NormShield Success Story: Leveling Up Third-Party Risk Assessment with Domain & IP Intelligence

WhoisXML API, Inc.

Overview

WhoisXML API is proud to announce its partnership with cybersecurity solution provider NormShield. NormShield enables enterprises to evaluate their external cyber risk posture by letting them conduct non-intrusive third-party risk assessments. NormShield's growing client base operates in various industries, among which are financial services, healthcare, manufacturing, retail, and tech in general.

The results of third-party risk assessments powered by NormShield come in the form of intuitive scorecards that immediately tell enterprise users what their most salient cyber risks are. The scorecards also contain recommendations on how to deal with each risk based on its priority level.

NormShield relies on comprehensive and accurate domain, subdomain, and IP address data to conduct thorough risk evaluation of its clients' suppliers, subsidiaries, and other stakeholders. The company has partnered with us to integrate the IP Neblocks WHOIS Database Feed and Whois Database Feed into its processes — now monitoring more than 1.2 billion domains, 7 billion WHOIS records across 2,864 top-level domains (TLDs), and 9.1 million IP netblocks.

Here is more about the challenges our products have helped to deal with and the exciting details of this fruitful collaboration.

NormShield: The Launch of a Third-Party Risk Assessment Company

Third-party risk management is now fundamental. Highly publicized attacks on supply chain members worldwide have highlighted the need for organizations to consider their security posture beyond their own network.

Almost 60% of companies reported having suffered a data breach caused by a third party. Companies also cited increased dependence on external services and lack of visibility into ecosystems as common reasons for vendor-related breaches.

These trends are consistent with NormShield's co-founder and chief technology officer (CTO) Candan Bolukbas' first-hand experience. Having held senior cybersecurity positions at both public and private organizations, Candan pen-tested some of the most secure military & government systems ever built. On many occasions, Candan found that at the leading entry point into rock-solid institutional networks were third-party suppliers.

And so the need for a company like NormShield became evident. In Candan's words:

"We launched a startup showing companies how the third parties they're working with are risks for them, and so they better be monitored. The timing couldn't be better, considering that most organizations still resort to outdated risk assessment methodologies, like manual inspections and surveys."

NormShield is a member of MACH37, America's premier cybersecurity accelerator. MACH37 focuses on energizing the growth of next-generation cybersecurity companies. The accelerator has a uniquely-designed program that emphasizes product validation, relationship building with key stakeholders, and the establishment of an initial customer base. Some of the companies in MACH37's latest cohort include FortMesa, Aryia, Malwork, and Definitive Data Security.

Challenges in Gathering Adequate IP and Domain Intelligence

NormShield extensively relies on external IP and domain data feeds to carry out thorough risk analyses. But gathering the said information can be difficult because of:

1. **Disparate data sources:** WHOIS and IP data points are scattered across hundreds of registrars and ISPs. Acquiring the information at the scale required to protect the world's most important businesses involves lengthy bureaucratic processes and an incredible amount of manual work. This calls for a mountain of bandwidth that would only distract NormShield's industry-leading analysts from other mission-critical tasks.
2. **Inconsistent data formats:** Registrars and ISPs differ in the way they collect and store IP and domain information, so a lot of work needs to go into the data processing and parsing of ever-changing formats before the records can be leveraged for third-party risk assessment.
3. **Vendors without proper agreements:** Not all domain and IP data providers have the necessary working agreements with registrars and ISPs to cover the entire WHOIS and IPv4 spaces beyond what's made publicly available.

This is where WhoisXML API stepped in.

Partnering with WhoisXML API

NormShield's partnership with WhoisXML API enabled the company to obtain complete and well-parsed values from WHOIS and IP records to support its monitoring processes. WhoisXML API's comprehensive databases contain more than 1.2 billion domains, 7 billion WHOIS records across 2,864 top-level domains (TLDs), and 9.1 million IP netblocks.

NormShield uses the IP Neblocks WHOIS Database Feed and Whois Database Feed to identify domains and IP ranges that organizations and individuals use to interact with its clients' networks. The data points available on IP ranges include netblock borders, administrator details, contact information, assigned organization, and country, among others. WHOIS API, meanwhile, provides NormShield with domain information from multiple registrars, which has been parsed and normalized into individual entries.

*"We're excited to get the data as **it's above our expectations in terms of accuracy**. We haven't used data feeds like WhoisXML API's before. They were among the main components that we used to spin up our business."*

WhoisXML API collects data from multiple sources and has agreements with hundreds of registrars and ISPs. We provide NormShield with complete and accurate data feeds that can be readily integrated into its systems.