IBM Security Forum

Soluções para um ambiente seguro

Um framework para gestão pró-ativa de segurança

Kleber Stroeh
Ícaro Technologies
kleber.stroeh@icaro.com.br

Agenda

- Motivação
- Lições da História
- Framework para Gestão de Segurança
- Correlação de Eventos
- Conclusões
- Sobre a Ícaro Technologies

Motivação

Por que segurança merece nossa atenção?

Segurança ainda é um desafio…

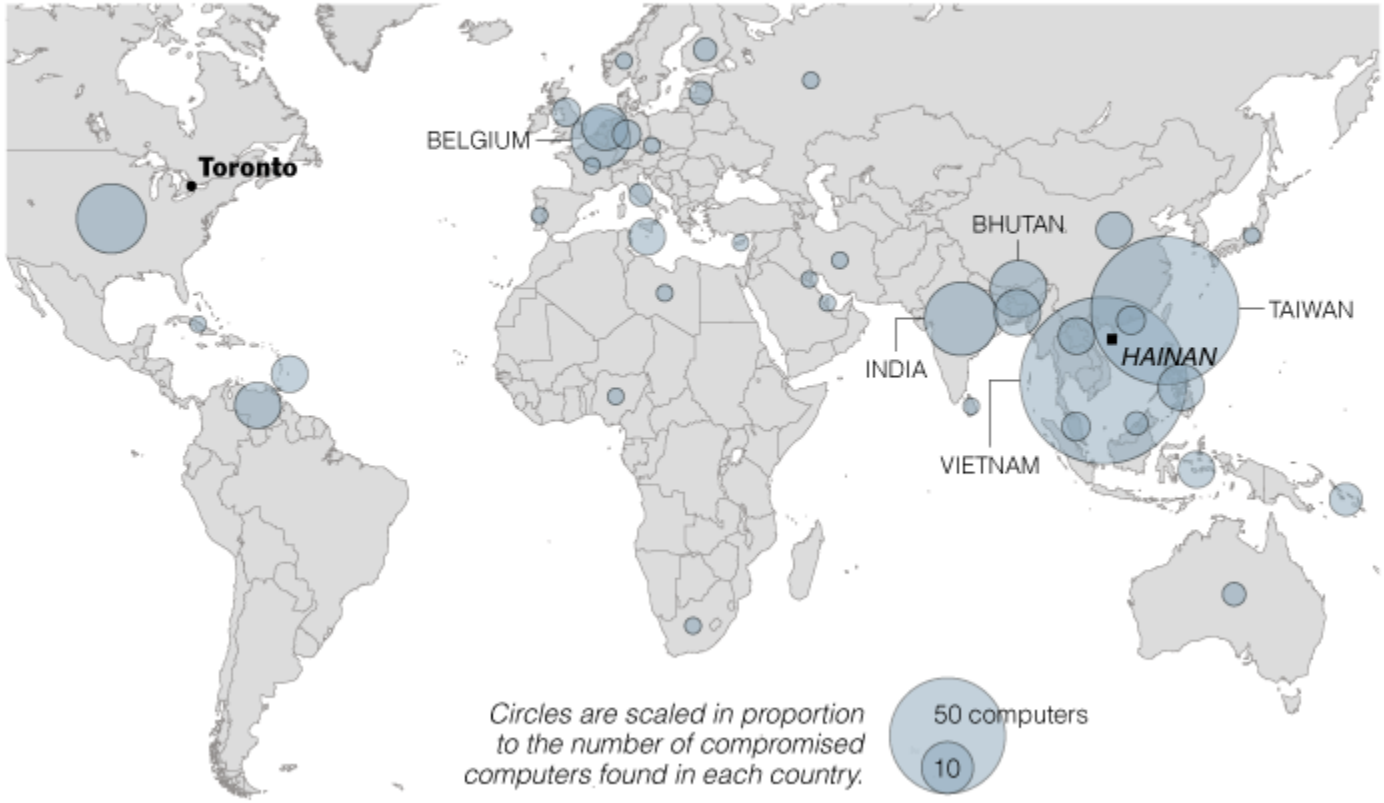
- “O roubo de dados e crimes cibernéticos custaram às empresas, em todo o mundo, cerca de **US$ 1 trilhão**” (Estudo da McAffee apresentado no último Fórum Econômico Mundial, em Davos)

- Um único episódio em 2009, expôs dados de cartões de créditos, que especialistas estimam ter afetado **50 milhões de pessoas**, o que está sendo entitulada de “a maior violação de dados da história” (Folha de São Paulo)

… para corporações e nações …

The Vast Reach of 'GhostNet'

