4º edição
IBM Security Forum

Utilizando a análise estática e dinâmica para aumentar a segurança em aplicações web

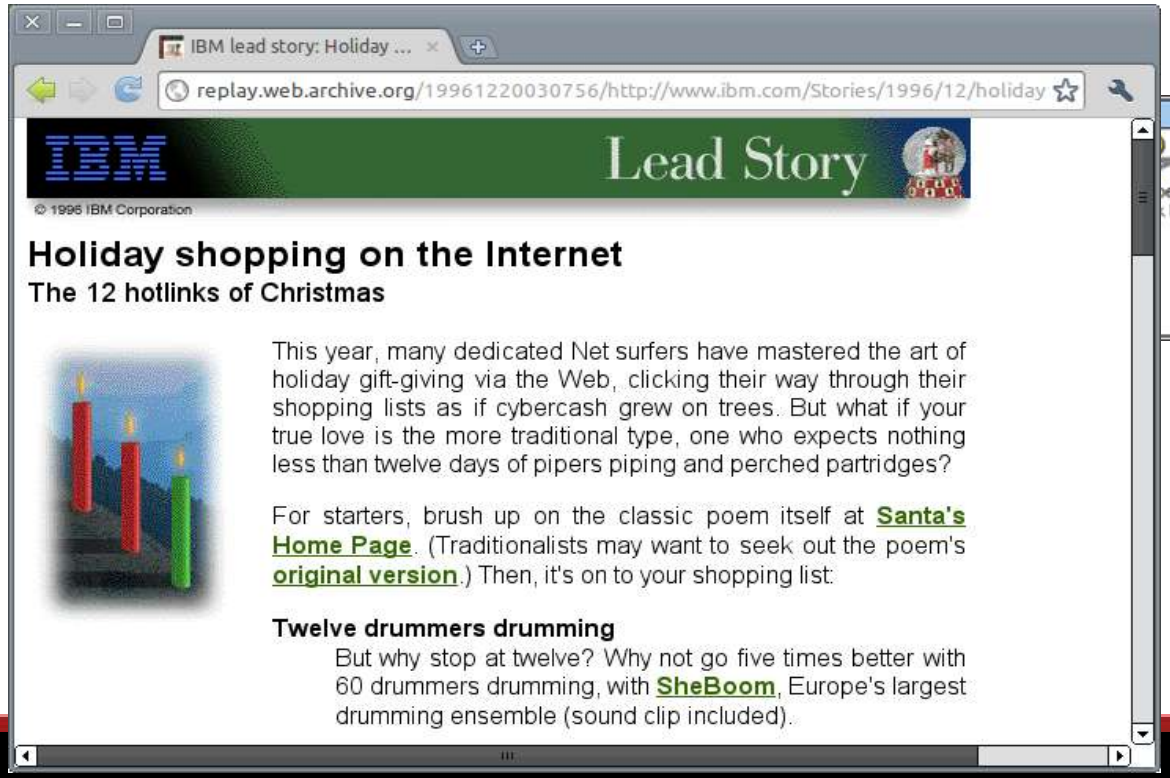
Thiago Canozzo Lahr
Security & Privacy Consultant
IBM Security Services
tclahr@br.ibm.com

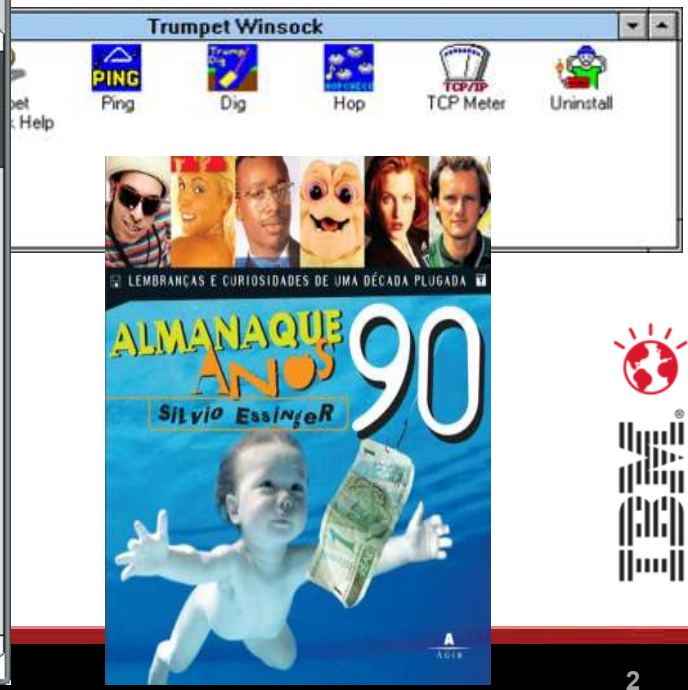
Luis Fernando M. Callado
Senior Deployment Specialist/Mentor
IBM Rational Latin America
callado@br.ibm.com

