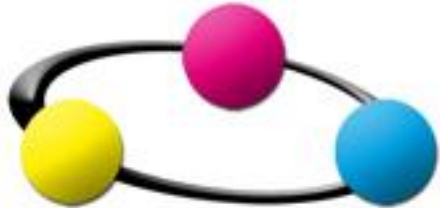


SECURITY



SUMMIT

Oracle Community For Security

Security Summit 2010

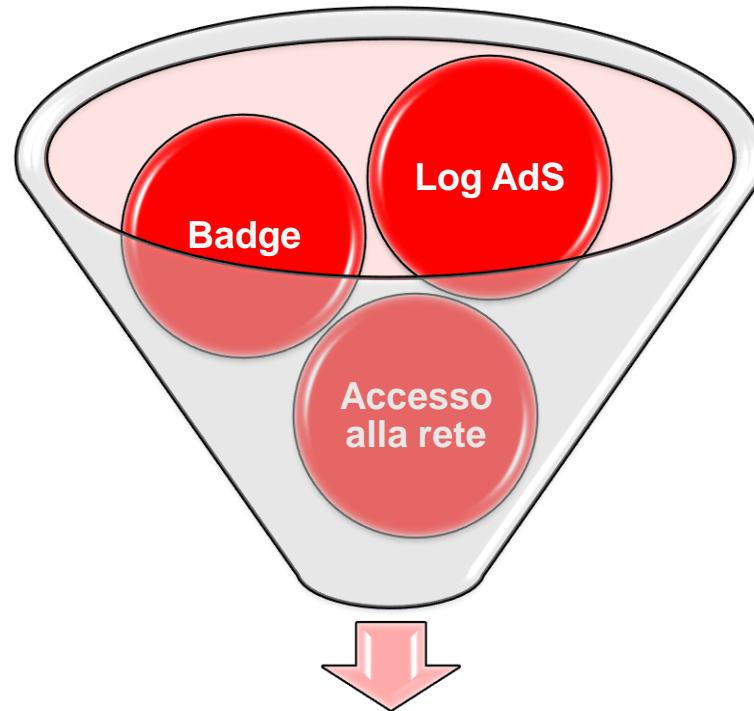
Frodi interne: la gestione dell'incidente – Wilmana Malatesta
Visiant Security



Indice

- Eventi Fraudolenti
- Aspetti legali delle frodi
- Le frodi interne
- Le trappole
- Il fraud gate

Le informazioni



Cosa nascondono ?

Tipologie di eventi

Possono dipendere:

- Dal tipo di accesso
- Dal tipo di vulnerabilità
- Dal tipo di terminale utilizzato
- Dagli obiettivi del frodatore
- Dall'interlavoro di reti/operatori differenti
- Dai protocolli di segnalazione di rete

La raccolta più completa e sistematica delle famiglie di frode viene effettuata dalla FIINA (Forum for International Irregular Network Access)

La produzione ed il dispacciamento dei Fraud Alert viene effettuata settimanalmente dal CFCA (www.CFCA.org)

Frode da Insider

- Vendita di informazioni relative a clienti ai competitor
- Attivazione di “ghost phones” o Servizi “Non Fatturati”
- Rimozione non autorizzata di somme dalla fattura, o rimozione di limitazione ad alcuni servizi

Frode da Dealer/Reseller

- Accettare consapevolmente false generalità per ottenere la commissione
- Accettare consapevolmente la non solvibilità di un cliente
- Offrire promozioni/sconti a persone che non ne hanno diritto
- Attivazione di servizi a defunti

I riferimenti legali

Legge 547 del 23/12/1993

- Art 491 bis del c.p. (*Falsità in documenti informatici*)
- Art 616 del c.p. (*Violazione della corrispondenza*)
- Artt. 617 quater. Quinquies, sexties (*Le comunicazioni informatiche o telematiche*).

