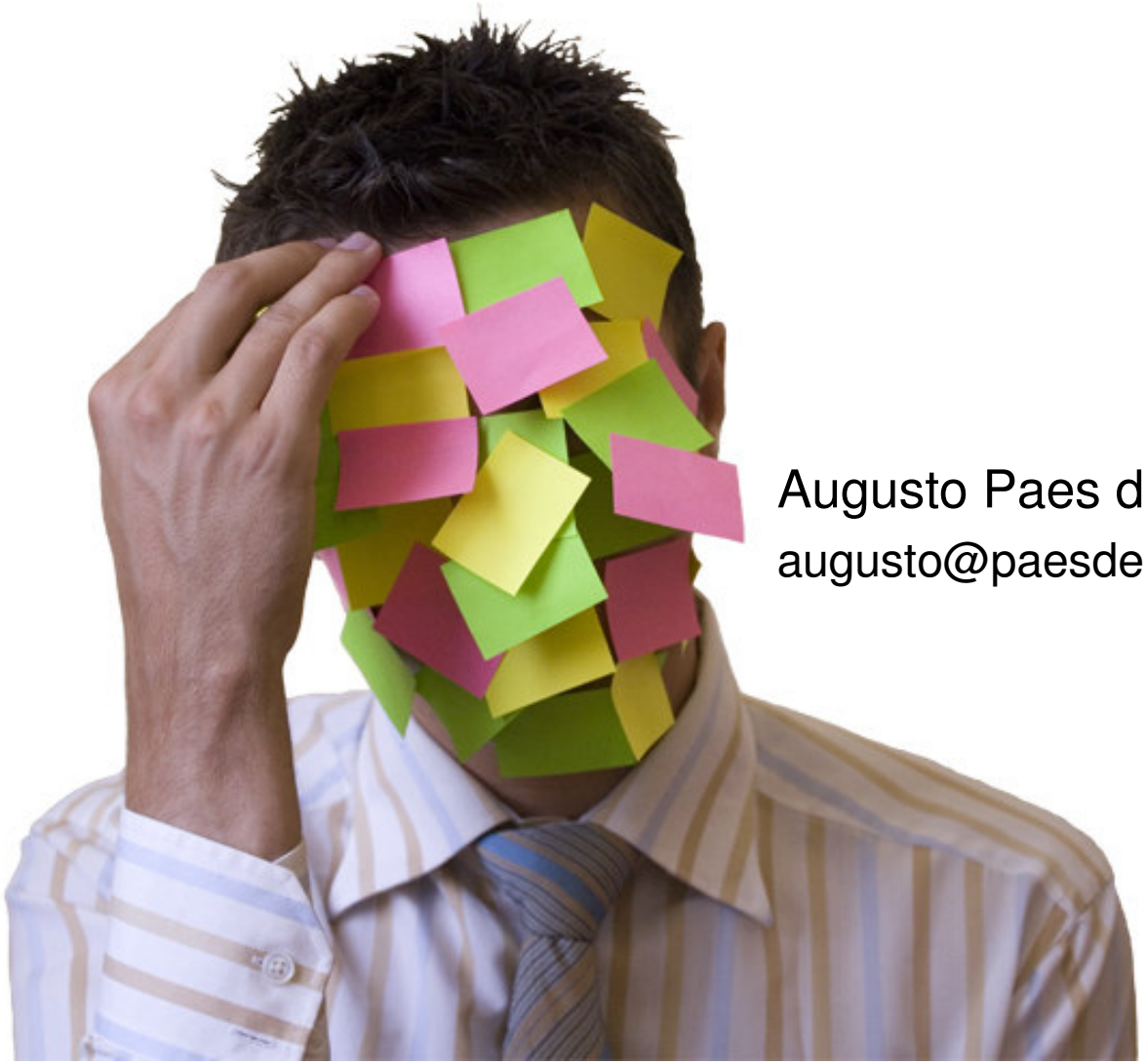