São Paulo, 28 de Abril de 2011

Introdução

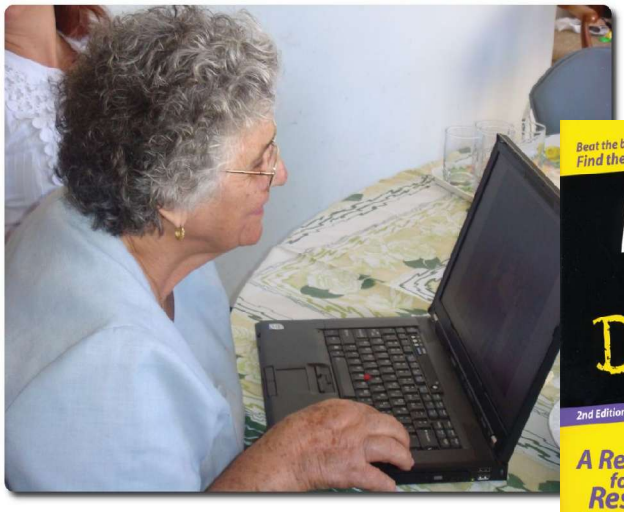
- Inicio dos anos 90
  - Surgimento do protocolo HTTP
  - Páginas estática e sem muita interação com o usuário

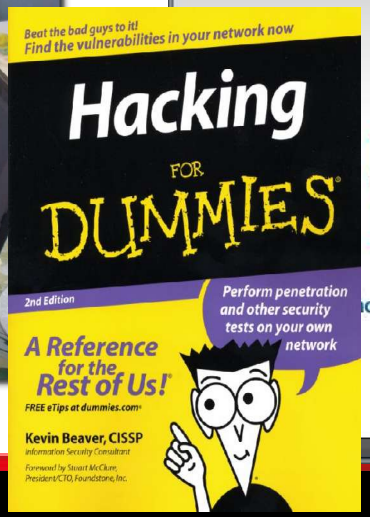




Introdução

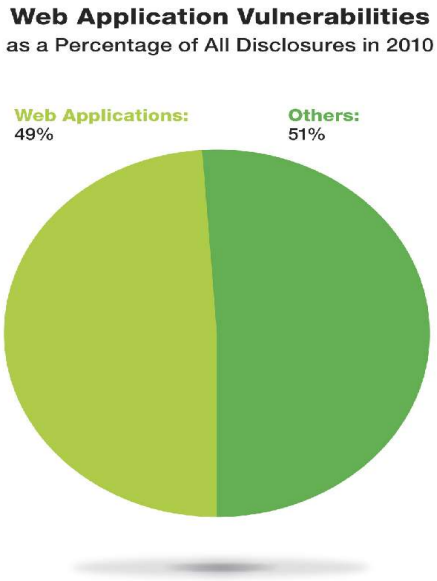
- Web 2.0
  - Internet como plataforma
  - Plataforma primária de desenvolvimento
  - Dados sensíveis
  - **Alvo de ataques!**