Legge 48/2008

- Art. 615-quinquies (*Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*)
- Art. 635-bis (*Danneggiamento di informazioni, dati e programmi informatici*).
- Art. 635-ter (*Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità*).
- Art. 635-quater (*Danneggiamento di sistemi informatici o telematici*).
- Art. 635-quinquies (*Danneggiamento di sistemi informatici o telematici di pubblica utilità*).
- Art. 640-quinquies (*Frode informatica del soggetto che presta servizi di certificazione di firma elettronica*).
- Art. 24-bis del D. lgs. 231/01 (*Delitti informatici e trattamento illecito di dati - introdotta da 48/08*)

Provvedimento del Garante della Privacy sugli Amministratori di Sistema

Le frodi interne

- Processo di Fraud Management per le frodi interne
- Mappature delle utenze e delle abilitazioni e dei ruoli
- Gestione delle abilitazioni/disabilitazioni in caso di variazioni (traslochi, cessazioni, assunzioni, ruoli)
- Tassonomia delle frodi interne
- Criteri per la detection
- Prevenzione (Verifica periodica)
- Liste di inclusione /esclusione
- KPI per le frodi interne

Cooperazione tra aziende del gruppo

La cooperazione va costruita e stimolata, in relazione ad aspetti di contrasto, almeno per:

- Frodi intra-gruppo
- Alert in caso di nuovi meccanismi
- Alert in caso di fenomeni che riguardano altre società del gruppo

E' necessario avere come riferimenti base per tutto il gruppo:

- Una terminologia delle frodi coerente con quella internazionale
- Una tassonomia delle frodi
- Modelli economici condivisi per la valutazione del danno in ciascun tipo di frode

Obiettivi

- Avere una vision cross-company del fenomeno fraudolento
- Garantire un reporting periodico dei danni da frode
- Assicurare un approccio metodologico omogeneo e coerente e sviluppare un ambito di riferimento
- Identificare le best practices e farle diventare patrimonio del gruppo intero
- Monitorare e coordinare le scelte strategiche a livello tecnologico, investigativo
- Promuovere e coordinare la cooperazione intracompany/intragruppo per conseguire il massimo dell'efficacia
- Creare un riferimento operativo per le frodi cross-company e cross-border
- Monitorare, raccordare e indirizzare la partecipazione agli organismi nazionali ed internazionali per conseguire massima efficacia ed efficienza

Elementi per un tentativo di definizione

- Attori potenziali coinvolti nella frode
- Frodatori e frodati
- Danno e danneggiati
- Frode ed intenzionalità
- Responsabilità
- Conseguenze a livello operativo nella gestione di una frode: denunce, storni, note di diminuizioni, perdite, danno di immagine
- Dimostrabilità
- Quantificazione del danno
- Migrazione esterna (da un operatore all'altro)
- Migrazione interna (da un segmento di mercato all'altro)
- Caratteristiche cross-border

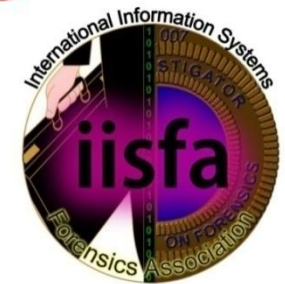
Le trappole giuste

- Screening dei clienti e dei servizi
- Regole di analisi del traffico su base relazionale sintomi-meccanismo di frode
- Consumi oltre soglia solo:
 - Come complemento di informazione
 - Per accertare la consapevolezza del cliente in relazione al traffico svolto
 - In caso di meccanismi non noti e non monitorati

Fraud testing Analysis

Test Proattivi: Visiant Security vanta anni di esperienza nelle attività di Penetration Test anche black box. In ambito frodi, testiamo i nuovi strumenti/servizi rilevando tutte le vulnerabilità di sistema o di processo che possono permettere la realizzazione di una frode.

