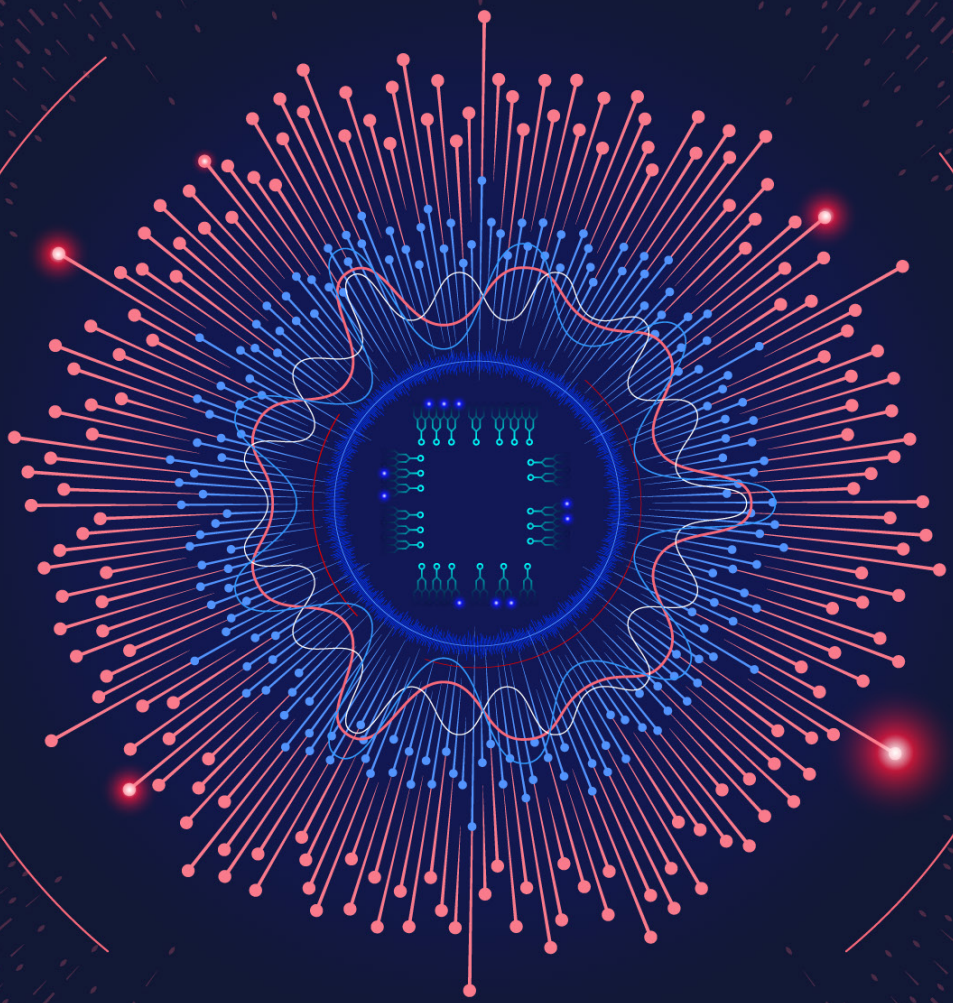
smarsh®



THE SURVEILLANCE LEADERS NETWORK

PUTTING TECH TO WORK IN SURVEILLANCE

Whether delving into the behaviour of traders or fine-tuning the volume of alerts, technology such as artificial intelligence and machine learning has the potential to overcome many of the biggest challenges in surveillance.

The opportunities and challenges of sales and trader profiling as well as regulators' expectations of the use of artificial intelligence (AI) and machine learning (ML) dominated discussions at 1LoD's latest Surveillance Leaders Network event. UK-based participants met in London on 21 September while other attendees from across the world joined in via Zoom.