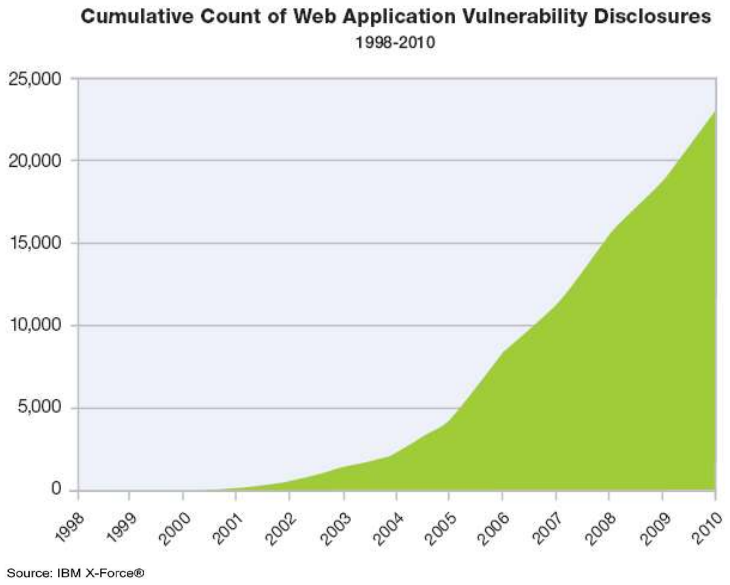


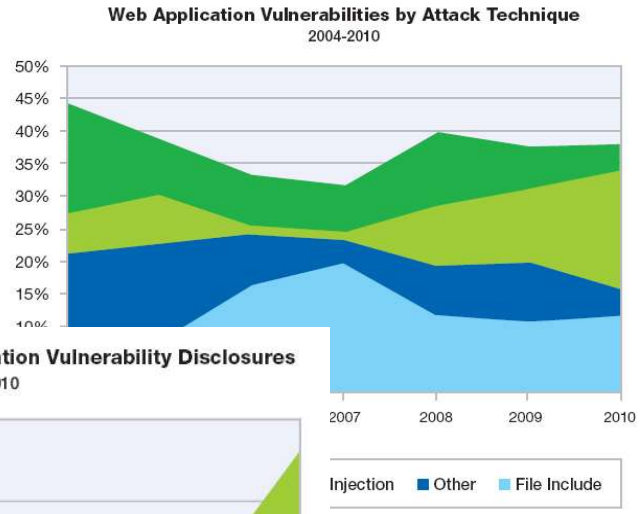


Porque segurança em aplicações web é tão importante?

- Roubo de informações confidenciais
- Quebra da integridade da informação
- Indisponibilidade da aplicação







Preocupações das empresas

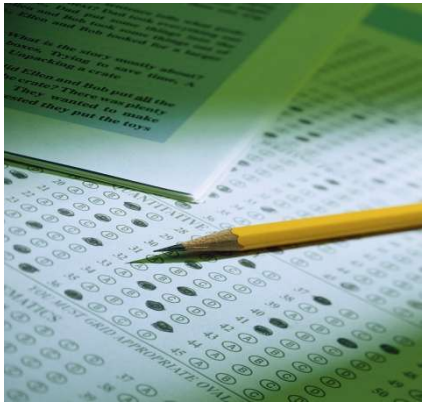
- Identificar riscos e ameaças
- Dificuldades de implementação
- Normas de segurança requerem testes de segurança em aplicações web
- Necessidade de proteger dados críticos e confidenciais
- Visibilidade para os clientes e investidores
- Custos para corrigir problemas pós-produção tem aumentado a necessidade de corrigir problemas de segurança na fase de desenvolvimento

Qual o preço para corrigir uma vulnerabilidade?

80% dos custos de desenvolvimento são gastos para identificar e corrigir problemas
National Institute os Standards & Technology (NIST)

Durante a fase de programação
$25/problema

Durante a fase de compilação
$100/problema



Durante a fase de QA/testes
$450/problema

Uma vez promovido para produção
$16000/problema
+
Problemas com processos, perda de confiança, dano a marca, etc...

* Caper Jones (Applied Software Measurement, 1996)
assumindo 8hs para encontrar, solucionar e corrigir um problema no código fonte da aplicação

Como se proteger?

