



SAS® FORUM  
PORTUGAL 2016

# Bem Vindos

# Combate e Prevenção à Fraude Online em Tempo Real

Carla Miranda

Business Solution Specialist

SAS Portugal

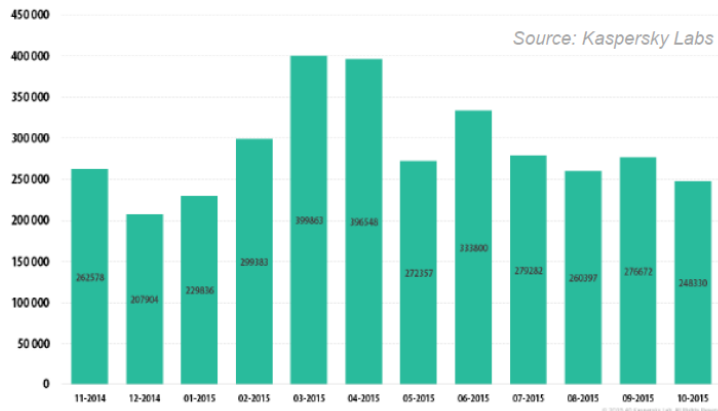
**DESAFIOS**





# COMBATE E PREVENÇÃO À FRAUDE ONLINE EM TEMPO REAL

# VELOCIDADE NA ALTERAÇÃO DO “MODUS OPERANDI”



The number of users attacked by financial malware, November 2014-October 2015



**Portugal: 6-10% banking malware attacks in 2015**

Kaspersky Security Bulletin 2015

Home » News » Money mule schemes targeted in several European countries, including Portugal

## Money mule schemes targeted in several European countries, including Portugal

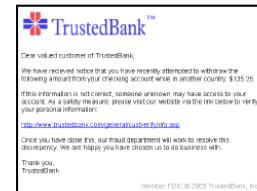
IN NEWS - 03-03-2016 14:01:00 - 0 COMMENTS

Source: [www.theportugalnews.com](http://www.theportugalnews.com)

**mule**   
accounts on the rise



You have been randomly selected for a BestBuy gift. Get your \$1000 gift card at [www.bestbuy.com/youre-a-winner.net?id=chrftvck](http://www.bestbuy.com/youre-a-winner.net?id=chrftvck)



**Fraud in Digital Advertising  
Advertisers will lose \$7.2 billion globally to  
bots in 2016.**

19/01/2016



**Firm loses \$44m due to an online email scam  
Europe's largest Electrical Cables Manufacturer Leoni AG fell  
for an online scam and transferred \$44m into a wrong bank  
account.**

03/09/2016



**Roughly £650m stolen from worldwide banks  
in last two years.**

16/02/2015



**UK loses £11 billion a year to fraud and  
cybercrime.**

19/10/2016



**Australians lose over \$229 million to  
scams in 2015.**

16/05/2016





# ABORDAGEM SAS





**SOLUÇÃO OPEN BOX**



**Transação**

Score das transações com base em:

- Comportamentos anómalos
- Alteração de detalhes
- Transferências de fundos de contas poupanças (*me2me transfers*)



**Cliente**

Score os clientes tendo por base:

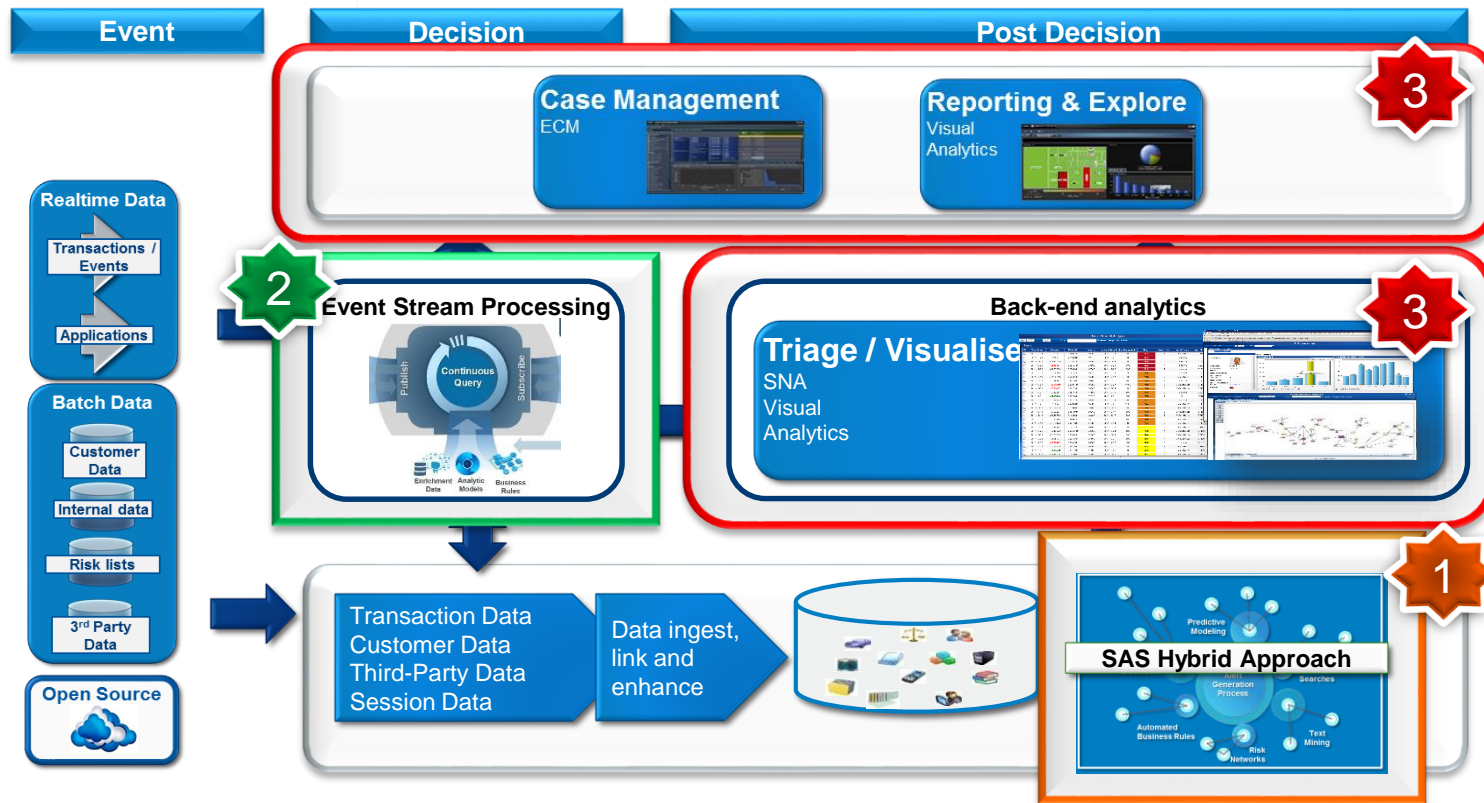
- Possíveis *mule accounts*
- Vulnerabilidade
- Identificação em *watch-list*
- Comportamentos anómalos



**Terceiros**

- Novos beneficiários
- Velocidade das transações
- Atividades suspeitas

✓ **Criação de Alertas!**



1

## Abordagem Híbrida

**sas**

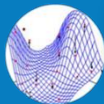
### SAS Hybrid Approach



#### Regras

Desenhar e implementar regras para filtrar transações fraudulentas.

*Duas transações em curto espaço de tempo de IP e de países distintos.*



#### Deteção de anomalias

Detetar padrões anormais individuais e agregados.

*Numero de transferências superiores ao desvio padrão do seu peer group.*



#### Analítica Avançada

Descoberta de conhecimento e avaliação preditiva.

*Descobrimo novos comportamentos de fraude através modelos preditivos.*



#### Text Mining

Extrair padrões suspeitos de dados não estruturados.

*Analisar as descrições de transferência para descobrir as palavras-chave que indicam fraude.*

