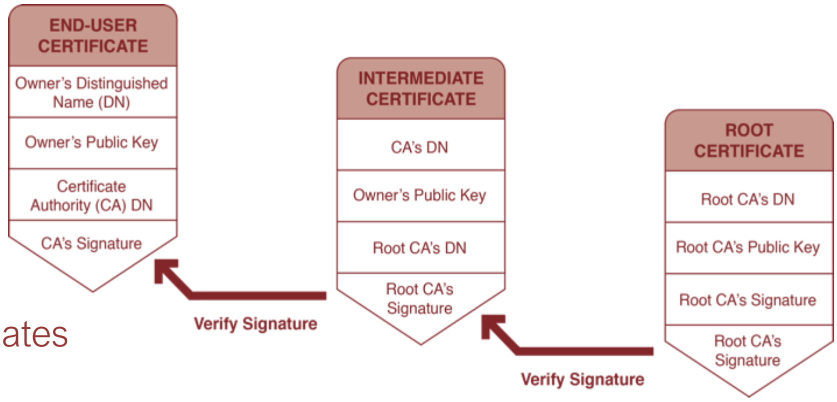
Product Sheet

WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

Real-Time SSL Certificate Chain Coverage

The lock icon before URLs could provide Internet users with a false sense of security. Failing to further validate SSL certificates can lead to danger.



The general public often delegates the security of Internet connections to Secure Sockets Layer (SSL) certificates, and rightly so. Aside from authenticating websites, SSL certificates provide encryption between browser and website traffic. But threat actors know that this mechanism is heavily relied on and look for ways to exploit it.

In fact, it has become a common practice to obtain or hijack SSL certificates for weaponized domain names, lulling users to feel a false sense of security. Such a tactic may sound scary, but is nonetheless actionable and detectable. Validating and investigating SSL certificates are urgent cybersecurity practices, which require access to extensive SSL certificate data. But the hierarchical, time-bound, and dynamic nature of SSL certificate assignments do not make this endeavor easy.

You need to tap the right data partner that can dig into domains' entire SSL certificate chains at a meaningful scale with a satellite view of the global Internet, while providing granular outputs—trace the end-user certificate to its intermediate and root certificates and unravel critical data points relevant to every SSL.

Widen cybersecurity measure coverage with real-time and streamed SSL certificate chain data.

WhoisXML API's stack of Internet intelligence sources is made even more inclusive, targeted, and relevant with the addition of SSL certificate chain data. Over a decade of web crawling and Internet data parsing has allowed us to build an extensive domain repository comprising 565+ million active domains, for which we have gathered millions of SSL certificates.

With these records, organizations can retrieve a domain name's whole SSL certificate chain with the help of our unified, consistent, and normalized delivery models, including downloadable batch feeds, real-time APIs, and real-time data streaming. We offer scalable data access packages, flexible licensing options for data redistribution, and enterprise-grade customer support and infrastructure. Contact us for more information or download our SSL certificate chain data samples here.

30 million+	565 million+	200 million+	300,000+
SSL certificates processed daily	Active domains tracked	Domains tracked quarterly	Domains updated daily