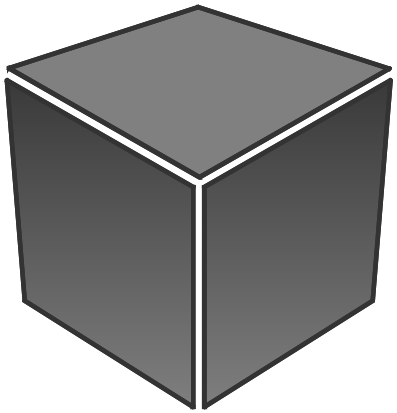
DESENVOLVIMENTO SEGURO

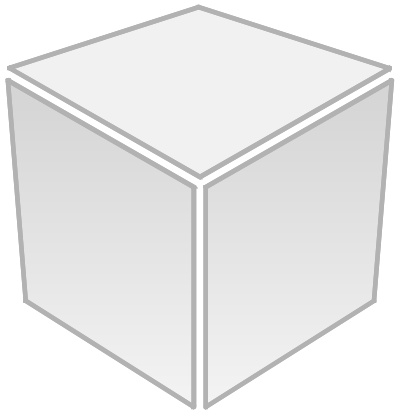
ASSESSMENTS DE SEGURANÇA

- REVISÃO DE CÓDIGO FONTE
- TESTES NA APLICAÇÃO

Análise de segurança em aplicações web

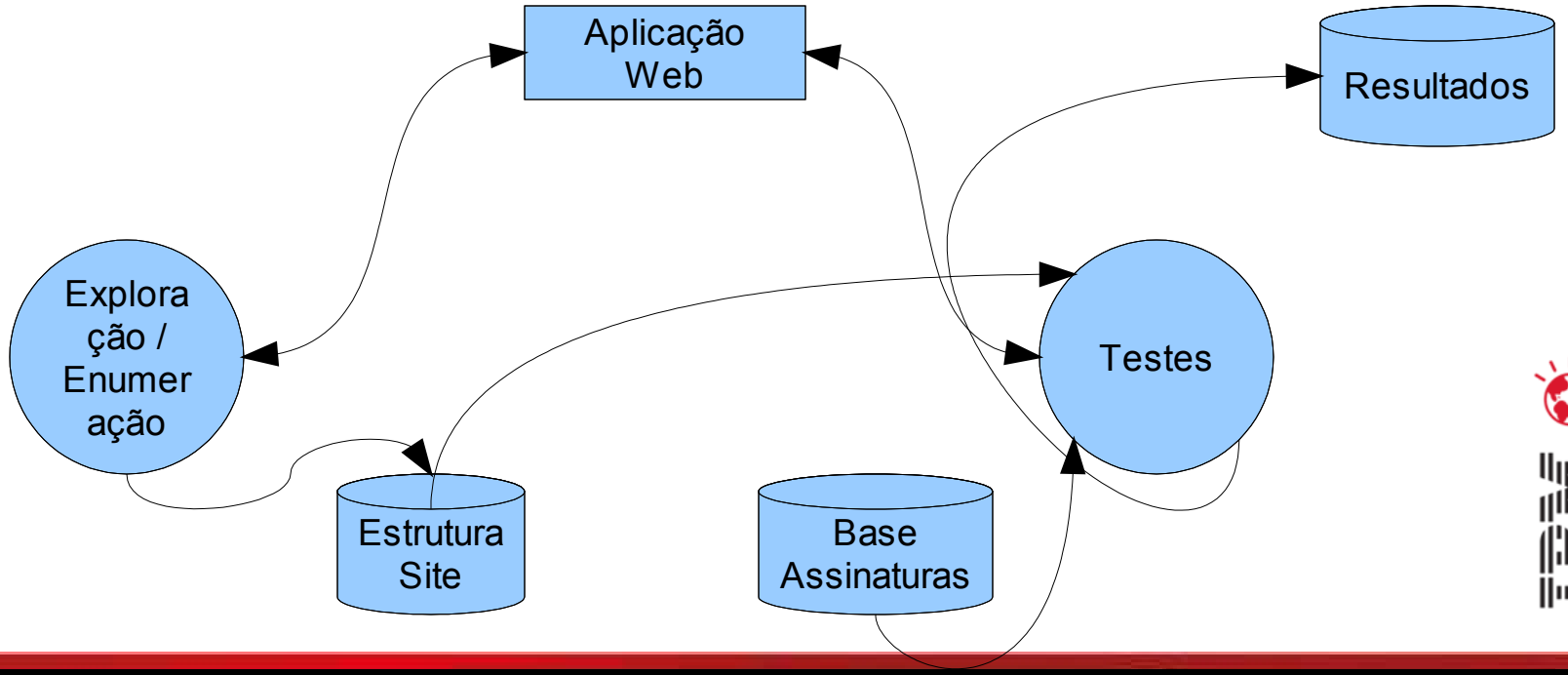
- Metodologias predominantes:
  - Análise estática (testes de caixa-branca)
  - Análise dinâmica (testes de caixa-preta)
- Ambas as abordagens tem como foco encontrar falhas de segurança
- Cada metodologia possui pontos fortes e pontos fracos





O que é Análise Dinâmica?

