ELIT NET

Onyx FMS

Real-time Hybrid Fraud Management System for CSPs

According to the Communications Fraud Control Association (CFCA), the estimated global fraud loss for communications service providers reached $28.3 billion in 2019. This includes various cases of fraud carried out against either CSPs or their subscribers, such as IRSF, bypass fraud, subscription fraud, roaming fraud and others.

Although global fraud loss has been on the decrease due to the providers' ability to prevent some of the most common cases and increased regard for cyber security, fraudsters and scammers have also been improving their methods to profit from CSPs and subscribers alike.

To address the ever-changing threats to CSPs and their subscribers, a hybrid approach which connects traditional rule-based methods and state-of-the-art Machine Learning (ML) applications is necessary.

Elitnet's **Onyx Fraud Management System** (Onyx FMS) is a real-time hybrid system for combatting fraud in telecommunications networks. The system detects and prevents various types of fraud in real time, reducing the fraud window, maximizing cost savings, and ensuring continuous quality of service.

Onyx collects data from various points in the network and employs a rich set of methods for fraud detection ranging from rational rules on aggregated counters and signaling pattern recognition to ML-based anomaly detection, traffic and subscriber classification, and real-time stream analysis.

Onyx FMS is capable of detecting and preventing the following telecommunications fraud types:

International Revenue Share Fraud

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

Interconnect Bypass Fraud

Interconnect bypass fraud mainly includes CLI replacement and SIM box usage. It allows fraudsters to profit from the difference between low and high call termination rates. Another case of interconnect bypass fraud is OTT bypass, where calls are terminated via OTT applications such as SkypeIn without paying the termination fee to the communications service provider.

Wangiri Fraud

Wangiri or callback fraud involves execution of short-duration calls from premium-rate numbers with the intention to initiate a call-back from the subscriber. Real-time call data analysis allows to detect and block these attacks in an early phase.

Subscription Fraud

Subscription fraud results in an attacker impersonating a subscriber by hacking or cloning a SIM/eSIM or injecting malware into the victim's device with an intention to make a large number of premium-rate calls or messages or subscribe to various services.

Roaming Fraud

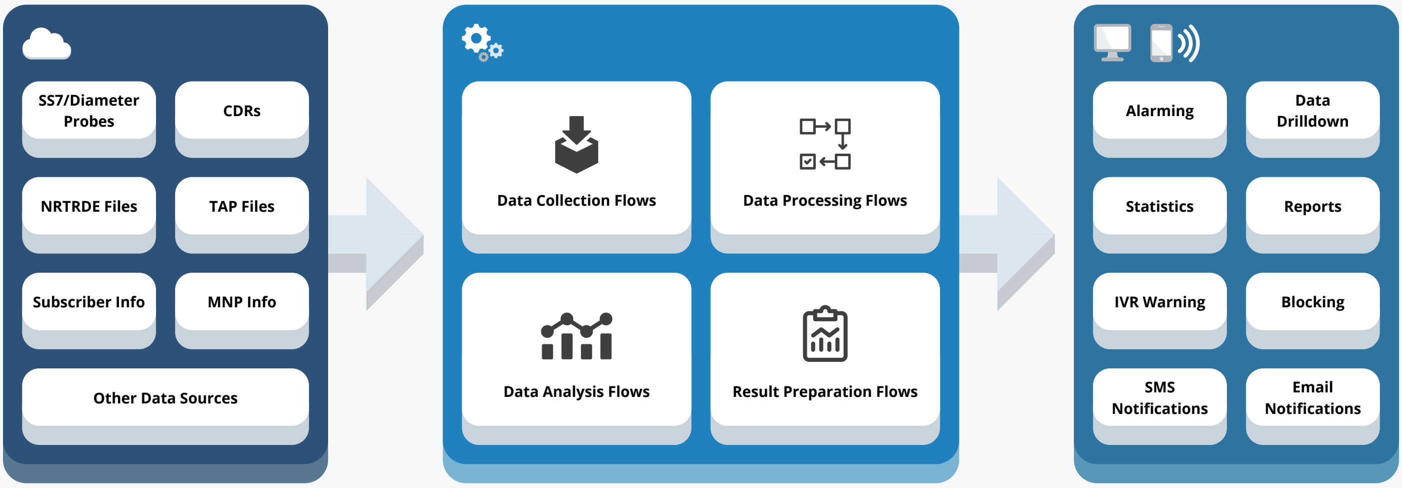
Roaming fraud involves fraudulent actions carried out using SIM cards in roaming, including CLI replacement, high-cost international revenue share calls, and emulation of user registration abroad with a purpose to intercept calls or deny service.

