How a Website Categorization Database Can Contribute to Fraud Monitoring

Posted on October 11, 2019

Fraud detection and prevention solutions are on the rise, and so are expectations from vendors. Many enterprises users are looking for providers that can offer holistic products and augmented capabilities. Let's dive into that point and talk about how a **Website Categorization Database** can prove useful as a means for data enrichment.

What Makes a Good Fraud Monitoring Tool?

To start, a good solution should be able to detect and respond to a variety of cases of fraud, either applying to an entire industry or specific to an organization. What's more, it should identify odd occurrences (if and when these happen) as well as easily integrate into existing ecosystems. That's a given.

In 2019, however, some advanced capabilities are starting to become necessary, driving the emergence of next-generation solutions that modern fraud detection teams can no longer live without. For instance:

The Ability to Detect a Wide Range of Cases of Fraud via Machine Learning

An ideal fraud monitoring tool should run a solid rule engine with an advanced set of rules, one that can identify potential cases of fraud based on certain criteria. It shouldn't, however, rely on this feature alone — primarily because rule-based systems may no longer be able to keep up with today's more advanced attacks.

The good news is that some tools use machine learning (ML) to meet this requirement. ML hastens a tool's ability to analyze a larger volume and variety of data. It does away with the human factor as well, thus reducing human error. An ML-based solution can employ different algorithms to come up with relevant findings for expert verification.

Using a Dynamic Approach to Determining Authentication Flow

A fraud monitoring system should be compatible with already existing systems and solutions as well as even the most advanced multifactor authentication tools. It must constantly evaluate risks

tied to a certain event and facilitate seamless authentication flow based on its analysis. Furthermore, it should be able to dynamically trigger the best solution for a given scenario based on the risk it poses.

For instance, if a specific transaction has been categorized as suspicious due to an information mismatch, solutions should be able to move on to the next authentication criteria. Then it is necessary to test the event against all parameters first, rather than simply reject or put a transaction on hold for manual review as soon as it is flagged.

Having Out-of-the-Box Fraud Prevention Capabilities

An effective anti-fraud tool should be capable of detecting a fraudulent transaction right from the start. Be sure though that it can support business continuity demands by ensuring smooth transitions. The reason why? Companies can't afford for their tools to freeze while processing risk analytics and cases. As such, a solution that can provide an acceptable level of protection in a timely fashion is essential.

Although an out-of-the-box solution is a good start, its capabilities need to be flexible so it can be customized according to a client's needs.

What's the Link between Website Categorization and Fraud Monitoring?

Companies that specialize in offering fraud monitoring solutions can benefit from a website categorization database as this serves as an additional source of website intelligence. It provides users with a well-structured domain name database that is updated for accuracy on a daily basis.

Our solutions, including Website Categorization API, use ML for near real-time results even when dealing with new cases. They also come with versatile rules that have been predefined by industry experts, allowing users to acquire data on active domain names without needing to conduct manual web scraping or research.

This capability is particularly useful since most cases of fraud involve the use of several websites. In fact, millions of domains are registered each year by threat actors who aim to scam organizations.

WhoisXML API Offers Streamlined Website Categorization

Our web categorization database can be filtered according to a variety of categories. This allows users to analyze data in different ways, depending on what they are looking for. The information in the database can be filtered and analyzed by:

- **Website location:** Our database provides website information for a single country, several countries, or all countries should users be identifying cases of fraud in specific locations. It does so because it covers domains registered worldwide, including those that use ccTLD and the newly created gTLD extensions.

- **Website category:** We currently classify websites into 25 categories. Note that a website can appear in several of them at once. Fraud investigators that require additional categories can send in requests to fulfill their threat data requirements.

Our **website categorization database** gives fraud detection and monitoring companies accurate website information practically in real time with the aid of ML technology. Although not an all-in-one solution, the categorization tool still offers a step in the right direction for those in the fraud investigation business. If you want to know more about our products, send us a message.