"Regulators are starting to understand why AI and ML can make a difference, and why it's important to stay in tune with innovation that's happening in these tools" GOUTAM NADELLA, CHIEF PRODUCT OFFICER AT SMARSH

Sales and trader profiling

The majority of participants at 1LoD's Surveillance Leaders Network event already had a clear interest in sales and trader profiling, the topic of the first session. An attendee poll showed that 62% of participants were developing the business case for such capabilities and had launched small-scale proofs of concept. But the degree of commitment varied: another 15% said profiling was a low priority for their organisation, while 23% described it as a medium-level or high priority for 2022.

One participant said that Covid-19 and remote working had provided an impetus to embark on the path towards profiling. Others said it was still difficult to argue the business case. Another agreed, but said it was imperative to start work on profiling even before clear use cases emerge.

Varied input signals

The input signals that banks see as fundamental to current or future profiling work are also varied.

One participant said that his organisation focused purely on metadata as inputs for profiling communications and trade, and looked for anomalies rather than targeting specific behaviours. Another said the 1LOD at his firm has explored applying behavioural science and natural language processing (NLP) to E-comms to identify potential rogue individuals.

The most fruitful place to start with profiling might be examining how traders interact with the market, according to Mike Coats, chief technology officer at TradingHub. Trading data is more immediately available, relevant, structured and easily analysed than, for example, data about staff breaks or social media posts, he said, plus it builds a richer picture of a trader's behaviour over time. It would also provide commercial insights for the front office and senior management – for example about whether a trader makes their P&L from market positioning rather than from the value of the sales franchise – which is information that could justify cost-sharing.

Approaches outlined by other participants included monitoring the velocity of P&L recovery to profile for market abuse and using pre-configured score card weightings – covering email traffic volume through to P&L signals – to identify potential rogue traders.

Several participants cited complex book structures as a challenge given that traders often run multiple books or share books with others. They proposed initially aggregating books for analysis until individual P&L owners could be identified.

Collaborative tool-building

Banks' tech efforts for profiling mostly involve in-house sandbox exercises, with several participants building or enhancing existing surveillance systems or building tools on top of data lakes that are fed from multiple sources across the organisation.

Work typically involves collaboration across the three lines of defence, although participants acknowledged that ultimately each line will probably develop separate processes.

In some firms, internal audit has stolen a lead on compliance – for example, by hiring data scientists or building their own dashboards in order to assess which traders or behaviours to prioritise.

This work is at too early a stage in most firms to yield hard results. However, one participant noted that by stimulating dialogue with the 1LOD, broader benefits could follow.

Regulatory and ethical challenges

Regulations complicate efforts in many jurisdictions to expand profiling beyond trading indicators, participants noted. The EU Market Abuse Regulation (MAR) has helped to overcome General Data Protection Regulation (GDPR) hurdles in many EU countries by legitimising the monitoring of emails for the detection of market abuse or insider trading. But Finland is one of the strictest regimes when it comes to the protection of employees' personal data: one participant pointed out that Finland's Act on the Protection of Privacy in Working Life, combined with its lack of any legal requirement to monitor conduct, means that opening an employee's email for such purposes could result in a two-year prison sentence.

To move ahead with profiling, the industry first needs to identify and provide legitimate reasons for accessing and processing data for this purpose, he said, and must satisfy regulatory concerns by establishing controls around privacy.

Social media accounts are rich in data that could – where regulations allow – help banks to build trader profiles, especially as consumers become more relaxed about authorising companies such as Instagram or Google to access their microphones, contact lists or locations, said Paul Liesching, director of enterprise sales at Truphone. Some organisations may be uneasy about tapping such sources even in jurisdictions where it is permitted, he said: "is there a cultural way of getting around that or addressing that?" he asked.

Participants agreed that collaboration – for example through the formation of a lobby group to engage regulators about the use of data for trader profiling – could be a helpful next step.

Several participants expressed a longer-term ambition to develop their profiling work to incorporate the conduct data available at banks and to build predictive

analytics on the back of broader behavioural profiling, although they struggled to pinpoint how long this would take. Advances in artificial intelligence or machine learning could speed up the work by enabling banks to integrate nascent capabilities – for example concerning rogue trading, follow-the-money and conduct – more effectively, one participant added.

While the use of personal data for trader profiling remains controversial, participants were more comfortable with using it to hire traders. Several participants noted that financial crime teams in banks already undergo similar checks for client onboarding, and that a degree of personal profiling – for example, using personality questionnaires – is already standard practice in the human resources department for filling many banking roles.

AI and ML: future goals and regulatory expectations

Participants focused on regulatory expectations for leveraging AI and ML in their second debate, and the extent to which such technologies would be essential for identifying future market abuse risks.

An introductory poll showed that AI, ML or NLP technologies are already routine in the surveillance operations of 30% of participants, while another 40% said they were being applied selectively. A further 10% said such technologies were being evaluated at a preliminary stage, and just 20% said they were not yet being considered at all.

Participants mostly agreed that E-communications are the most intuitive place to start applying such technologies – albeit with an emphasis on NLP rather than on pure AI or ML. One participant predicted real progress in this field in the next five years.

But applying these technologies to trade surveillance will be more difficult, and some participants questioned the value of an additional ML layer if optimisation and calibration have already succeeded in reducing the number of alerts.

Surveillance functions have much to learn here from financial crime and fraud functions where the work of applying ML to transaction monitoring, for example, is more advanced, some participants noted.

Data analytics are essential

Participants stressed that investment in data analytics was a necessary precursor to AI and ML becoming more mainstream in surveillance.

While AI will "definitely deliver benefits" in helping to identify malicious intent in E-communications and eventually voice, said Goutam Nadella, chief product officer at Smarsh, banks must take a "data science- centric approach," ensuring that data is captured the right way and stored in a single place.

However, another participant questioned whether investing in AI and ML was financially viable, given

the need for prior investments in data analytics, back testing and model risk-management components. Another suggested that data analytics currently represents better value for money for surveillance than AI and ML – an important consideration in today's cost-constrained environment – although he said he remained committed to working towards the selective use of ML and AI in the future.

Participants expect AI and ML to improve efficiency, mostly through the reduction of false positives, but also in terms of being able to spot any patterns missed by rules-based systems.

One participant said that reducing headcount costs was not a high priority as her organisation was likely to focus on improving the skills of its junior analysts if ML reduced the workloads associated with low-level

alert triage. Another noted the increased expense of hiring data scientists to support the use of AI, while a third suggested that improved alert quality might also increase workloads by triggering more escalations and investigations.

Participants noted that existing rules-based systems would run in tandem with new capabilities for some time, reducing the potential for headcount savings.

Cautiously supportive regulators

This use of both systems in parallel should reassure regulators, participants agreed. Even though many regulators are exploring AI capabilities themselves, they tend to be conservative. Explainability is also a concern among banks, especially for AI solutions.

Several participants said their discussions with regulators about employing AI and ML had been broadly positive. One noted, for example, that Japan's Financial Services Agency is vocal in its support of machine learning and is distrustful of more basic vendor tools. Another flagged a US regulatory forum last year in which attendees agreed that banks must explore new surveillance tools to optimise their operations and keep pace with growing volumes of high-frequency electronic trading.

A third participant said that some regulators were keen to understand how his bank aimed to harness new technologies and expected it to be investing in NLP, for example, within communications.

As financial institutions strive to scale up their surveillance across an ever-bigger area, "regulators are starting to understand why AI and ML can make a difference, and why it's important to stay in tune with innovation that's happening in these tools, at least in the E-comms space," concluded Nadella.

Links to content from:

smarsh®

Understanding Conduct Surveillance: A Discussion With Smarsh Product Leader Brandon Carl

A New Era of AI and Machine Learning in Compliance Tech

This information was taken from 1LoD's Surveillance Leaders Network September 2021 meeting. For more information on 1LoD please visit http://www.1lod.com