transmit security

DATA SHEET

Enhancing Real-Time Fraud Detection with **Post-Detection Analysis**

Post-detection analysis examines historical data in batch mode to find abnormal patterns that help teams scale responses and improve real-time detection for future attacks.

While real-time detection is vital for swift responses to individual fraud attempts, cross-correlating and clustering cases can help improve models and expedite responses to coordinated attacks.

To complement its state-of-the-art real-time detection mechanism, our Research Labs team has developed a set of post-detection models that enable model enhancements, improve fraud investigation, provide insight into fraud MOs and expedite resolution of emerging and coordinated attacks.

This paper will explain how post-detection analysis delivers these benefits and enhances the immediate protection offered by real-time detection.

Benefits of post-detection analysis

Faster detection of new MOs

Confirmed anomalies found in post-detection analysis can be fed into real-time models to quickly train them on new attributes of fraudulent activity, improving detection rates for changing attack MOs.

Scalability and performance

Batch analysis of large volumes of data can leverage substantial computing resources to perform cross-correlation across accounts that would be time and cost prohibitive to conduct in real time.

Resolving campaigns & fraud rings

Cross-correlated data & clustered cases help analysts identify coordinated attacks, understand the MOs fraudsters use to execute them & determine high-impact actions that can quickly resolve them.

Real-time detection vs. post-detection analysis

Real-time detection with Transmit Security

Our AI-based Detection & Response Services process hundreds of telemetry types using multiple detection methods to pinpoint anomalies in application usage and individual behavior patterns throughout the entire end-user journey.

This critical context is used to deliver a real-time risk score and out-of-the-box recommendation to Trust, Allow, Challenge or Deny each customer request, enabling:

- **Instant response times**

  Risk scores and recommendations are near-instantaneous, allowing for immediate action and preventing fraudulent activities from causing significant harm.

- **Adaptive learning**

  Our AI models learn from real-time data so we can detect suspicious requests as they occur and provide continuous improvements to detection that reduce the need for manual updates to decisioning.

- **Automated alerts**

  Suspicious activities trigger immediate notifications to relevant parties for further investigation and intervention.

Real-time detection methods

- Network reputation
- Global intelligence
- Device reputation
- Account changes
- Event intelligence
- Behavioral biometrics
- Authentication events

How post-detection analysis enhances detection

Whereas real-time detection prioritizes speed and efficiency to help stop threats as they arise, post-detection analysis (also known as offline analysis) provides a more thorough inspection of large-scale datasets using batch analysis.

This enables fraud teams to:

- Improve detection models by correlating past events with present intelligence
- Analyze large-scale parallel events, such as a parallelized attack of 500 fraudulent attempts
- Produce model results and insights on aspects of detection real-time models haven't been trained for

Post-detection analysis capabilities

- New fraud MOs and patterns detection
- Campaign detection
- Link analysis tools
- Time-series anomaly detection
- Single pane of glass for large-scale campaigns
- And many more

Uncover fraud rings with link analysis

Today's cybercriminals are more organized than ever. Connected communities of fraudsters may distribute suspicious requests across multiple users with diversified behavior to avoid triggering detection thresholds or launder money through mule accounts to obscure the beneficiaries of illicit funds.

By correlating data across large numbers of user accounts, analysts can detect reused IPs, geolocations or devices suggestive of fraud rings or uncover patterns of rapid funds transfer across networks of connected accounts used for money laundering.

However, cross-correlating across hundreds or thousands of accounts to search for these complex patterns in real time would add significant delays that negatively impact user experience and could lead to dropoffs.

Our link analysis tools help analysts detect and document fraud rings using visual graphs of connected networks, IPs, users, devices and other data points to expedite investigation, analysis and reporting — significantly reducing the time and effort needed to pinpoint these complex connections using traditional databases.

This information can be further leveraged to better understand the fraud MOs that criminal networks are using to target your platform, enabling your team to quickly take high-impact actions to detect and mitigate these tactics.

Link analysis use cases

- **Save time on analysis** by visualizing fraud ecosystems rather than manually scanning users or querying databases
- **Pinpoint mule accounts** that are used to transfer funds to illicit accounts
- **Share intelligence more efficiently** with auditors and internal stakeholders
- **Expedite KYC/AML reporting** for money laundering
- **Spot synthetic identities** where fraudsters reuse or share IPs, devices or other data to open multiple accounts
- **Find users closely linked to known fraudsters** and quickly block them
- **Understand fraud MOs targeting your business** by visualizing interconnected fraud networks

Rapidly respond to fraud campaigns

Coordinated campaigns waged by fraud networks require swift mitigation to prevent substantial losses, but the significant computing resources needed to process large numbers of parallel events can cause delays during real-time detection.

In addition, prioritizing strategies to mitigate campaigns can be difficult without a way to quickly visualize information related to the attack, especially when similar cases or alerts must be reviewed one by one in order to gain insights into the campaign.

With offline analysis to process large-scale parallelized events and a single pane of glass to understand the scope and attributes of campaigns, Transmit Security enables rapid detection and resolution of large-scale attacks. With it, analysts can:

- **Understand the timing and sequence of events** to better distinguish between campaigns and isolated anomalies
- **Cluster alerts by levels of similarity** and filter recommendations by campaign ID to detect campaigns faster, uncover related cases and reduce the need to review cases one by one
- **View the top deny reasons** for recommendations in order to understand the MOs used to wage fraud campaigns and determine high-impact actions that can be used for fast mitigation

Streamline tuning with time-series anomaly detection

Fraudsters often build up synthetic identities through months or even years of legitimate behavior before weaponizing that trust to make massive transactions on their accounts.

With time-series anomaly detection, fraud analysts can pinpoint outliers or unusual patterns based on batch analysis and correlate current intelligence with past events to improve post-mortem investigations and pinpoint false negatives. This helps AI models to better detect patterns of synthetic identity fraud and other hard-to-spot anomalies in real time.

To expedite tuning, false negatives can be quickly and easily labeled directly in the UI or using our Labels API, which requires only two inputs — the subject and label type, such as "known malicious" — to tune recommendations using a single API call.

Synergy between real-time detection and offline analysis

In the battle against fraud, the collaboration between real-time detection and offline analysis is key. Transmit Security helps fraud teams harness this synergy with a rich set of tools for offline analysis and daily updates to our real-time detection algorithms based on confirmed anomalies and deviations uncovered in post-detection analysis — giving fraud teams the fastest and most accurate protection against changing tactics.

To learn more how Transmit Security helps enterprises improve detection and save millions in fraud losses, view our case study on how a leading bank achieved 1300% ROI with our Detection & Response Services.

About Transmit Security

Transmit Security provides modern tools for businesses to create secure digital identity journeys. With a CX-focused approach, their CIAM platform ensures smooth, fraud-protected experiences across channels. Trusted by major brands, Transmit serves industries responsible for over $1.3 trillion in annual commerce.
Learn more at www.transmitsecurity.com.