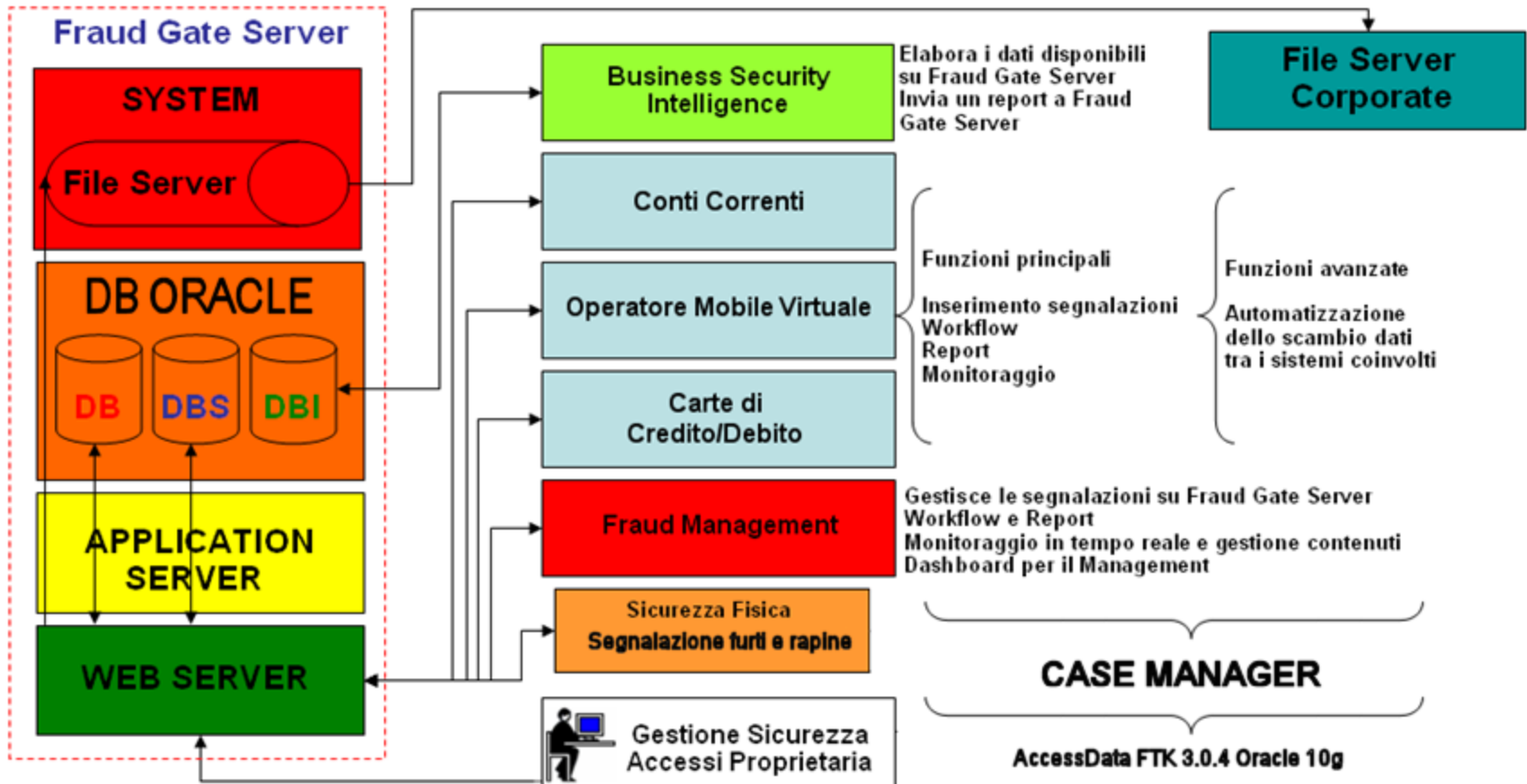
Significa che possiamo collaudare un sistema, applicazione, un processo, in ambito sicurezza e prevenzione frodi. Visiant Security vanta personale certificato e costantemente aggiornato nelle attività di Analisi del Rischio (Piani di Sicurezza, Compliance, ecc.).