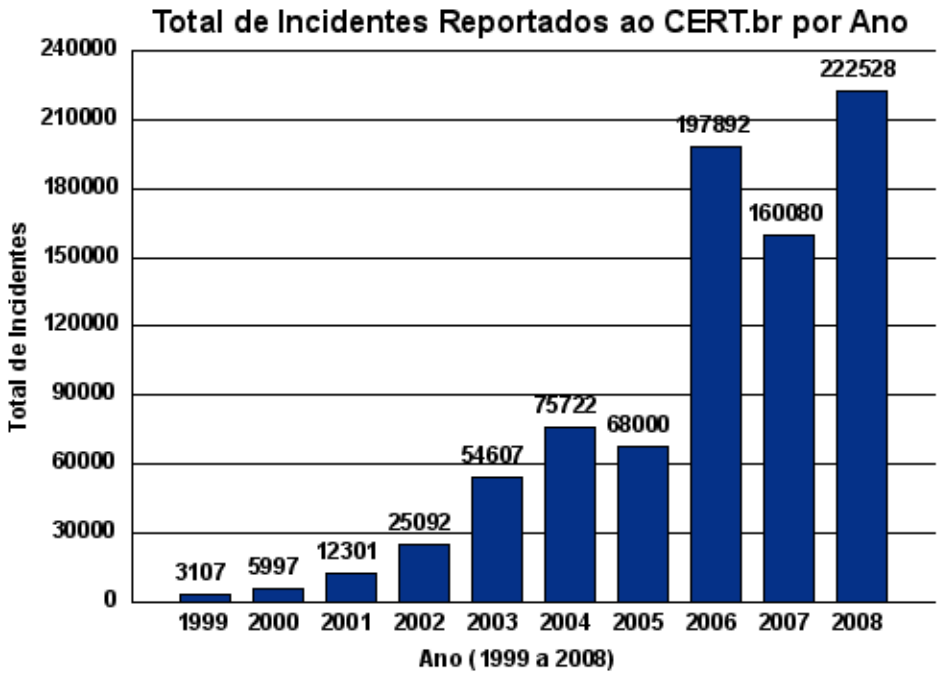
Researchers have detected an intelligence gathering operation involving at least 1,295 compromised computers. Below, the locations of 347 of the compromised machines, many of which were tracked to diplomatic and economic government offices of South and Southeast Asian countries.

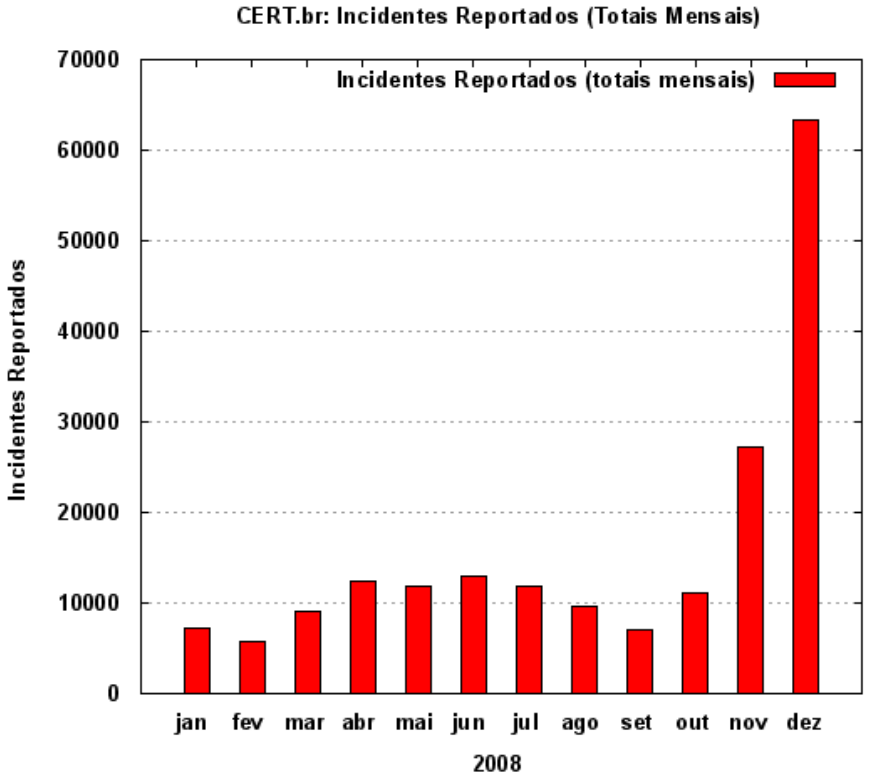


Source: Information Warfare Monitor

THE NEW YORK TIMES

… nos dias de hoje.





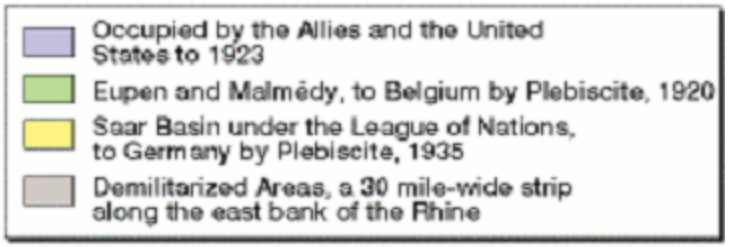
Por que isto ocorre?

- Crescimento do valor de ativos digitais:
  - cartões de crédito
  - declarações de Imposto de Renda
  - informações de defesa
  - estratégias políticas
  - prontuários médicos
  - outros
- Dependência de uma infraestrutura de TI mais complexa (mais vulnerabilidades)
- Negócios exigem agilidade (novamente as vulnerabilidades…)
- Ataques mais produtizados
- Abordagens estáticas (defesa de perímetros), pouco flexíveis e nada resilientes
- Volume de eventos (milhões/mês) e falsos positivos implicam falsos negativos
- Falta de consciência situacional (*situational awareness*)
  - “Eu dormia o sono dos justos, protegido pelo manto da ignorância” (cliente anônimo)
- Desalinhamento: processos / ferramentas / pessoas
- Vantagem do atacante
  - escolher onde e quando

Lições da história

O que podemos aprender com o passado?

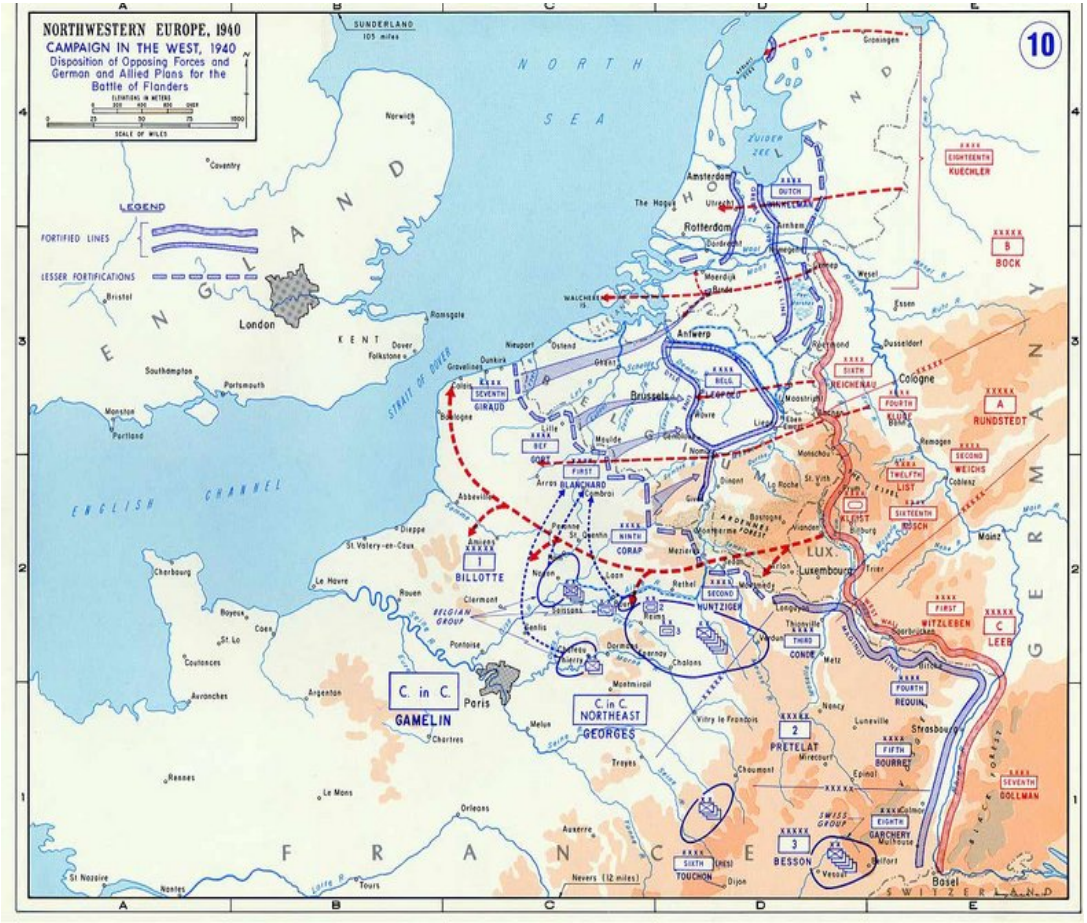
Lições históricas: a linha Maginot



- Linha fortificada estática que separava a França da Alemanha e Itália
- Complexo de bunkers para milhares de homens, 108 fortes principais (a 15km de espaçamento), fortes menores e casamatas, e mais de 100km de túneis.
- Custo: 3 bilhões de francos

Batalha da França

- Alemanha invade a França através dos países baixos em tempo recorde
- Início da Campanha:
  - 10/05/1940
- Rendição da França:
  - 22/06/1940



Lições históricas 2: O sistema Dowding

- Maquinário complexo de detecção, controle e comando para proteção da Grã-Bretanha
- 4 grupos aéreos
  - 10 Group: País de Gales
  - 11 Group: Sudeste da Inglaterra
  - 12 Group: Terras médias e leste
  - 13 Group: Escócia e Irlanda do Norte
- Sistema de inteligência
  - Radares
  - Corpo de observadores
  - Modelo de comunicação claramente definido
  - Uso do rádio
  - Vetorização da interceptação

Batalha da Inglaterra

- Superioridade numérica alemã
- Início:
  - Agosto/1940
- Término:
  - Maio/1941
- Hitler desiste de invadir a Grã-Bretanha após contundente derrota na batalha

"Never was so much owed by so many to so few"

(Winston Churchil)

Maginot x Dowding

- Maginot
  - Modelo estático e inflexível
  - Reatividade
  - Gerência de vulnerabilidade inexistente
    - Cobertura parcial das fronteiras
  - Gerência de incidentes ineficaz
    - Reação lenta e ineficiente
  - Baixa coordenação de atividades
    - Não havia plano para responder às ameaças
  - Altos investimentos em estratégia ineficaz

Resultado:
Fracasso e altos custos

- Dowding
  - Modelo flexível; mobilidade
  - Pró-atividade
  - Gerência de vulnerabilidade eficaz
    - Cobertura competente de todas as fronteiras
  - Gerência de incidentes eficaz
    - Mobilidade, agilidade, inteligência, comunicação
  - Alta coordenação de atividades
    - Coleta, correlação, decisão e ação
    - Integração de tecnologias, processos e pessoas
  - Otimização de recursos escassos