Practical Usage

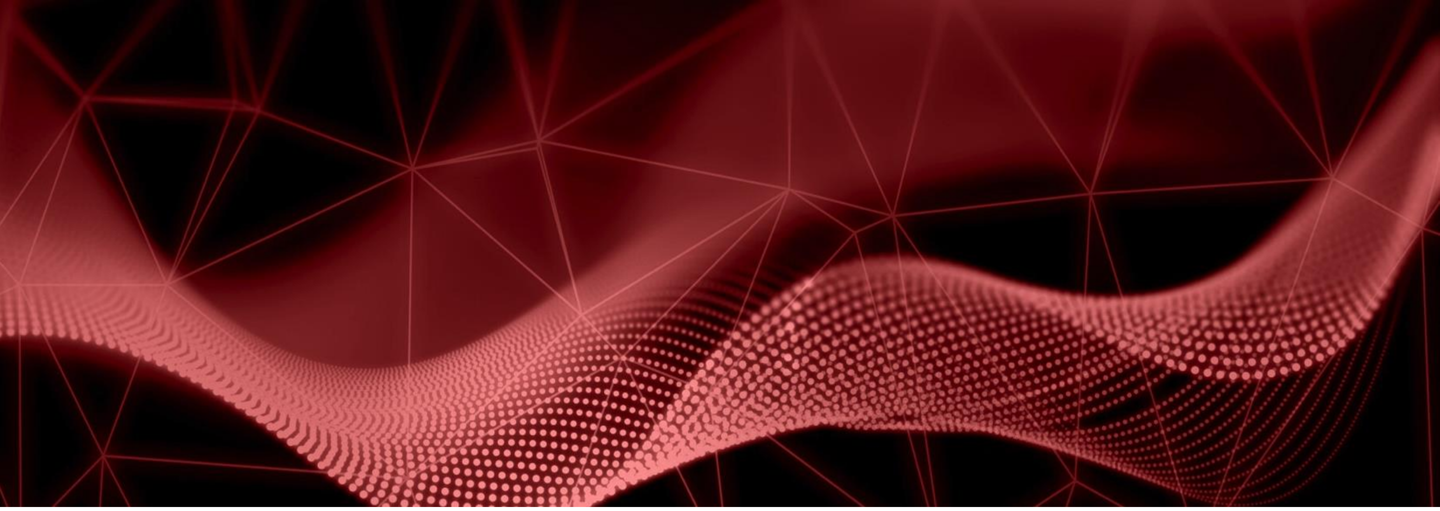
Get the SSL certificate intelligence you need to:

- Get alerted to domains with self-signed certificates to avoid related risks.
- Identify untrustworthy domains by checking their SSL certificates and SSL certificate chain.
- Uncover any domain's entire SSL certificate chain to check for inconsistencies and misconfigurations.
- Pivot off the SSL certificate data of malicious domains to expand threat investigations and enrich tools, tactics, and procedures (TTPs) identification.
- Monitor SSL certificate and SSL certificate chain modifications to keep pace with domain ownership changes.
- Augment the capabilities of security incident and event management (SIEM); security orchestration, automation, and response (SOAR); threat intelligence; and other platforms.

What SSL Records Are Included?

Our SSL certificate chain intelligence contains relevant data points that help determine SSL certificate chain hierarchy, connection, and validity.

Data Points	Description
Domain	Refers to the domain name the SSL certificate chain belongs to
IP Address	Refers to the IP address the domain resolves to
Port number	Identifies the port on which the SSL connection was established
Status	Determines if the domain name's owner just added, dropped, or updated an SSL certificate (applicable only to Real-Time Streaming)
Certificates	Lists all SSL certificates uncovered for the domain name
Chain hierarchy	Identifies the position of the certificate in the chain - end-user, intermediate, or root
Validation type	Refers to how the certificate was validated - domain, organization, extended, individual, self-signed, or self-signed certificate authority (CA) validation
Validity Period	Reveals the certificate's validation and expiration dates (with their corresponding time of day)
Serial Number	Provides the unique identifier of the certificate within the CA system
Signature algorithm	Refers to the algorithm used to sign the certificate's public key
Issuer Information	Reveals the distinguished name (DN), organization, location, and other details relevant to the certificate's issuer
Certificate Privacy Enhanced Mail (PEM)	Provides the certificate's raw data encoded in PEM format
Certificate extensions	Lists the available certificate extensions and other related details, such as subject key identifier, usage, certificate revocation list (CRL) endpoints, and issuer details
Public key information	Provides the certificate's public key details, including algorithm and length



What SSL Certificate Chain Data Delivery Models Do You Provide?

Our SSL certificate chain intelligence is accessible through data streaming, batch feeds, API calls, and GUI tools. See the table below for an overview of our main data delivery models.

Product	Delivery Model
Real-time SSL Certificates Coverage	Real-Time Data Streaming
	Daily Batch Feed
	Real-Time API and GUI Lookups

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 at sales@whoisxmlapi.com for more information about our products and capabilities.

WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence