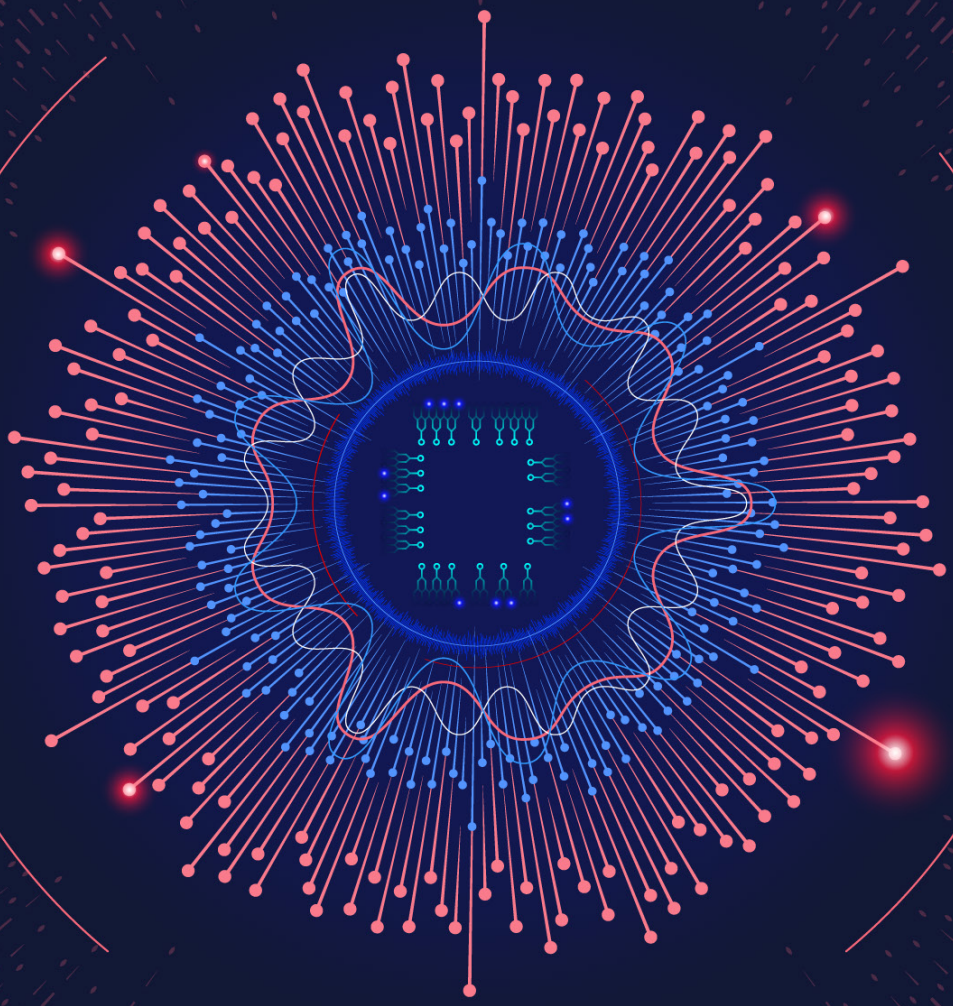
smarsh®

SURVEILLANCE:
A BIGGER BANG FOR YOUR BUCK



While banks can choose from an array of models and solutions, much of the focus is on calibration and integration, industry experts reveal at 1LoD's latest gathering of the Surveillance Leaders Network.

Industry leaders from all over the world gathered online for 1LoD's latest meeting of the Surveillance Leaders Network to discuss best practices and the use of calibration and integration in their operating models.

Calibration, an administrative burden

Banks are under regulatory pressure to invest more in surveillance, particularly for voice communications. But ensuring that such surveillance models work well is expensive, and their calibration and testing is an administrative burden. Some participants raised the question of how much value can be added from investments here, even though most leaders continue efforts to optimise such processes.

One of the participants described efforts to achieve consistency in terms of classifying parameters in order to reduce duplication and false positives. Mike Coats, Chief Technology Officer at TradingHub, one of the meeting's sponsors, suggested it could be useful to share curated sets of transactions with industry peers as this would create a larger pool for calibrating models.

Another participant proposed calibrating certain categories of clients or desks differently. Some agreed that similar offences, such as spoofing, can present differently according to the type of client, requiring banks to build more three-dimensional capabilities, so it could be useful to collaborate with regulators in order to benefit from their wider scope

Most participants agreed that risk assessments are important for demonstrating the effectiveness of programmes. One speaker discussed efforts to differentiate between types of market abuse and their relevance to individual products in order to better tailor the parameters to risk, but added that risk assessments for monitoring financial crimes are more binary in nature.

Another described how his bank has set up a global surveillance effectiveness team that cuts across trade, e-communications, transactions and anti-fraud surveillance. This is staffed with analysts from each area of surveillance who tune and calibrate scenarios according to clusters that then map back to either the market abuse risk assessment or the typology analysis of the financial crime. Improving the identification of any gaps in control in this way adds credibility during budget discussions, he added.

As banks' market abuse programmes mature, they need more objective data capabilities to show what they are calibrating and why, as well as to improve the quality and completeness of the data, strengthen their analysis of patterns and experiment with metrics. This has led to increased demand for data scientists whose skills can be put to many other uses within the same organisation — whether behavioural analysis for the human resources department, or trader profiling for compliance —and thus shared between departments and across functions. However, both banks and vendors said it was difficult to recruit and retain such skilled staff.

More banks are exploring surveillance models based on people, in parallel with those based on activity. One bank risk-ranks traders for unauthorised trading on a monthly basis, runs the report globally and tries to intercept those riskier traders using market abuse surveillance. Another is engaged in an exercise to identify higher-risk groups and is working out which data points it needs to apply. Still another participant said that fines for breaching general data protection regulations served as a deterrent.

The smarter use of technology will make surveillance more effective and cost-efficient, argued Goutam Nadella, Chief Product Officer at Smarsh, another sponsor of the meeting. Moving data capture, archiving and surveillance to a single cloud reduces fragmentation and costs, he added, while using cloud infrastructure and cloud-native software can slash data-ownership costs by as much as 70%.

Integration

Surveillance is not the only weapon in a bank's arsenal, but should be considered part of a much bigger armoury, participants said. Nadella and Coats noted that the signals for activities such as money-laundering and market abuse increasingly overlap. Coats added that integration efforts tend to be either vertical, where the data is pooled and then customised by area of expertise, or horizontal, where the data is kept in silos.

The levels of integration between financial crime, market conduct and other surveillance functions are very mixed: some banks are already advancing along this path while others either have no plans to do so or are at an early stage. The key drivers for those following this route include cost and operational efficiencies.

Data management is a big challenge for surveillance integration because large volumes of structured and unstructured data are involved across multiple jurisdictions. Several participants questioned whether the data pools at their own banks were in good enough order to be normalised and integrated: one even warned that attempting to do so could lead to missed signals. Another argued that the data associated with market abuse and financial crime are too dissimilar to be aggregated at a micro level.

Coats proposed that integrating structured data, such as financial crime or watch list data, would offer more bang for the buck, and recommended giving that priority over unstructured data, such as communications content.

The issue of data ownership also gets in the way of stakeholders working together, one participant said. Information flow between trade surveillance and financial crime teams, for example, tends to be one-way because the latter cannot reciprocate by sharing confidential information.

Bringing surveillance output together and developing target operating models in a consolidated way can be complicated by the 1LOD and the 2LOD playing different roles within the surveillance programmes. For example, one participant noted that market abuse trade surveillance is run in the compliance department at his bank, but communications surveillance is run by the 1LOD. This makes coordination rather than outright integration more achievable. Another said that while coordination between the 1LOD and the 2LOD can be difficult, it is important to aim for enterprise-wide surveillance.

One participant said his bank is focusing its efforts more on operational rather than functional or technological integration in order to improve coordination and the sharing of information. For example, if the financial crime team flags unusual money flows for a client, that information can inform trade surveillance or market abuse reviews, and vice versa.

But participants said that regulators tend to avoid giving instructions or rules on this topic and appear to be more concerned with how effectively individual surveillance programmes are designed and run than with whether or not they are integrated.

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