Resultado:
Sucesso e custos controlados

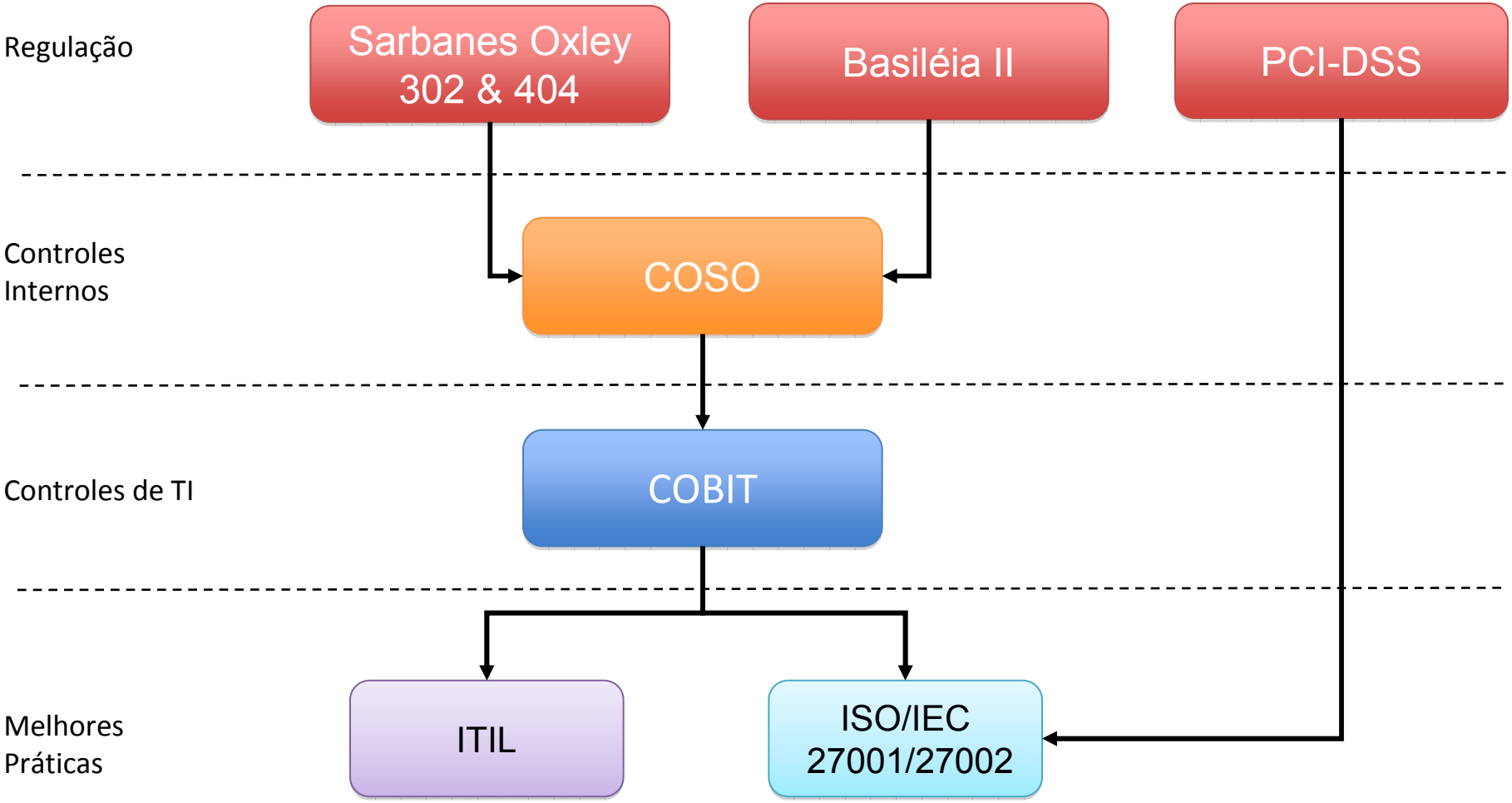
Framework para gestão de segurança

Como endereçar a gestão da segurança?

Requisitos

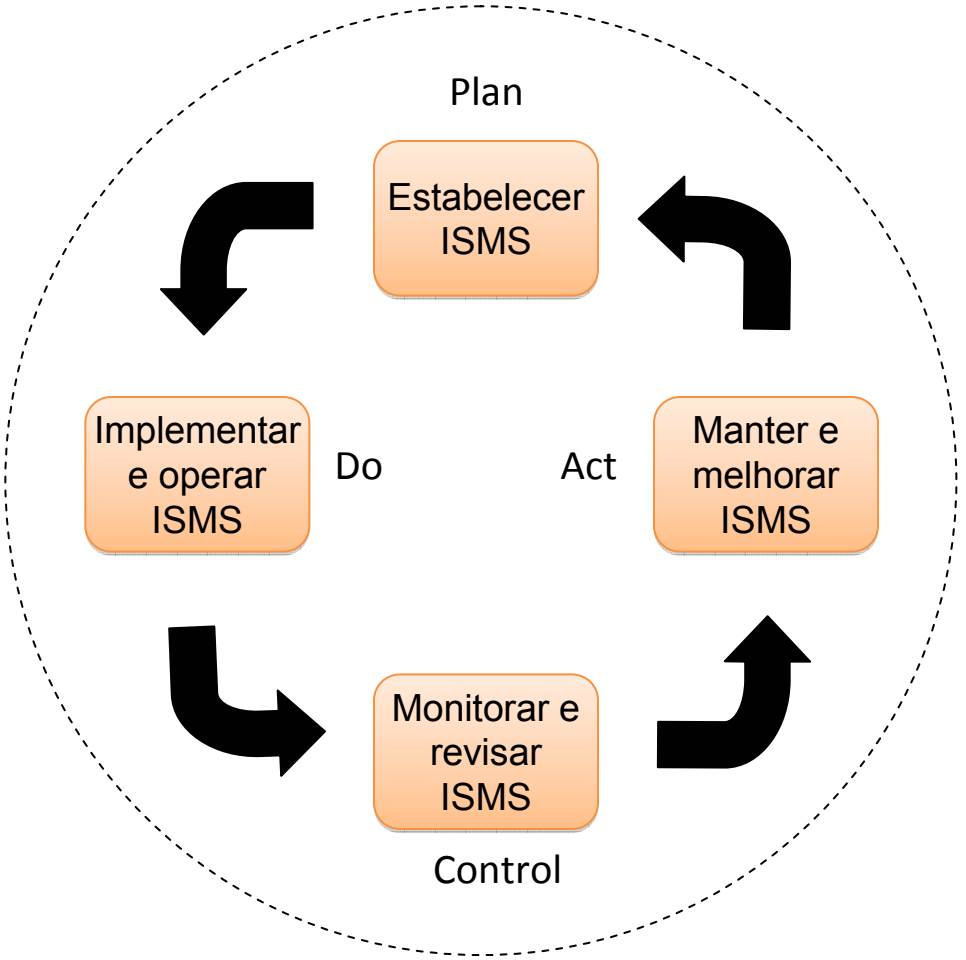
- Suporte a aspectos regulatórios
- Flexibilidade no atendimento do negócio
- Agilidade para tratamento de situações imprevistas
- Resiliência
- Boa relação custo/benefício