Other Fraud Types

Rule-based methods as well as AI/ML-based methods such as anomaly detection are also used to detect other types of fraud as well as new previously undetected ways to defraud the communications service provider and its subscribers.

The Onyx FMS Approach

Onyx FMS consists of three key types of components: data collection components, data processing and analysis components, and reporting and enforcement components.



The system gathers data from various points in the network in real time or near real time, including CDRs/SDRs, SS7/Diameter messages, NRTRDE files, subscriber information, and other types of data. The collected data is then processed using various methods, each of which is used for detecting specific types of fraud:

Pattern Recognition

The pattern recognition method is based on rules which describe fraud patterns in the form of signalling message (including SS7 and Diameter) sequences.

The rule engine allows detecting fraudulent and malicious activities taking place on the network, including illegal subscriber location detection, attempts to intercept SMS messages or record calls, as well as SS7 message sequences which realize denial of service (DoS) attacks against network infrastructure elements.

Onyx allows flexible configuration and expansion of the active rule set. The patterns of newly discovered attacks and associated rules may also be obtained from a centralized rule/pattern database.

Rational Rules

Onyx FMS uses fully configurable rational rules based on quantitative ratios for fraud detection. Rules are described using metadata (aggregated counters), functions, and logical expressions.

Machine Learning

ML-based methods allow detecting new fraud types and manifestations, adapting to specific operator data, and minimizing false positive rates while maintaining maximum recall rates.

Onyx uses ML methods such as classification and clusterization to detect atypical fraud cases without a clear, previously known pattern which may be described by rational or signalling sequence rules. For example, this ensures precise detection and prevention of new types of Wangiri attacks.

Anomaly detection, including subscriber behavior anomalies and trunk traffic anomalies, allows detecting new international revenue share fraud schemes as well as subscription frauds, such as injection of malware into a subscriber's device.

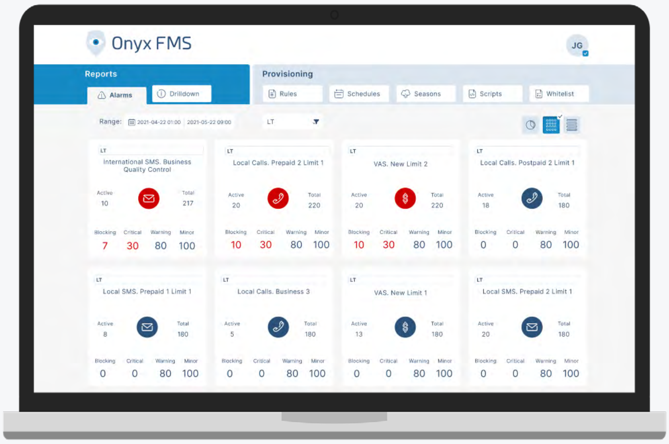
Stream Analysis

Onyx carries out filtration of potential targets which show signs of a CLI replacement fraud and executes voice stream analysis for these targets to confirm whether a fraud is taking place.

Data stream analysis is used to apply ML-based classification for recognition of OTT bypass fraud cases, such as usage of SkypeIn and other OTT services to terminate calls.

When fraud cases are detected by Onyx, the system uses its reporting engine, alarm facility, and enforcement engine to carry out further actions.

- **Reporting Engine.** Onyx's powerful reporting engine includes statistical reports, revenue assurance functionalities, and individual fraud case drilldown, all accessed via a sophisticated graphical user interface (GUI). Onyx GUI also provides users with a rich set of tools for system management and configuration.
- **Alarm Facility.** Onyx's alarm facility ensures that fraud managers are alerted about fraud cases depending on their preferred configuration. All alarm types and lifecycles are fully configurable.



