Centaur

telbit

With the on-going all-IP migration and the introduction of new services and platforms, telecommunications fraud exposure is becoming increasingly high. In this reality, Telecommunication operators depend on experienced fraud analysts and efficient Fraud Management Systems (FMS) to minimize fraud losses.

Telbit's **Centaur** is a state of the art FMS, specially designed for Telecommunication operators that require **fast integration** of their current and new coming services and platforms with the FMS, for optimal service coverage in a natural and efficient way.

Centaur is truly unique due to the combination of three factors:

- Best-of-breed FMS that provides a **holistic risk management** approach;
- **Premium support** where dedicated teams are always available to help you, providing high standard and fast services;
- **Low-cost** commercial proposition that is tailored to your real needs assured either in the installation or support phases.
  No hidden-costs with us!

Features

INTEGRATION

- **Integration of all relevant data sources**, mainly: switches, Transferred Account Procedure (TAP), VoIP, platforms (SMSC, MMSC, NGN), subscriber information (pre-paid and post-paid), billing information, commercial information and others;
- **Aggregation of several data inputs** which allows a optimized business view for fraud detection and analysis;
- **Near real-time call processing**;
- **Built-in rating engine** capable of replicating any real world tariff plan.

DETECTION

Covers **all fraud types**: subscription, technical, dealer and internal.

Pre-built detection processes for:

Subscription Fraud:
- Aggregated High Usage for all traffic sources by MSISDN, account or fiscal number;
- High Usage per specific traffic sources: e.g. Roaming/GPRS/3G/PRS/VoiceMail;
- Differentiated thresholds for specific group of customers;
- Sliding window approach that will closely monitor every new MSISDN/account/fiscal number until it pays a certain amount/number of invoices;
- High Risk countries/cells/PRS;
- Black Lists (IMSI, IMEI, MSISDN, PREFIX);
- Highly advanced prioritization mechanism that will assure that fraud analysts will tackle the real important alarms;
- Support of email High Usage Reports.

Technical Fraud:
- Non-existing Subscribers;
- Call Velocity and Call Collision;
- SMS Call Back services;
- Denial Of Service (DOS) Attacks;
- Long/Short calls;
- SPAM - Unsolicited Bulk Messaging;
- Interconnect Fraud;
- Strange Number Patterns ;
- Traffic Pattern Deviations and Trend Analysis by virtually any traffic source or field (e.g. international prefix, SMSC, cell, MSC, APN, etc);
- Abusive SMSC usage;
- NGN Anomalies (e.g. negative balances).

Dealer Fraud:
- Box splitting;
- Subscription fraud levels per dealer;
- Ghost SIM cards/accounts.

Internal Fraud:
- PABX Abuse;
- HLR abuse;
- IT systems abuse (e.g. grant special credits or access confidential information).

Technology:
- Detection process that can use and correlate virtually **any source of data** (CDR, EDR, logs), with any other data sources such as client, revenue assurance, billing and commercial data;
- **User definable detection processes** using a simple built-in wizard;
- Time windows:
  - sliding time windows mechanism with duration and overlapping configuration;
  - multiple time windows configuration for each detection process;
  - user customizable thresholds for each time window;
- **Artificial intelligence** detection using signatures, fingerprinting and profiling.

ANALYSIS AND MANAGEMENT

- **Revolutionary** user interface that guides the analyst to the finest details of the data related to each alarm;
- **Prioritization** mechanism for focusing analyst's attention on more critical alerts;
- Support of Email and SMS **alarm forwarding** based on user defined rules (e.g.: prioritization level, time, day of week, etc);
- Appealing management and configuration user interface wide range of graphics for easy analysis;
- **Built-in Case Manager** that ensures a centralized analysis platform and knowledge base for improved management of future fraud occurrences;
- **Risk based credit control** based in defined thresholds combined with customer payment/traffic behavior.

Architecture

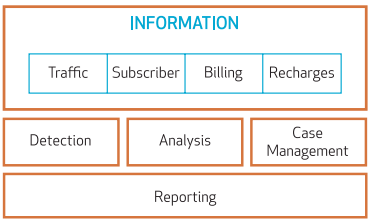
Centaur was designed taking into careful consideration the most relevant aspects of fraud management in a telecom operator.
It's common for a medium size operator to perform two or three upgrades a year on each service platforms or network elements resulting in CDR format changes. **Centaur** has an internal unified CDR format for each service type (voice, sms, data, mms, etc.) that abstracts the specificities of the underlying original records and thus guaranteeing system continuity over continuous network upgrades.

Most telecom operators have a wide range of independent systems and platforms from several distinct vendors and each of them has its own place in a revenue chain or business process. Valuable information stored in these systems could be used by fraud analysts to narrow suspects, raise new alarms, or help to make a final fraud decision. With this in mind, **Centaur** was built with a rich analysis environment that concentrates all the relevant information that can be retrieved from the operator's Operation Support Systems and Business Support Systems. This approach allows the analyst to be focused on a single application but retain global access to information.

Highly skilled fraud management professionals, tend to be disappointed by traditional FMSs, since they don't provide real control over the definition of each individual detection processes. With **Centaur**, the analysts can imagine and customize new detection processes, based on several interrelated date sources within a few minutes. This approach is so powerful that most built-in detectors are configured this way upon deployment, using several available detection templates.

Fraud management is a complex activity that normally requires very experienced professionals. With **Centaur**, even the most difficult analysis can be made in a simple way and is available to a wide range of professionals, lowering operational costs. Besides its simplicity, **Centaur** also has a **customizable prioritization** mechanism that sorts alarms according to their expected risk, focusing the analyst's attention primarily on the more critical alarms.

One of the most frequent limitations of traditional FMSs is the narrow scope of entities (IMSI or MSISDN) that can be targeted for analysis. **Centaur** can monitor, group and launch alarms over virtually any entity (IMSI, MSISDN, IMEI, CELL, DEALER,...) over a variety of information sources.



Centaur Architecture

Centaur is designed to be a fully scalable solution, ranging from low end single server systems to high end multiple distributed server platforms.

Benefits

- **Centaur** clearly pinpoints unwanted fraudulent activities from your subscribers, dealers, partners and employees;
- **Centaur** gives a clear view of these activities, simplifying analysis and aiding the decision making process;
- **Centaur** actively prevents fraud occurrences on all monitored services and platforms in near real-time;
- **Centaur** evolves naturally and in synch with customers systems and business needs;
- **Centaur** gives telecom's the independence to create their own detection processes;
- **Centaur** provides valuable fraud effort metrics, like **average avoided revenue loss** and **overall detection efficiency**;
- **Centaur** guarantees the best value for money solution, it is a low-cost system featuring all proven fraud detection and analysis technologies;
- **Centaur** contract negotiation is clear and straight, your solution is built with your own needs and budget in mind, no hidden costs nor unexpected extra modules;
- **Centaur**'s support and development team is dedicated to you and guarantees premium service, from Operations and Management to Custom Development and even Fraud Advisement and Consulting.

Centaur is developed by Telbit in partnership with PT Inovação (Portugal Telecom R&D).