Alinhamento

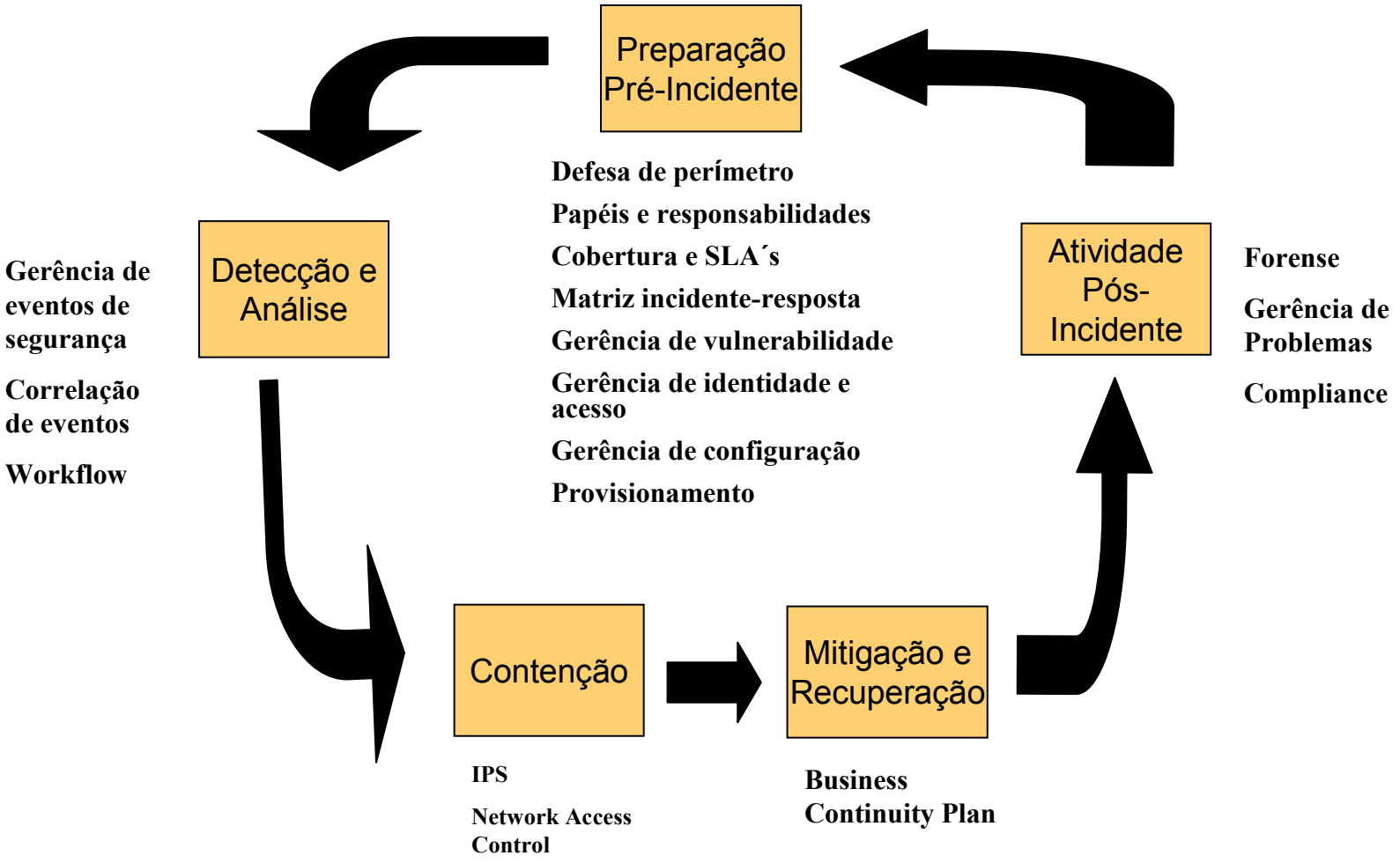


Gestão da Segurança é um processo

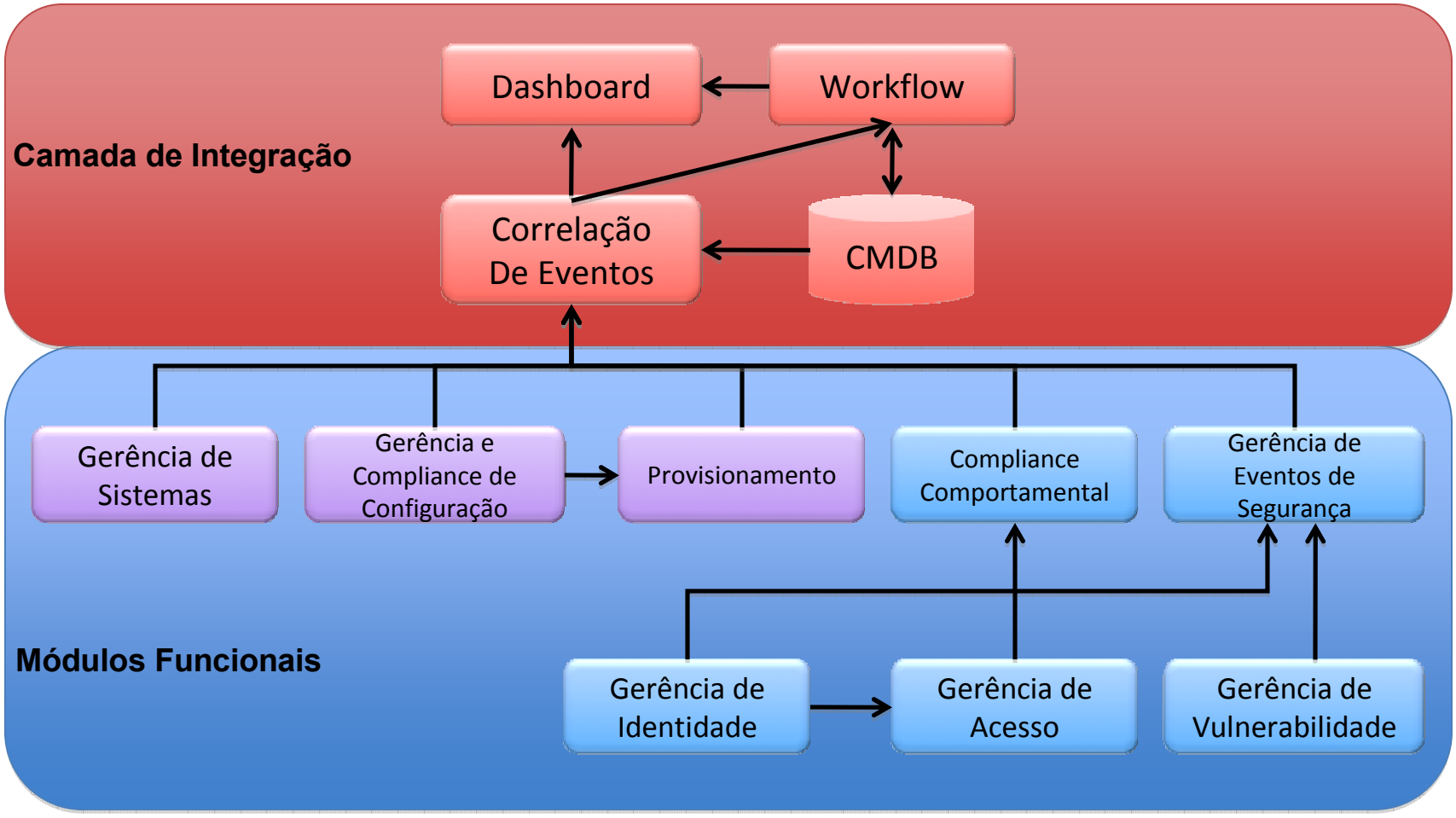
- ISO/IEC 27001 define processo para...
  - Estabelecer (Plan)
  - Implementar e Operar (Do)
  - Monitorar e Revisar (Check)
  - Manter e Melhorar (Act)
- Sua implementação ocorre por controles
  - ISO/IEC 27002



Respostas a incidentes



Um Framework Integrado e Automatizado



Reflexões

- Gerência de Identidade
  - Considerável volume de esforço está associado a fluxos de comissionamento e descomissionamento de usuários
- Gerência de Acesso e Compliance Comportamental
  - Grande volume de incidentes e fraudes está associado a usuários internos
- Compliance Comportamental e de Configuração
  - Grande volume de esforço de compliance está em gerar evidências dos controles estabelecidos

Reflexões 2

- Gerência de Problemas
  - Segundo Julisch*:
    - “Algumas poucas dúzias de causas raízes persistentes, em geral, são responsáveis por 90% dos alarmes gerados por IDSs”
- Gerência de Configuração
  - Parte relevante das causas raízes estão associadas a problemas de configuração e sua gestão

Evolução continuada

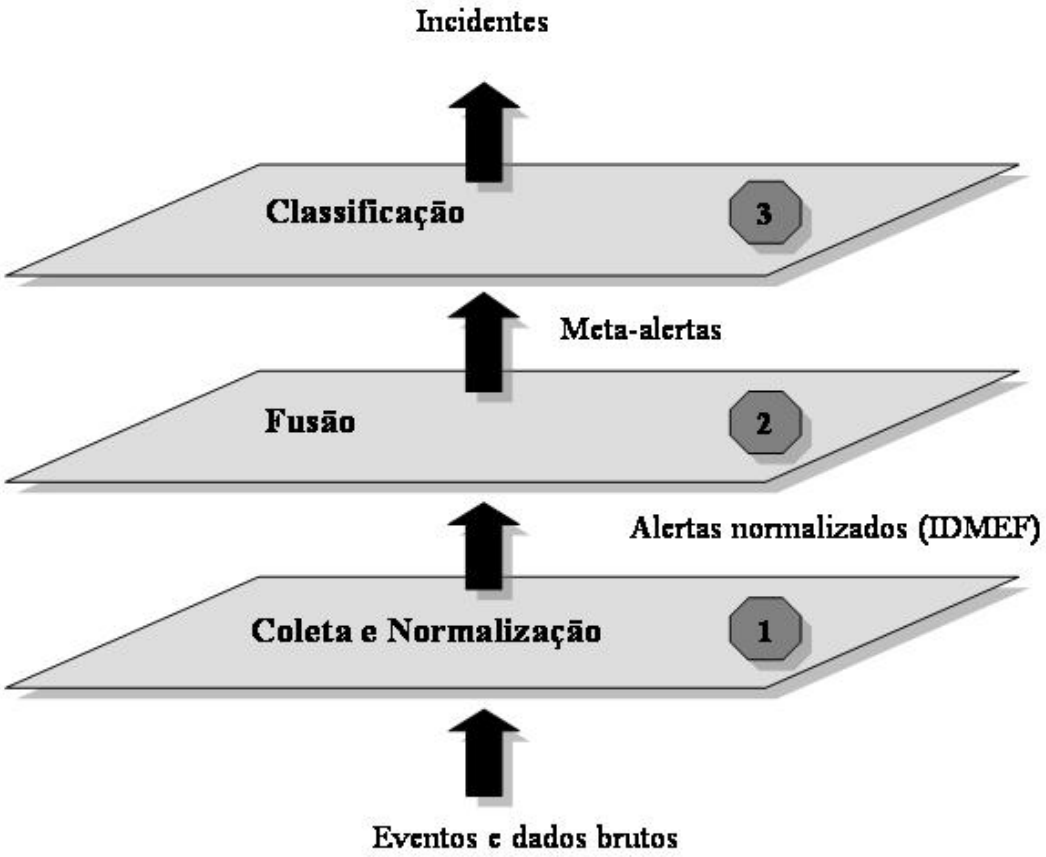
Correlação de eventos na prática

Por que correlacionar eventos é essencial?

Por que correlacionar eventos é crítico?

- Tratar eventos é pré-requisito para uma gestão de segurança pró-ativa
- Grandes infraestruturas de TI geram centenas de milhares a milhões de eventos por dia
- Não há capacidade operativa para tratar tal volume de eventos

