



Case Study: IRSF Detection

Onyx FMS Implementation for Bité Group

Background

Bité Group is a leading telecommunications and media group in Lithuania, Latvia, and Estonia. Among other subsidiaries, Bité Group controls two mobile network operators: Bité Lietuva in Lithuania and Bite Latvija in Latvia. Elitnet has been providing Bité with various telco software solutions since 2005, including telecom application servers, value-added services, and data analytics applications.



Challenge

According to the Communications Fraud Control Association's (CFCA) global Fraud Loss Survey, International Revenue Share Fraud (IRSF) has been causing the most losses among all fraud types to communications service providers for a number of years. As of 2021, it has still been named as the number one fraud type faced by telcos both in the home network and roaming.

IRSF is a fraud type which involves a fraudster teaming up with a high termination rate CSP which shares the interconnect fee with the fraudster, while the fraudster implements artificial traffic generation to high termination rate numbers. Typically, it uses hijacked SIM cards or devices, PBX hacking, Wangiri scam, and mobile malware to generate the fraudulent traffic.

To combat IRSF, Bité was using a system based on counters of the quantity and total duration of calls which raised alarms whenever a certain counter was exceeded. Due to a large variety of constantly changing IRSF patterns, configuring counters which would ensure a high recall rate and an acceptable fraud window while keeping false positives to the minimum was a challenging task despite high expertise of Bité's fraud managers. The previously used method was also slow to react to changing IRSF patterns, as new patterns had to be thoroughly investigated before a new optimal counter value could be determined.

As a result, Bité was in the market for a solution which would deliver a high precision and recall rate when detecting IRSF cases, ensure a short fraud window while maintaining a low number of false positives, and be able to adapt to new, previously unnoticed IRSF patterns.

#1

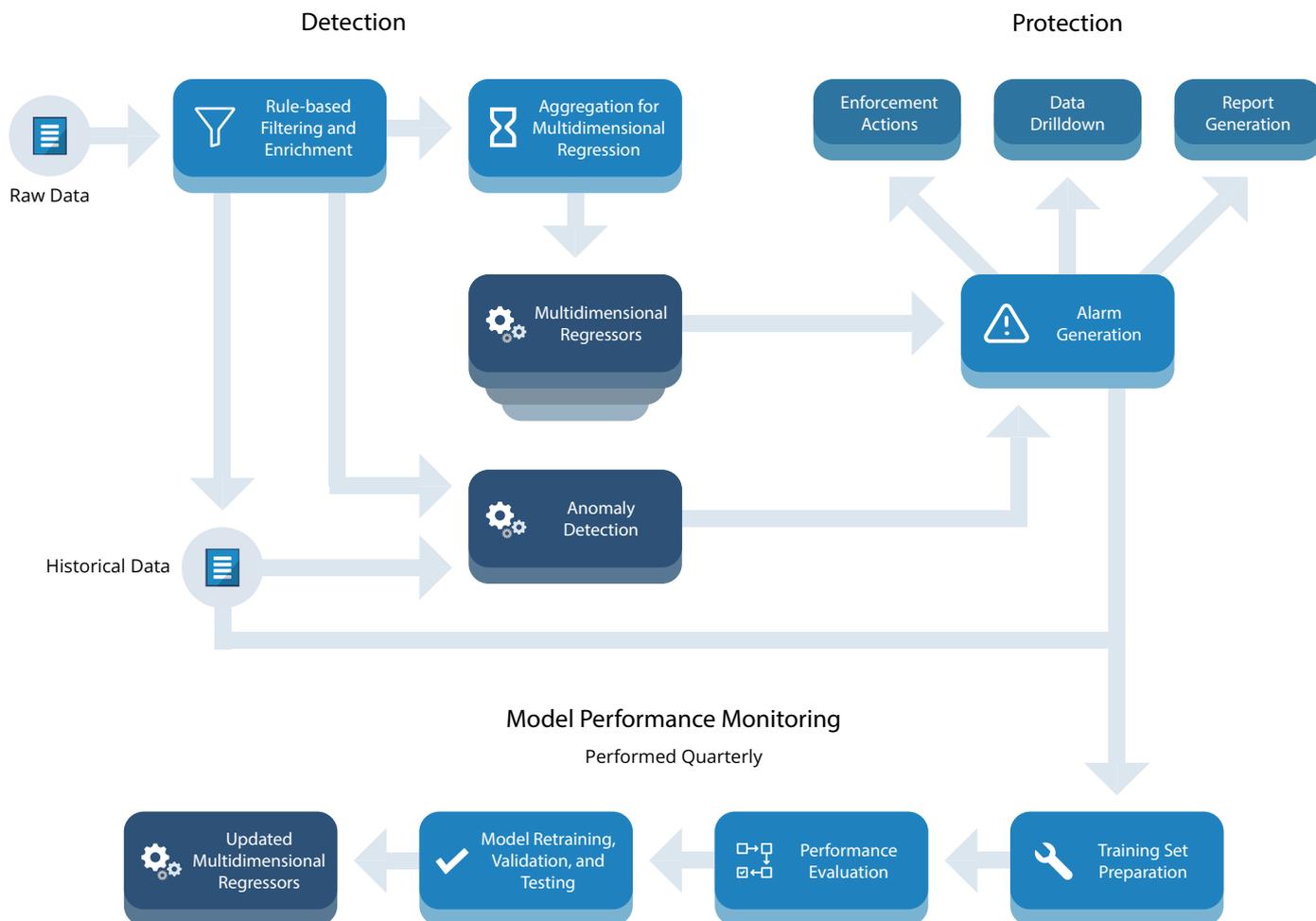
Fraud type causing losses according to carriers