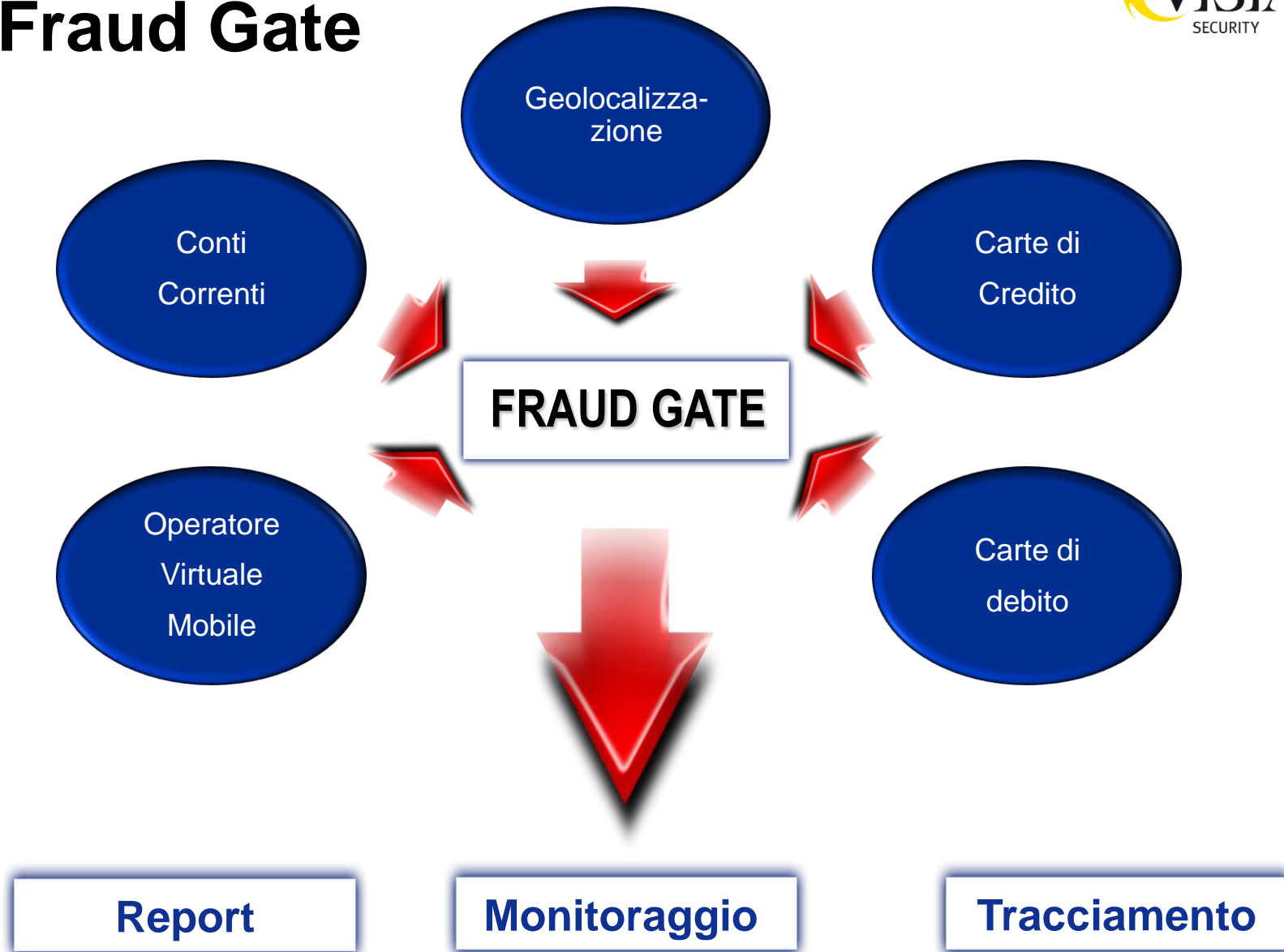
Fraud Gate

Sistema nato per contrastare le nuove frodi verso i servizi VAS Distintivi tramite Operatore Virtuale Mobile. Il portale supporta tutte le funzioni operative del Fraud Management, viene utilizzato da tutti i reparti che inviano le segnalazioni al Fraud Management, permette così la conservazione di eventi vitali per la prevenzione frodi. Il Fraud Gate fornirà un avanzato sistema di monitoraggio e reportistica personalizzato per ogni struttura coinvolta .