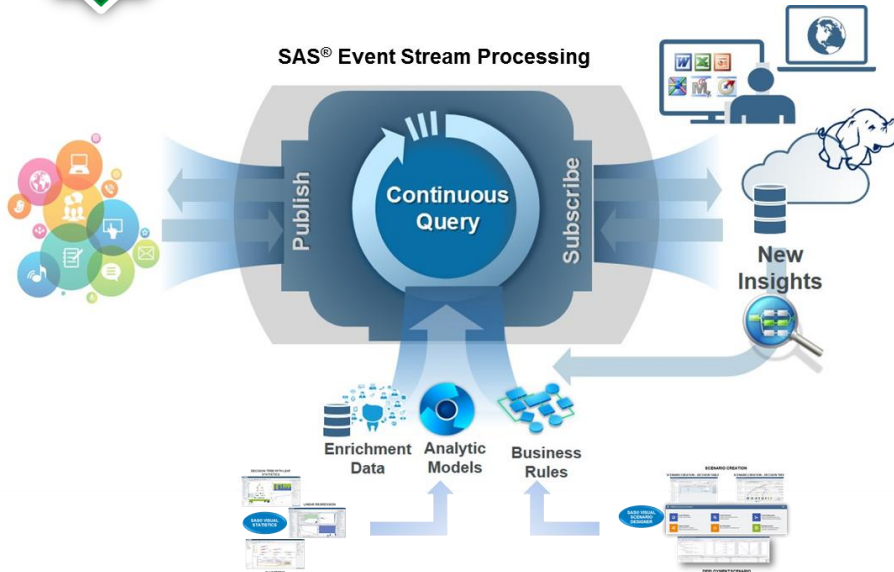


#### Redes

Executar a descoberta de conhecimento através da análise de redes.

*Descobrir links entre mules, alteração de entidades, redes organizadas..*

2



Milhões de eventos por segundo  
com latência de resposta  
milissegundo-microssegundo

- Rotinas de controle de qualidade de dados pré-construídas.
- Regras de negócio.
- Análítica avançada:
  - Score de eventos
  - *Machine Learning clusters*
  - Extrair, classificar e identificar entidades (metodos NLP – Natural Language processing)
- Filtrar, agregar e correlacionar eventos.
- Dados históricos de referência (in-memory).
- Queries contínuas ou periódicas.

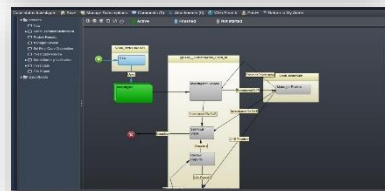
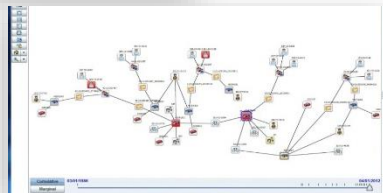
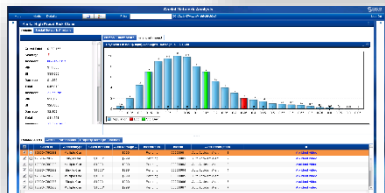
3



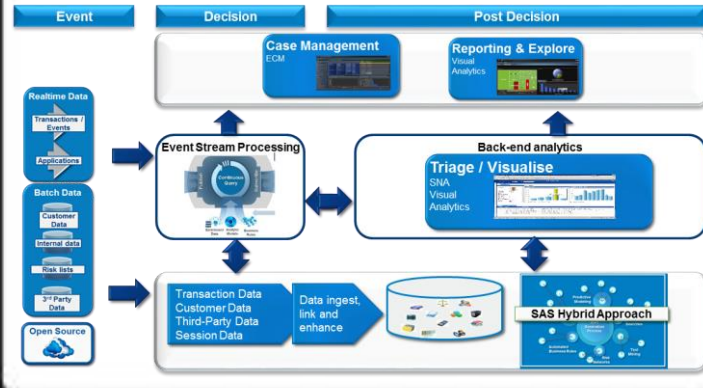
ID	DATA	VALOR	RISCO	STATUS	TIPO	ORIGEM	DESTINO	VALOR	DATA
00111	2012-11-15	10000	ALTO	OK	TRANSFERENCIA	001	002	10000	2012-11-15
00112	2012-11-15	5000	MEDIO	OK	TRANSFERENCIA	001	003	5000	2012-11-15
00113	2012-11-15	2000	BAIXO	OK	TRANSFERENCIA	001	004	2000	2012-11-15
00114	2012-11-15	1000	BAIXO	OK	TRANSFERENCIA	001	005	1000	2012-11-15
00115	2012-11-15	1000	BAIXO	OK	TRANSFERENCIA	001	006	1000	2012-11-15

### Interface de Investigação

- Geração de alertas de entidades suspeitas.
- Priorização os alertas com base na severidade.
- Filtragem por critérios de relevância.
- Redes – ligação entre entidades.
- Workflow de investigação.
- Reporting.



# DEMO



# REFERÊNCIA



# ON-LINE FRAUD DETECTION

## BUSINESS CHALLENGE

- Under attack from fraudsters and voice-fishing ("vishing")
- Experiencing a huge false positive ratio
- Lack of key elements in detection logic (e.g., beneficiary profiles, PC session logs)
- Reimburse defrauded customers to avoid reputational harm

## RESULTS

- Real time analysis of the transactions with very short latency to trigger real time alerts and actions
- Behavioral profiling of accounts using analytics
- Automation of decisions and stopping of suspicious transactions
- Alert triage and case management for manual investigation

BANKING





# Obrigado