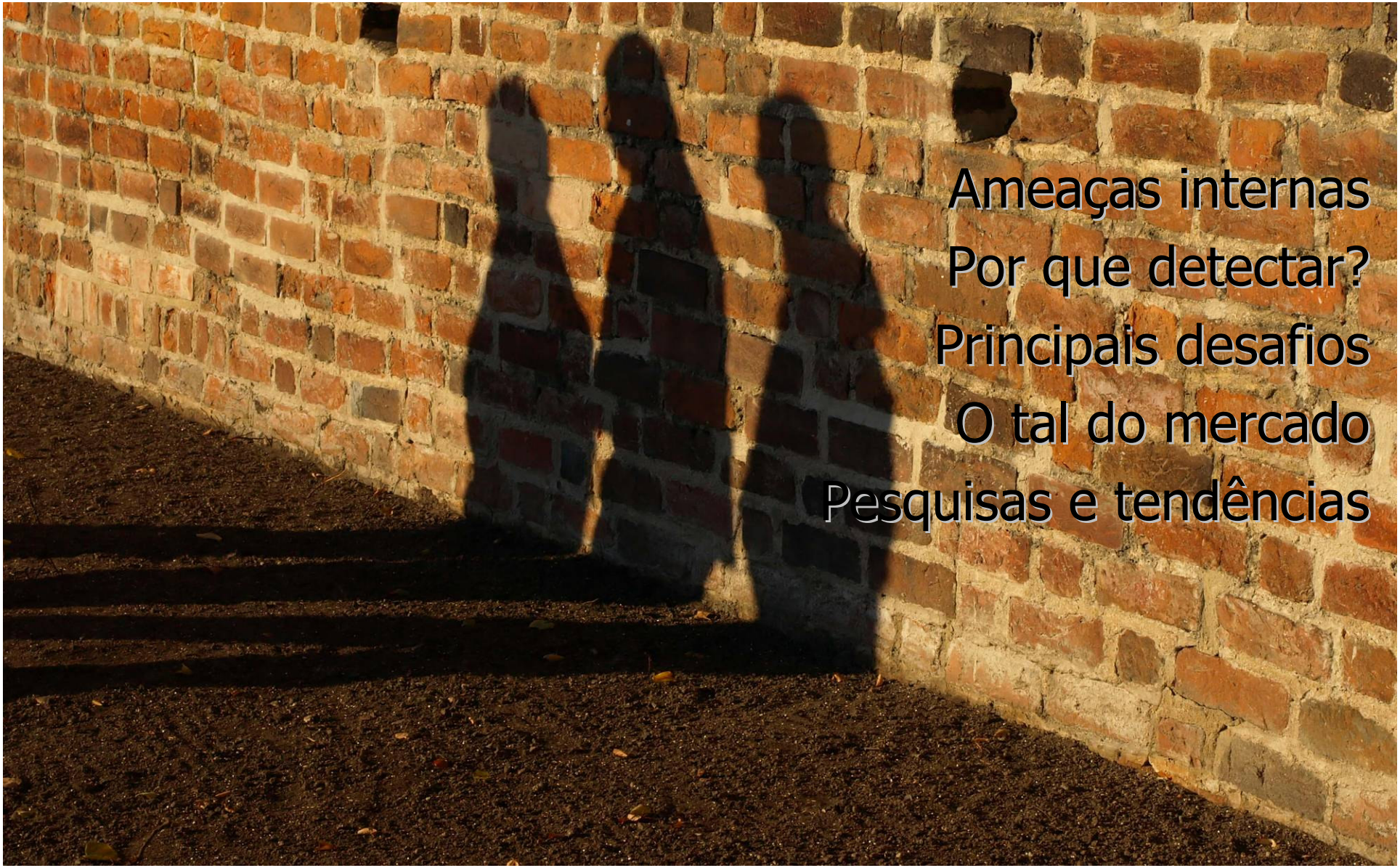
Detectando ameaças internas



Augusto Paes de Barros
augusto@paesdebarros.com.br

Agenda


Ameaças internas
Por que detectar?
Principais desafios
O tal do mercado
Pesquisas e tendências

Ameaças internas

Quem são eles?


Funcionários descontentes


Financeiramente motivados


Pseudo-insiders

Por que detectar?

Porque é muito difícil evitar

Por que o impacto é extremamente alto

IDG Now! » Mercado » Legislação

MERCADO

LEGISLAÇÃO

Cientista admite ter roubado US$ 400 milhões em segredos da DuPont

Por Jaikumar Vijayan, para o IDG Now!*
Publicada em 19 de fevereiro de 2007 às 11h00
Atualizada em 19 de fevereiro de 2007 às 11h04

E-mail Imprima Comente Erros? del.icio.us Digg a a a

Framingham - Após nova proposta de emprego, Gary Min invadiu servidor com segredos técnicos e de mercado e roubou quase 40 mil documentos.

over $691 million. In 30% of the cases, the financial loss was in excess of $500,000. One company did not suffer any financial loss.

- In 91% of the cases, the insider activity had at least one other adverse impact on the organization.

U.S. Secret Service and CERT Coordination Center/SEI
Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector
Page 18

Supporting Data
Eighty-one percent of the organizations experienced a negative financial impact as a result of the insiders' activities. The losses ranged from a reported low of $500 to a reported high of "tens of millions of dollars." The chart below represents the percentage of organizations experiencing financial losses within broad categories.

U.S Secret Service and CERT Coordination Center/SEI
Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors
20

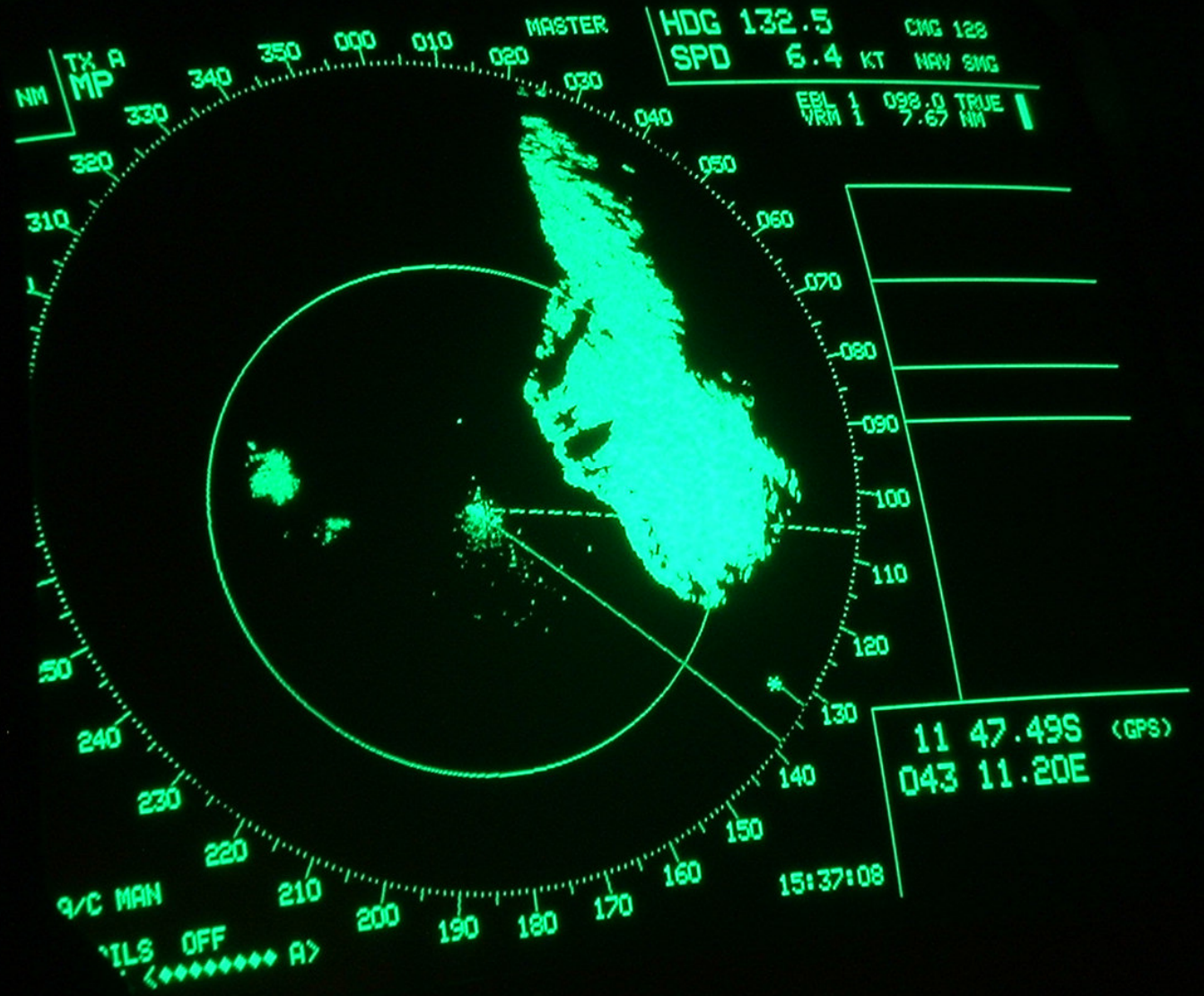
Casos

DuPont – Gary Min

FBI – Robert Hanssen

UBS – Roger Duronio

Principais desafios



Quem é a maçã podre?

Ferramentas projetadas para ameaças externas

Poucos pontos de controle

O tal do mercado

Logs!

- SIEMs

Análise de Logs

Data Leak Protection

WEBSENSE.

VONTU

VERICEPT

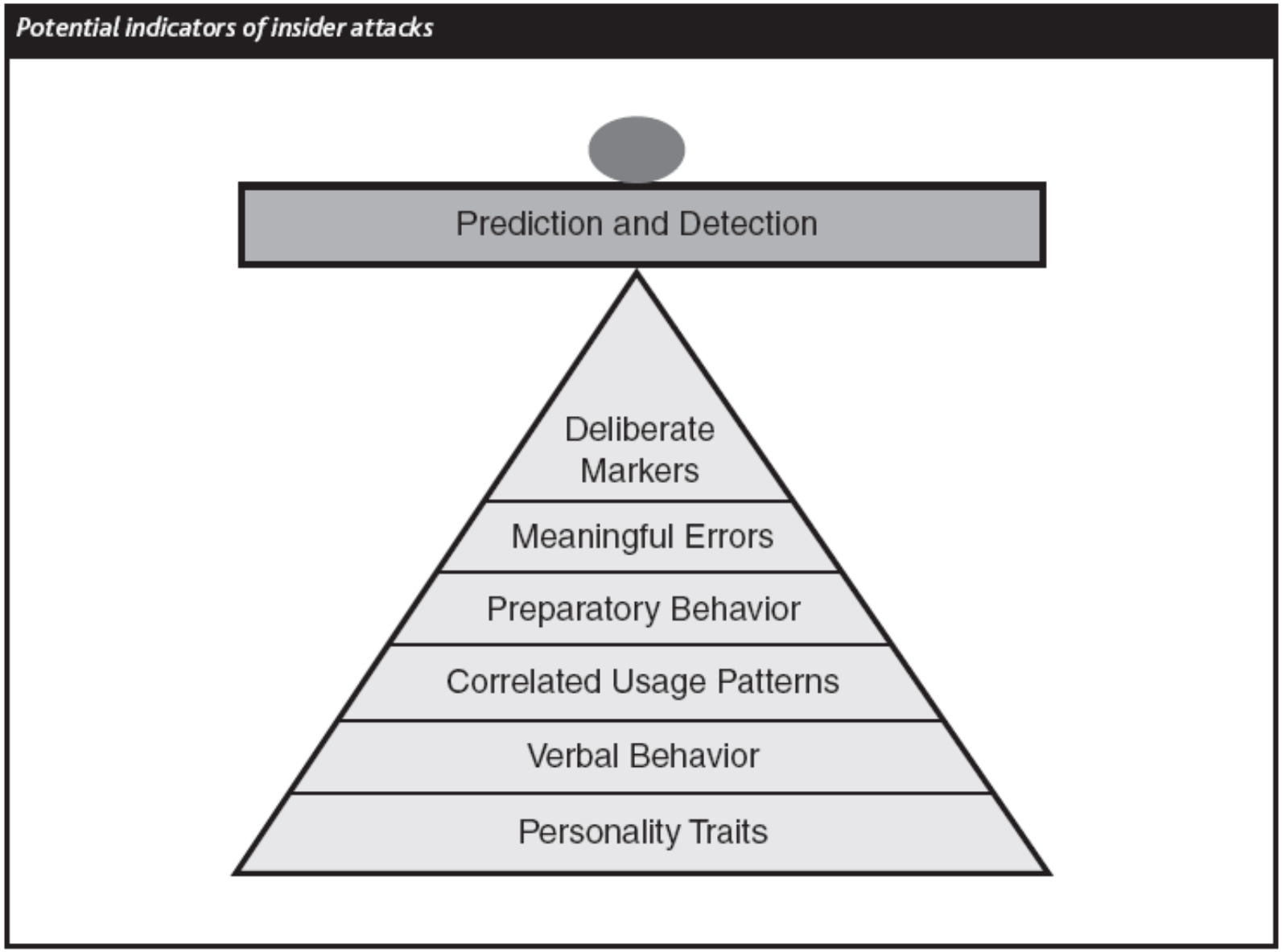
Reconnex
INFORMATION PROTECTION. ALWAYS.™

McAfee®

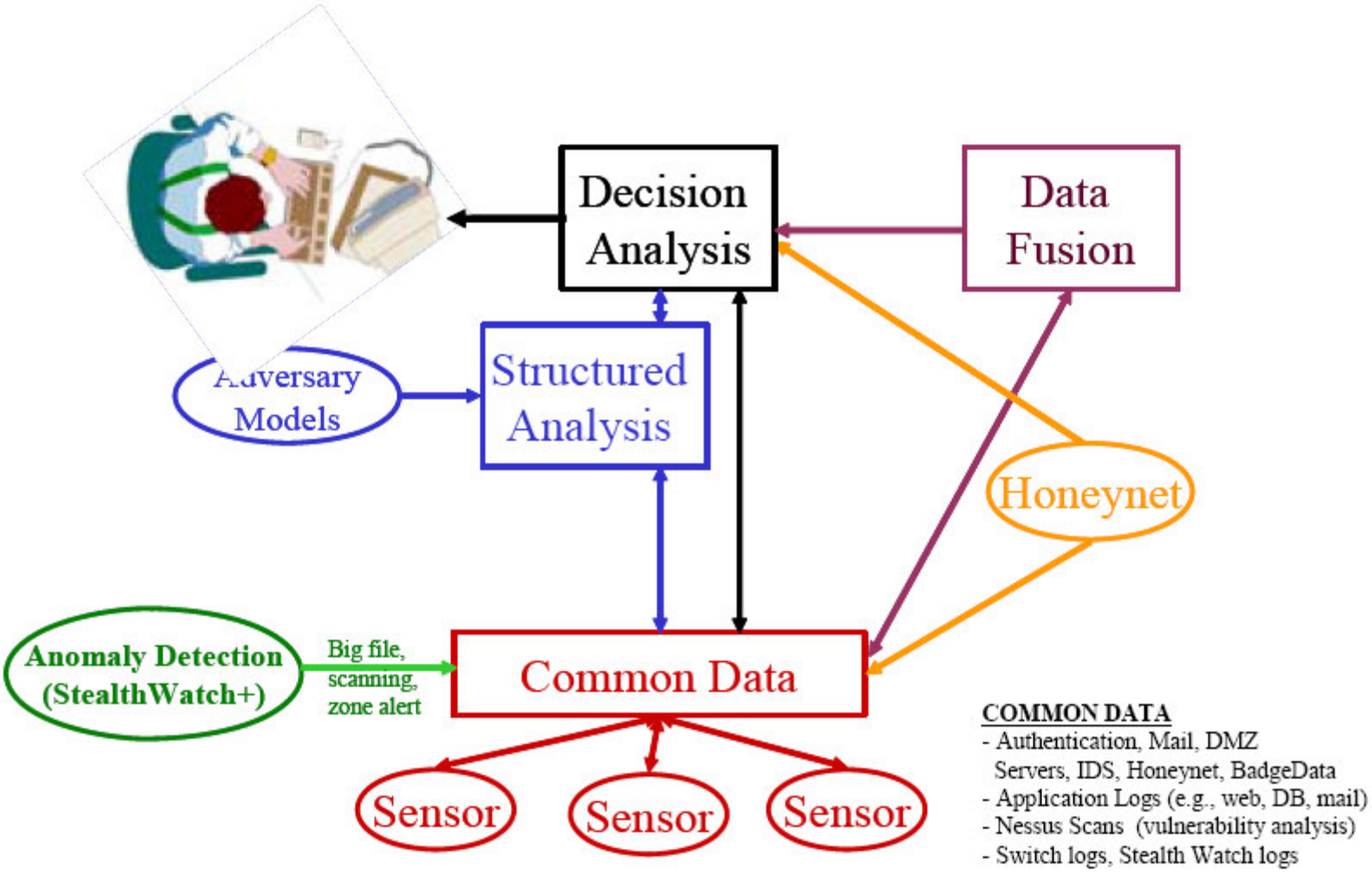
CLEARSWIFT™
Simplifying content security

Pesquisas e tendências

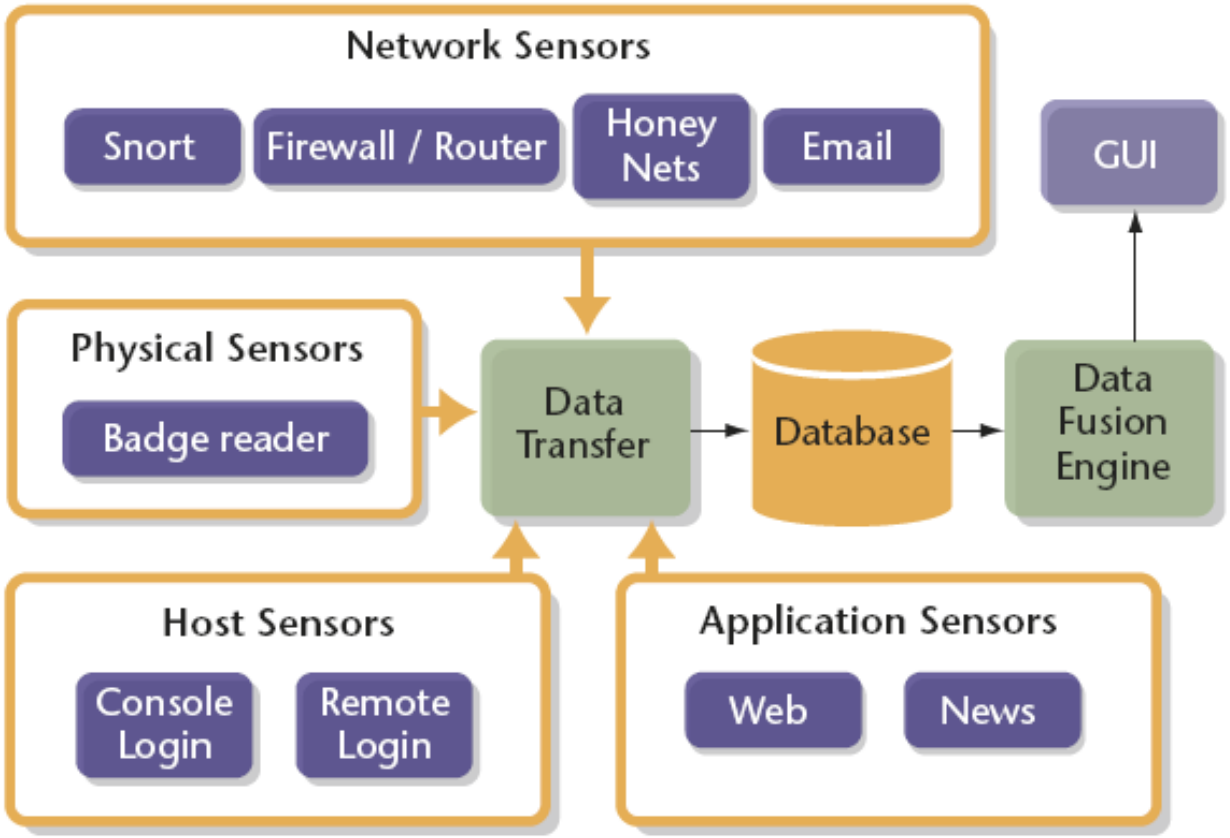
Eugene Schultz - 2002



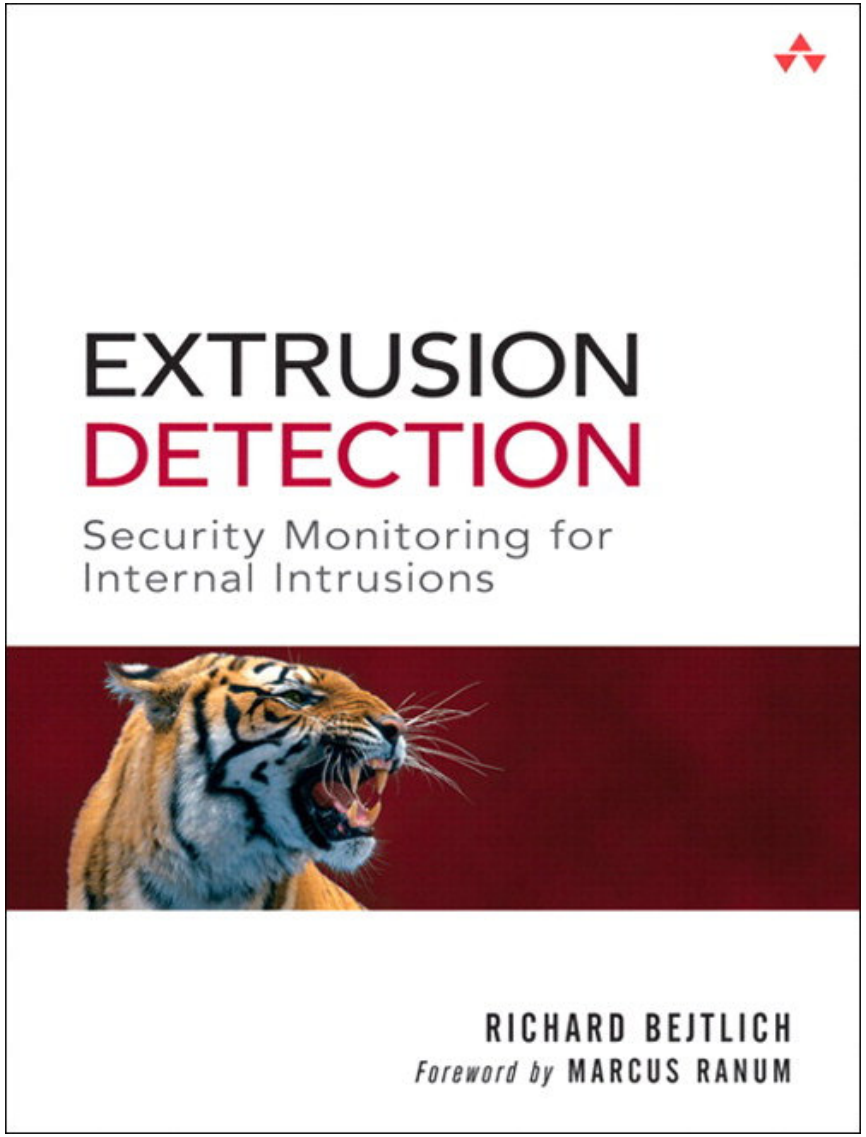
ARDA/MITRE Workshop - 2004



Matzner & Hetherington - 2004



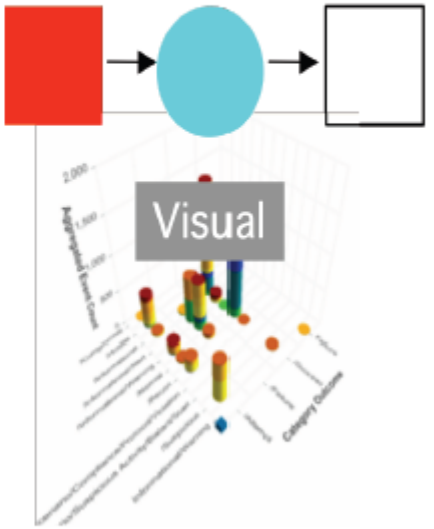
Richard Bejtlich - 2005



Raffael Marty - 2007

Visualizing Log Data


```
Jun 17 09:42:30   rmarty ifup    : Determining IP information for eth0...
Jun 17 09:42:35   rmarty ifup    :  failed; no link present.  Check cable?
Jun 17 09:42:35   rmarty  network: Bringing up interface eth0:  failed
Jun 17 09:42:38   rmarty sendmail   :  sendmail   shutdown succeeded
Jun 17 09:42:38   rmarty sendmail   :  sm-client    shutdown succeeded
Jun 17 09:42:39   rmarty sendmail   :  sendmail startup      succeeded
Jun 17 09:42:39   rmarty sendmail   :  sm-client startup      succeeded
Jun 17 09:43:39   rmarty vmnet-dhcpd  : DHCPINFORM from 172.16.48.128
Jun 17 09:45:42   rmarty  last message repeated 2 times
Jun 17 09:45:47   rmarty vmnet-dhcpd  : DHCPINFORM from 172.16.48.128
Jun 17 09:56:02   rmarty vmnet-dhcpd  : DHCPDISCOVER from 00:0c:29:b7:b2:47 via vmnet8
Jun 17 09:56:08   rmarty vmnet-dhcpd  : DHCPOFFER on 172.16.48.128 to 00:0c:29:b7:b2:47 via vmnet8
NH
```



- ✓ Interpret Data
- ✓ Knows Data Formats
- ✓ Re-use don't re-invent
- ✓ Find some at: http://secviz.org/?q=node/8

Meus palpites

- Ampliar entidades monitoradas
  - Sair de IP, serviço, usuário, para:

Informações, transações, pessoas, recursos, endereços IP, nomes, endereços físicos, localidades geográficas, entre outros

Meus palpites

- Integrar bases auxiliares de conhecimento
  - Diretórios, perfis, vulnerability management systems...

Meus palpites

- Integrar mais dados para identificação de desvios
  - Netflow, Logs de proxy, etc.

Meus palpites

- Atenção às questões de controle de acesso

Menos “cool”, mas o problema, na maioria das vezes, está lá!

Obrigado

- Perguntas, sugestões, observações?

augusto@paesdebarros.com.br