Resposta: Correlação de Eventos



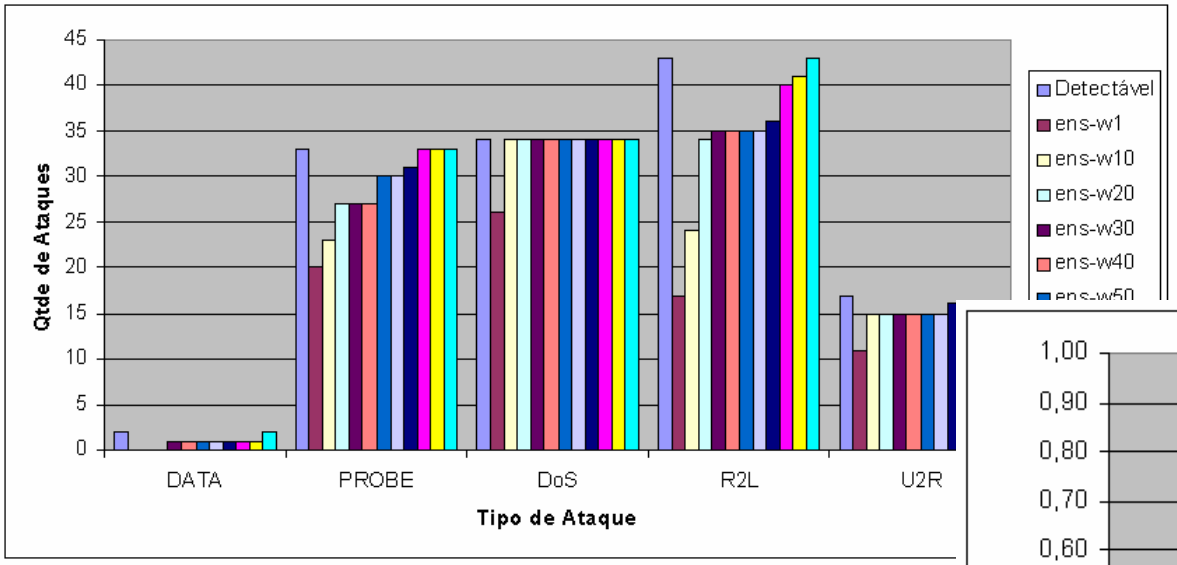
Correlação de eventos na prática

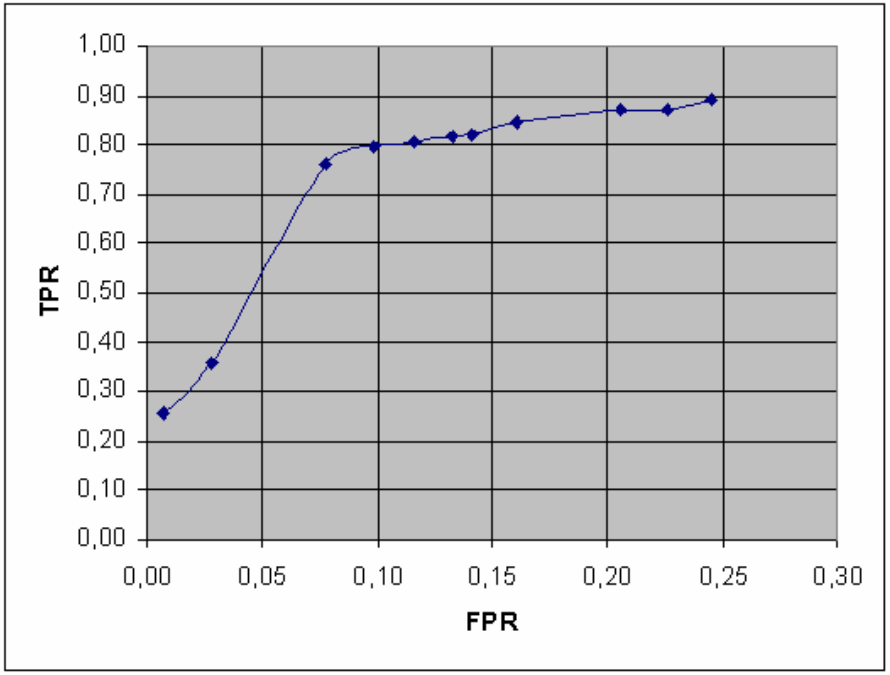
- Desafio proposto pelo DARPA em conjunto com o MIT Lincoln Labs
- Simulação de uma rede LAN de uma base aérea americana
- Ataques à infra-estrutura são executados e documentados
- Dados:
  - Período: 3 semanas de dados de treinamento, 2 semanas de teste
  - Fontes: arquivos tcpdump, logs de eventos Windows, logs de segurança BSM, e dados de auditoria
  - Volume: aprox. 10GB de dados comprimidos
- Classificação de ataques:
  - DoS (Denial of Service)
  - R2L (Remote to Local)
  - U2R (User to Root)
  - PROBE

Fusão e Classificação

Entidade	**Quantidade**
Registros	24.278.195
Alertas	569.108
Meta-alertas	19.550
Ataques Indicados	268
Razão de Redução	**2.124**

Resultados (base DARPA)





Folhas, árvores, florestas…

- Risco em gestão de segurança:
  - Focar nas folhas e não enxergar a floresta
- Como endereçar...
  - Eventos (folhas) devem ser fundidos em meta-eventos (árvores)
  - Meta-eventos classificados, separando-se as árvores boas (falsos alarmes) das más (ataques)
  - O conjunto de meta-eventos descreve sua floresta

Correlações de eventos de segurança são aplicáveis em…

- Infraestrutura de segurança e TI
  - Corporações e governo
- Redes de telecomunicações
  - Fixas e móveis
- Redes de ATMs e agências (setor financeiro)
  - Segurança lógica e física
- Redes de varejo
  - Segurança lógica e física
- Outros…

Conclusões

O que podemos concluir ?

Conclusões

- Há uma nova ordem em segurança da informação
  - Ativos digitais mais valiosos
  - Vulnerabilidades mais presentes
  - Novas ameaças
- Defesa de perímetro não é mais suficiente (Linha Maginot)
- Pró-atividade em segurança (Sistema Dowding) pressupõe:
  - Integração de disciplinas
    - Gerência de identidade, acesso, compliance, gerência de eventos de segurança, etc
  - Automação
    - Ferramentas implantadas e integradas
  - Correlação de eventos
    - Fusão e classificação

Conclusões 2

- Um framework de segurança permite:
  - Pró-atividade e agilidade para tratamento de incidentes
    - Recuperar-se de situações inusitadas
    - Resiliência
  - Evolução contínua da gerência da segurança até o nível de Risk Awareness e Situational Awareness
    - Enxergar a floresta (a partir de suas árvores e folhas)
  - Otimizar o uso de recursos
    - Automação de funções e correlação de eventos
  - Suportar nativamente requisitos regulatórios

Sobre a Ícaro Technologies

Quem somos e como podemos ajudar ?

Sobre a Ícaro Technologies

- Integradora de Soluções de Gerência
  - Security Management
  - IT Infrastructure Management
  - IT Service Management
  - BPM
  - Consultoria
  - Outsourcing

Destaques

anuário INFORMÁTICA HOJE destaque do ano 2008

EXAME PME 100 EMPRESAS QUE MAIS CRESCEM

AAA Accreditation AAA Tivoli Netcool/OMNIbus 1 dos 5 no mundo. Primeira na Am. Latina

IBM MELHOR PARCEIRO DE SOFTWARE 2007

Authorized IBM Training

Tivoli software

Tivoli AWARD 2009 IBM Tivoli Service Management Solution Award 2009

PRÊMIO 2008 As Melhores Empresas Para ESTAGIAR

ICARO TECHNOLOGIES

Oferta em Gerência de Segurança com IBM Tivoli

- Gerência de Identidade (TIM)
- Gerência de Acesso (TAM)
- Compliance de Configuração (TSCM)
- Compliance Comportamental (TCIM, TSIEM)
- Gerência de Eventos de Segurança (TSOM, TSIEM)
- Provisionamento (TPM)
- Correlação de Eventos e Dashboard (Netcool)
- Workflow (Maximo)

Perguntas?