NICE Actimize

Datasheet

Detect Previously Unknown Suspicion

SAM Advanced Anomaly Detection

Identify unknown AML scenarios and undiscovered risky behavior with unsupervised anomaly detection, model governance included.

The Key to Complete Coverage

Rule-based models typically focus on specific transaction types corresponding to known money laundering typologies and often result in coverage gaps. Rules have their place, but they lack the ability to detect suspicious outliers or anomalous activity associated with changing or evolving criminal typologies.

SAM's advanced anomaly detection model analyzes all entities and transactions against peer and historical activity, providing you with richer suspicious activity monitoring and detection capabilities.

Discover previously unknown typologies and ensure continuous monitoring of all suspicious behavior. Advanced anomaly detection works alongside known detection scenarios to offer comprehensive and fully-compliant coverage.

What Does SAM's Anomaly Detection Do

Find Context Anomalies

SAM's anomaly detection uses an unsupervised time series anomaly algorithm to compare each customer's recent activity with their historical behavior and highlight changes in activity patterns. The contextual anomaly detection checks for both activity increases and decreases, including changes in:

- Total transaction amounts and volumes
- The spread of activity within a month
- The stable or erratic nature of activities

Pinpoint Peer Anomalies

SAM uses machine learning algorithms, such as isolation forests, to compare each customer's recent activity to peer activity across the organization and calls out behavioral differences. By performing comparisons from multiple, different perspectives, SAM's anomaly detection provides the ability to evaluate each customer relative to multiple peer groups.

Peer anomaly detection creates peer groups automatically based on account and party attributes. After initial peer grouping, the model assesses peer groups on an ongoing basis and may create additional peer groups to extend coverage and the number of discoverable typologies.

Combining context and peer anomaly detection offers these benefits:

- An entity that has been laundering money from day one wouldn't necessarily be picked up by the context anomaly model, but it would be highlighted when compared to its peers
- A context anomaly may not be deemed suspicious if all the peers are doing the same thing, so combining the two helps reduces the noise

What Distinct Situations Does Anomaly Detection Consider?

Besides identifying peer and context anomalies, the anomaly detection model also asks:

Where did the cash go?

As much as unusual increases in high-risk activity can be considered suspicious, a decrease in activity could also be indicative of money laundering. For example, a local grocery store performing regular cash deposits could become suspicious if the usual cash deposit amounts were suddenly reduced. The question would be "where did the cash go?" SAM's advanced anomaly detection model monitors both increases and decreases in activity.

Where did cash come from?

For high-risk transaction types, it flags new behavior, as that can be indicative of a first-time offender.

How Does the Anomaly Detection Model Help Reduce False Positives?

The anomaly detection model uses several strategies to minimize noise:

- It considers both types of anomalies combined to determine whether an activity is truly suspicious. This eliminates false-positive alerts derived in isolation from the context anomaly model by comparing an entity to their peers
- It prioritizes transaction types more commonly associated with money laundering over lower-risk transaction types when evaluating the risk of an activity
- The anomaly detection model continuously learns from investigator feedback on the alerts it generates, optimizing its understanding of which anomaly combinations are high risk

What Happens After an Anomaly is Detected?

After detecting an anomaly, SAM generates an issue. That issue is added to an alert, either existing or new. The alert is risk ranked based on the transaction types and the entity's risk (CDD risk), enabling you to prioritize the highest risk alerts for investigation.

NICE Actimize's predictive scoring model can be used to enhance the risk evaluation process by learning what constitutes the highest risk anomalies. It provides a score for each alert, which indicates how likely that alert is to result in a SAR based on historical findings.

Investigators review alerts in the case management system, ActOne, and can see detailed explanations on each anomaly in the alert information.

Detect Suspicious Activity Better

Gain a more effective, holistic approach to detecting suspicious activity by combining network risk analytics with a variety of other approaches, including:

- Rules
- Advanced segmentation
- Automated tuning
- Network analytics
- Collective intelligence
- Predictive scoring

NICE Actimize can work with you to build a personalized monitoring and analytics strategy tailored to your specific needs.

Model Risk Management (MRM)

Comply confidently with all the documentation you need for effective model risk management. Actimize's anomaly detection includes:

- **Model developmental evidence** describing the development approach for your various anomaly detection models. This document is written by a third party specializing in documentation for governance and MRM teams
- **Full model development reports** explaining how your models were trained using your specific data
- **Monitoring dashboards** that assess model output quality on an ongoing basis
- **Explanations** that inform the investigator during alert review on why the model flagged the entity as anomalous

Rest confident your institution is fully covered. Discover previously unknown and unmonitored suspicious activity today with Advanced Anomaly Detection.