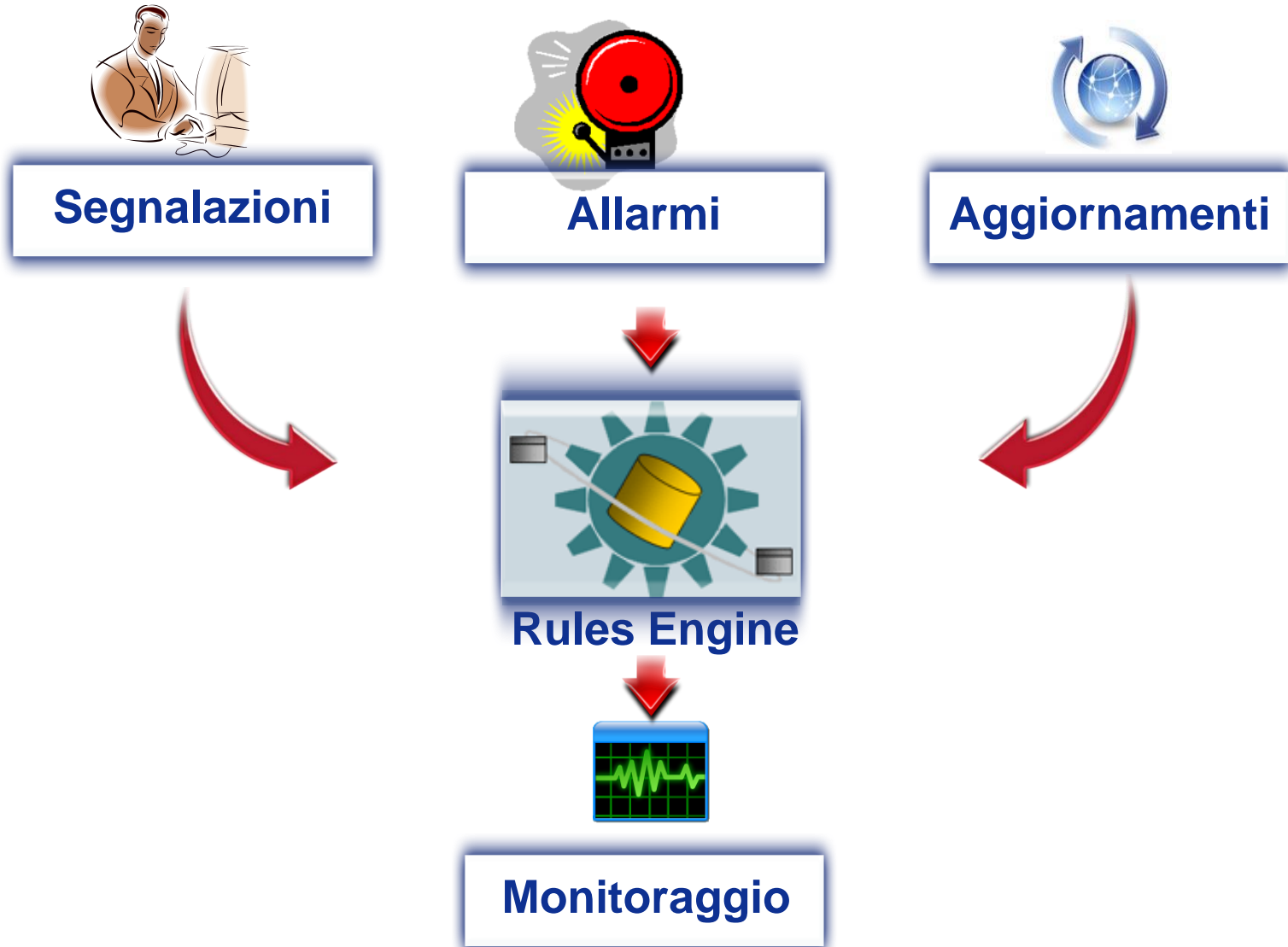
Fraud Gate



Fraud Gate



Fraud Gate



Fraud Gate

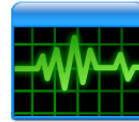
Applicazione della Classificazione della Frode anche in caso di solo sospetto (anomalia). Vengono così gestite e smarcate subito quelle classificate ad impatto critico.

