with data aggregated from multiple reputed security sources for malware threat level and assigns a categorized & weighted score to determine the Reputation of a domain. Our algorithm takes into account 120 attributes before predicting the Reputation Score & confirming if a domain is safe & legit.

Domain Reputation Scoring can help point forensic investigators toward those domains most likely to be of malicious nature even before it has struck someone. It also helps identify websites involved in malware incidents, fraudulent activities, and phishing activities. Online merchants can assess the risk levels of domains, to avoid mishaps and losses caused by fraudsters without taking the time and effort in manually checking each domain before associating with them.

Key Benefits of Threat Intelligence

- Aggregation of intelligence from multiple sources in a real-time view.

- Finding data points co-related to other Intel.
- Timely, relevant, and actionable insights.
- Understand infrastructure vulnerabilities & potential threats quickly, make smarter decisions and accelerate detection and response to cyber security incidents.
- API for seamless integration with existing security systems.
- Integrating your systems & tools with TI offered by Whois API Inc can provide all the back-end data intensive support to SOCs.
- Centralize data & customize our intelligence for integrating with other parts of security intelligence.
- Improve the performance & scalability of Security Information and Event Management (SIEM), Threat Intelligence Platform (TIP), Automation, and Orchestration Tools by automating domain & network data collection & processing.
- An excellent foundation for your incident response platforms and to create tickets in incident management tools.
- Enable a complete investigative workflow.
- Helps Managed Security Service Provider (MSSP) and Managed Detection and Response Provider (MDR) to differentiate their threat detection and management services.
- Provide more value-added service.

Now more than ever, it is vital to have accurate threat intelligence to support your team's efforts for security planning, monitoring and detection, incident response, threat discovery and threat assessment.

Access Threat Intelligence API: https://main.whoisxmlapi.com/cyber-security-research/threat-intelligence-api

Access Threat Intelligence Platform: https://main.whoisxmlapi.com/cyber-security-research/threat-intelligence-platform