Synechron
Digital / Business Consulting / Technology

Thought leadership

Lisa Toth
Global Head of Regulation & Risk

Measuring & Detecting Anomalies to Fight Financial Crime

Measuring & Detecting Anomalies to Fight Financial Crime

To affectively use data science in financial services, the industry requires a process capable of 'learning', adapting, and defining the ever changing shape of 'normalcy' in order to reliably detect anomaly. It must be capable of identifying anomaly in the shape of normalcy, operating under the premise that what you seek does not want to be found.

Leveraging passive anomaly detection, like that provided by SQREEM Technologies, firms are able to identify those accounts who are not who they say they are. This is effected through a dual control, looking concurrently at the footprint of the client based on their defined personal/firm information, their investment intent, and then layering on their transactions. Passive anomaly detection then looks for the "unknown unknowns" by comparing a firm's account and transaction data across all customers to establish a normalcy pattern. The next step is to run the data through a "look alikes" algorithm that identifies how many other clients have a similar foot print to weed out the false positives. This then leaves you with the true anomalies to investigate.

Autonomous & Self-Assembling Machine Intelligence

The key to engineering an autonomous process capable of performing such tasks lies in the ability to programmatically define the anatomy of behavior and intent. A person's actions, as random as they may appear when viewed individually, may actually be highly predictable when defined within proper behavioral context. And therefore, data science can be used to automate tasks like product recommendations or AML threat detection.

Active Detection - You know what you are looking for but don't know how it will happen.

Technologies like SQREEM have the ability to generate predefined, or rules based, threat scenarios designed to identify commonly misaligned intent (e.g. money laundering, unauthorized transfers, error cover-up, etc.) without requiring predefined patterns for successful detection. This is scaled to cover millions of actions taking place inside an organization, with the capability to analyze each individual transaction as to its wider behavioral context. Misaligned activity does not come about randomly, yet it most often remains undetected in the complexity, chaos, or apparent randomness of the many events and activities around it.

Passive Detection - You don't know what to look for, until it's too late.

New threats usually strike from an entirely unanticipated domain and represent the unknown unknowns. The key to passive threat detection with minimal false positives is to be able to establish the normalcy pattern and then measure the distance from normalcy for each account or transaction patterns. In simplified terms a passive anomaly is an activity for which no adequate intent can be established. Additionally, passive detection reliably identifies repeated occurrences of unintended mishaps, waste, inefficiency, liability, or professional incompetence, otherwise undetected.

While these approaches are fundamentally different, businesses are best-served with a hybrid approach that takes combined active and passive detection. A combination of rules-based systems searching for known threats, and anomalous activity detection identifying unknown threats becomes an even more powerful combination.

Synechron
Digital / Business Consulting / Technology

finlabs@synechron.com | synechron.com/finlabs

USA / Canada / UK / Switzerland / France / The Netherlands / Luxembourg / Germany / Hungary
Serbia / Italy / UAE / India / Singapore / Hong Kong / Philippines / Japan / Australia