\$6.69B

Estimated annual global loss due to IRSF attacks

Approach

To detect and prevent IRSF and other fraud types, Elitnet proposed to provide Bitè with Onyx Fraud Management System (Onyx FMS). To carry out real-time fraud prevention, Onyx collects data from various sources in the network and carries out data processing and analysis using both rule-based and Machine Learning (ML) methods. Data processing results are then used to provide statistics and reports, carry out fraud case management, generate alarms and notifications, and prompt other network components to take enforcement actions.



Onyx uses a hybrid approach including rule-based and ML methods (classification and clusterization) to detect IRSF cases in both outgoing and transit calls. To ensure maximum performance of the solution, it carries out pre-aggregation as well as rule-based filtering and enrichment of raw data before passing it on to the Machine Learning components. Onyx can detect IRSF cases in static directions such as destination countries as well as dynamic directions such as a thousand of MSISDNs.

Onyx employs multidimensional regressors which use data aggregated for different dimensions, or periods of time. This allows to achieve a high recall rate for different attack patterns while maintaining a short fraud window and a low number of false positives. The resulting regression numbers are converted to alarms with certain severity levels based on rules. Once alarms are generated, Onyx can carry out enforcement actions such as blocking attacks with a high severity level. Fraud managers also have full access to reports and data drilldown for any particular IRSF cases.

To ensure that the multidimensional regression ML model is up-to-date with new types of IRSF cases, it is re-trained quarterly based on past alarms produced by the anomaly detection component and the rule engine as well as other performance evaluation tools.

The anomaly detection component works in parallel with the multidimensional regressors to detect previously unknown IRSF patterns. It uses clusterization methods to look for anomalies in static directions, such as destination countries, and reports any unusual behavior which might indicate a new fraud pattern.

Results

Compared to the rule-based system previously used by Bitè, Onyx allowed the operator to significantly decrease the fraud window for the IRSF attacks taking place, as real-time data collection and hybrid rule and ML-based approach to fraud detection allowed Onyx to detect fraudulent patterns in a substantially shorter time-frame.

The multidimensional approach to data aggregation and processing enabled Bitè to detect and block a large number of IRSF attacks which would have been undetected by the solely rule-based system, including both high-intensity short-term attacks and low-intensity long-term attacks. Recall and precision rates were increased while false positive rates were kept to the minimum.

The system formerly used by the operator required constant management of counters to ensure that any new IRSF patterns are detected. In contrast to that, Onyx's anomaly detection capabilities enabled Bitè to detect new, previously unknown IRSF patterns without any input required from fraud managers. All of the above advantages of Onyx compared to the previous system allowed the operator to considerably reduce fraud-related losses.

The following results were achieved by Onyx when detecting IRSF attacks:

97%
Recall

95%
Precision

The main advantage which we have noticed after implementing Onyx is the significantly decreased fraud window for IRSF attacks. Even smaller attacks are detected earlier compared to the previous system, allowing us to substantially decrease losses caused by IRSF.

IRSF and other fraud prevention modules implemented with Onyx FMS have provided us with significant improvements in fraud detection, analysis, and prevention.

- Indrè Bobraitienė, RA Manager, Bitè Group

In addition to fraud detection and prevention, Onyx is a very valuable reporting system for business intelligence and revenue assurance. It also opens up new possibilities for device classification, predictive maintenance, and other promising solutions.

- Jonas Milerius, Head of Roaming, Interconnect & Fraud, Bitè Group

ELITNET

 www.elitnet.eu

 info@elitnet.eu

 +370 37 352706

 UAB Elitnet
Pasiles 102, LT 51314
Kaunas, Lithuania