

INTEGRAÇÃO E DESCENTRALIZAÇÃO DE ALERTAS

por Francisco Camargo,
Conselheiro da ApRisco,
Presidente da CLM

Risk Operations Center

Um milhão de alertas por mês!

Aparentemente duas palavras que são antônimos e não sinônimos.

Integração pressupõe centralização, consolidação, correlação e aumento do controle.

Pelo milagre da tecnologia a língua portuguesa é torcida e se obtém as vantagens da integração e consolidação com as vantagens da rapidez de reação só encontrada em ambientes descentralizados.

O Software do Risk Operation Center, **consolida e correlaciona**, todos os **alertas** que circulam pela empresa em um único lugar e o distribui descentralizadamente para as áreas que devem recebê-los, com controle e total segurança..

Em uma Instituição Financeira, uma grande variedade de sistemas emite alertas e alarmes:

- O Sistema Anti-Fraude do Cartão de Crédito
- O Sistema Anti-Fraude do Cartão de Débito
- Os sistemas *Cris-On-Line* da Visa e *Risk Find* da Mastercard
- O Sistema Anti-Lavagem de Dinheiro
- O Sistema de Controle dos Caixas Automáticos (ATMs)
- O Sistema de Alarmes das Agências e ATMs
- O Sistema de Catraca e Ponto Eletrônico
- O Internet Bank
- O Sistema de Monitoramento dos sistemas em Tempo Real
- O NOC (Network Operation Center) e o SOC (Security Operation Center)
- E assim por diante...

Existem sistemas, consolidados e correlacionados com outros, poderiam emitir alertas e alarmes:

- O Sistema de Controle das catracas eletrônicas de visitantes e funcionários

Em si, este sistema não teria o que alertar, mas correlacionado com o Sistema de Rede (AD ou LDAP) poderia verificar se algum usuário, fazendo *login* na Rede, está realmente na empresa e alertar para uma tentativa de *login* na "... estação 412," no 5.º andar, tem alguém fazendo *login* em nome da Sandra Antunes, que pelo Sistema de Controle de Catracas não se encontra neste edifício ...".

Foram correlacionados, facilmente, 3 sistemas:

1. O Sistema de Controle das catracas eletrônicas de visitantes e funcionários
2. O Sistema de Controle de Identidades da Rede (Windows Active Directory ou o LDAP)
3. O Sistema de Controle Físico do Ativo (que diz onde está cada estação)

Fornecendo uma informação útil, que não seria obtida de nenhum desses sistemas separadamente.

- O Sistema que controla a Mesa de Operações Financeiras
- O Sistema que controla o SPB
- O Sistema de Cartão de Débito
- O Sistema que controla os ATMs (caixas eletrônicos)
- O sistema de Controle de Posições e Risco de Mercado
- O Sistema de Concessões e Risco de Crédito

AM/PM - Risk Operations Center

WWW.MONITORPLUS.COM.BR

distribuído por **CLM**

Um milhão de alertas por mês!

Controle e catalogação do Risco Operacional

Algumas instituições financeiras recebem mais de um milhão de alertas por mês.

Isto, por vários fatores, dificulta a tarefa de ajustar o Software Anti-fraude para os cartões de crédito, geralmente usando rede neural proprietária e gerando um número excessivo de alertas. Alertas de outras fontes para os Cartões de Crédito, como o Cris - On-Line da Visa, o Riskfinder da Mastercard, o Lynx da Visanet, alertas dos próprios usuários com unicando perda ou roubo.

Para os cartões de débito, o problema se repete, e ainda tem que ser tratados os alertas da Rede de Caixas Eletrônicos, além disso muitos outros sistemas geram alertas, como o sistema anti-lavagem de dinheiro, alertas do IDS e do Firewall, e assim por diante.

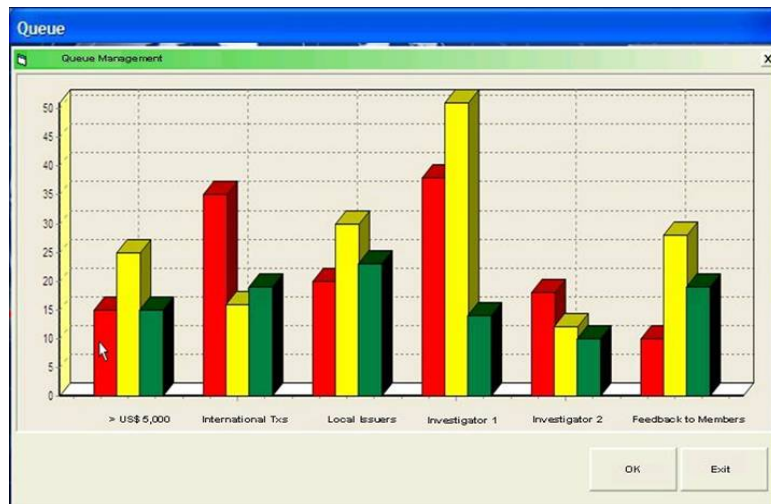
Outros alertas são gerados pelos diversos sistemas e pela infraestrutura de TI e pelos sistemas de Segurança de TI, normalmente são concentrados em um SOC (Security

Operations Center) e/ou NOC (Network Operations Center).

Evidentemente que ter um milhão de alertas por mês é igual a ter nenhum alerta por mês, pela impossibilidade prática de tratá-los de forma manual.

O AM/PM permite automatizar boa parte do processo de análise e investigação de alertas.

Com Administração inteligente e automática das filas de alertas



a investigar, classificação automática de Riscos por importância, análise da produtividade dos investigadores e analistas.

Estatísticas de Produtividade por Áreas de Investigação, por analistas e investigadores e muito mais.



O AM/PM é um sistema de inteligência artificial, baseado em regras, com sofisticado Módulo de Alertas, em que o envio de mensagens e de consultas pode se utilizar vários meios físicos, tais como Pop Up, e-mail, Pager e/ou telefone celular.

Conta ainda com sofisticado módulo de Análise do Comportamento (behavior) Histórico e de Padrões, dos clientes, no ambiente de investigação.

Workflow, com definição dos procedimentos de investigação, bem como de outros processos operacionais e de negócios, relacionados ou não com a investigação, permitindo o escalamento automático do Alerta.

Com a adoção de Ações Automáticas, o sistema pode agir automaticamente em situações de alto risco, permitindo execução de ações, tais como, o congelamento de contas.

Todo o histórico fica armazenado para fins de Risco Operacional, Res. 3380 e Sarbanes-Oxley.

AM/PM - Risk Operations Center

WWW.MONITORPLUS.COM.BR

distribuído por **CLM**