Applicazione della Classificazione della Frode.



Il motore elabora tutti i dati basati su regole definite, linkando tutti i dati utili, come ad esempio operazioni riconducibili ad uno stesso Cellulare o un determinato IP, ma anche qualsiasi dato riconducibile al soggetto che ha effettuato operazioni di frode anche sospetta. Il monitoraggio visualizzerà inoltre anche tutti i dati correlati con gli altri casi.

Fraud Gate



Monitoraggio

MONITORAGGIO REALTIME

Prima

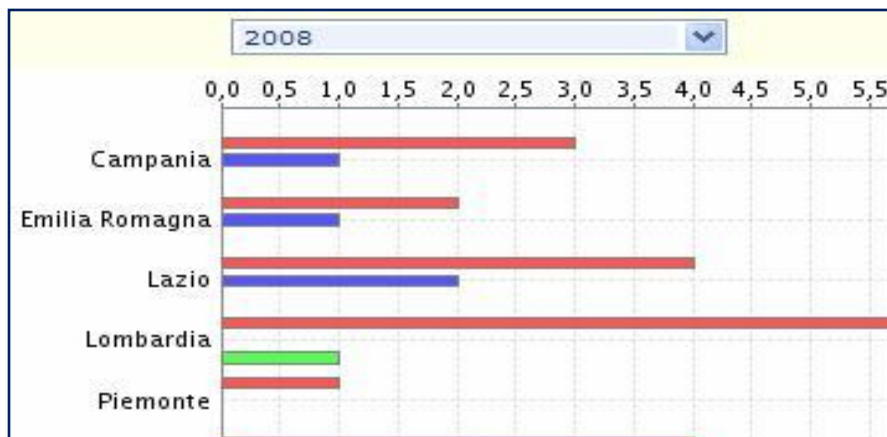
Il monitoraggio delle segnalazioni avveniva manualmente previa elaborazione dei dati che i sistemi e gli operatori inviano via e-mail.

Questo non permette di avere il polso della situazione in tempo reale.

Con Fraud Gate

Il sistema Fraud Gate è stato progettato per visualizzare vari tipi di monitoraggio sui dati aggiornati: un motore a regole dinamiche carica i dati, li elabora correlandoli con altri database assegnando lo scoring delle criticità rilevate. All'accesso dell'utente il Fraud Gate visualizza grafici dinamici ed evidenzia le segnalazioni in modo diverso in base alla criticità rilevata

Fraud Gate



Navigation: 1 2 3 4 5 6 7 8 9 10

	Cod. Caso	Cod. Ord. Id	Nome	Cognome	Codice Fiscale	Iban
Sicilia	313	ENRICO.MICHELIS-1234	Enrico	Micheli	XXXXXXXXXXXXXXXXXX	46000-01600-4600037D46000
Toscana	312	ANTONELLA.CORNELIA				00005-15400-000000003188
	311	ROBERTO.ORIA2006				00008-03230-000004880952
	310	MAURO.BIANCO	Mauro	Bianco	XXXXXXXXXXXXXXXXXX	44089-75870-000000044089
	309	GIUSEPPE.ALBANO-HF				00004-15201-000000820567
	308	LUCA.BOCCALONE				00002-01601-000000010183
	307	CRISTINA.COITE-LUI				
	306	MARIAFELICIA.BIANCO				
	305	MARIASPERANZA.GALEA				
	304	DANIELA.GIANINI-35	DANIELA	GIANINI	XXXXXXXXXXXXXXXXXX	

Grazie

Wilmana.Malatesta@visiant.it
Security Consultant

www.visiantsecurity.it