Range: 2021-04-22 01:00 2021-05-22 09:00 LT

LT International SMS. Business Quality Control: Active 10, Total 217; Blocking 7, Critical 30, Warning 80, Minor 100

LT Local Calls. Prepaid 2 Limit 1: Active 20, Total 220; Blocking 10, Critical 30, Warning 80, Minor 100

LT VAS. New Limit 2: Active 20, Total 220; Blocking 10, Critical 30, Warning 80, Minor 100

LT Local Calls. Postpaid 2 Limit 1: Active 18, Total 180; Blocking 0, Critical 0, Warning 80, Minor 100

LT Local SMS. Prepaid 1 Limit 1: Active 8, Total 180; Blocking 0, Critical 0, Warning 80, Minor 100

LT Local Calls. Business 3: Active 5, Total 180; Blocking 0, Critical 0, Warning 80, Minor 100

LT VAS. New Limit 1: Active 13, Total 180; Blocking 0, Critical 0, Warning 80, Minor 100

LT Local SMS. Prepaid 2 Limit 1: Active 20, Total 180; Blocking 0, Critical 0, Warning 80, Minor 100

- **Enforcement Engine.** The enforcement script engine ensures that as soon as a fraud attack is detected, Onyx sends out the necessary information to other network nodes to ensure that all further attack consequences are prevented.

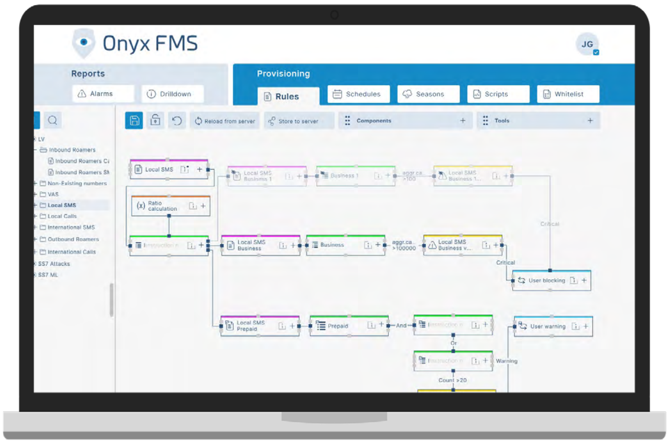
  For example, if a Wangiri attack is detected, the subscribers calling back to the numbers associated with the attack may be warned using IVR before connecting the call. This allows the CSP to minimize fraud-related losses in addition to maintaining quality of service and ensuring a positive subscriber experience.
- **Rule Designer.** For rational and pattern recognition rules, Onyx also comes with an intuitive rule designer which may be used to configure and update existing rules as well as easily create new ones based on statistical analysis and data drilldown.

Key Onyx FMS Features

Autonomous Fraud Prevention Lifecycle Management

Onyx provides fraud managers with a rich set of tools for in-depth analysis of the data collected by the system, including drilldown of individual fraud cases, allowing them to discover atypical fraud manifestations taking place in the network.

This analysis may then be used to design and configure a set of rational and pattern recognition rules which would allow detecting and preventing any future cases of these fraud types.



For ML-based components, a periodical model performance evaluation and retraining is carried out to ensure that the model is always capable of detecting the currently prevalent fraud attack types.

Proactive Real-time Fraud Prevention

Onyx can carry out predefined automatic actions to ensure that a fraud attack is stopped as soon as it begins, minimizing the fraud window. Onyx's anomaly detection components allow reliable detection of previously unknown fraud schemes and attack types.

All Onyx components are clustered to ensure high availability and zero downtime during maintenance, allowing 24/7 protection of the CSP and its subscribers.

Openness and High Integrability

Onyx's standardized interfaces allow smooth integration with new data sources as well as development of new data processors which may be created in Java, Python, or Scala using integrated libraries for ML tasks. Onyx can also be seamlessly integrated with existing Big Data infrastructure.

Investment Reusability

Onyx's architecture allows implementation of additional off-the-shelf and newly designed applications and use cases. The same platform can be utilized for other tasks such as predictive maintenance, network security, and device classification.

www.elitnet.eu

info@elitnet.eu

+370 37 352706

UAB Elitnet
Pasiles 102, LT 51314
Kaunas, Lithuania