- Análise de uma aplicação sem conhecimento prévio de informações
- Verificar o comportamento de acordo com vários estímulos



Análise Dinâmica – Pontos Fortes

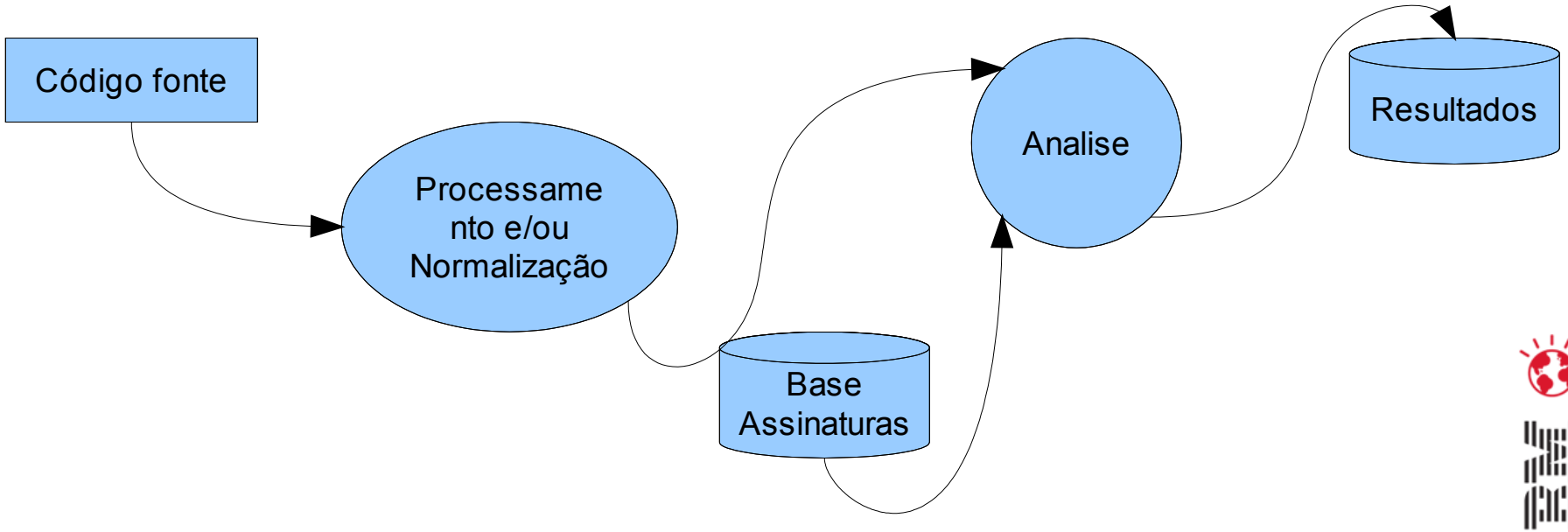
- Testes em aplicações “reais” permitem resultados mais confiantes
- Não há necessidade de especificações de projeto ou código-fonte
- Aplicação é facilmente testada através da rede
- Trabalha como se fosse um atacante
- Diferentes linguagens: maioria das tecnologias server-side

Análise Dinâmica – Pontos Fracos

- Impossível determinar a cobertura de código
- Falhas de lógica estrutural são difíceis de serem encontradas
- Necessita que a aplicação tenha sido implantada
- Testes de “mutações” podem não ter fim

O que é Análise Estática?

- Análise de uma aplicação com conhecimento prévio de informações como código-fonte e desenho estrutural



Análise Estática – Pontos Fortes

- Falhas de lógica estrutural são facilmente identificadas
- Muito efetiva para encontrar erros de programação e de execução
- Similar a auditoria de código

Análise Estática – Pontos Fracos

- Práticas de programação ruins podem resultar em falsos-positivos
- Acesso ao código fonte nem sempre é possível
- Algumas falhas são identificadas somente em ambientes de produção
- Aplicação não pode ser testada remotamente
- Diferentes linguagens requerem suporte especial

Análise Dinâmica		Análise Estática
	Cobertura do código	✓
✓	Necessidade código fonte	
	HTTP	✓
✓	Componentes	
	Estado da aplicação	✓
✓	Pré-requisitos	
✓	Custo implementação	

ANALISE DINÂMICA

- Cobertura do código
- Não necessita código-fonte
  - Somente HTTP
  - Suporte a múltiplos componentes
  - Requer aplicação implementada
  - Poucos pré-requisitos
  - Trabalha como se fosse um atacante

ANÁLISE ESTÁTICA

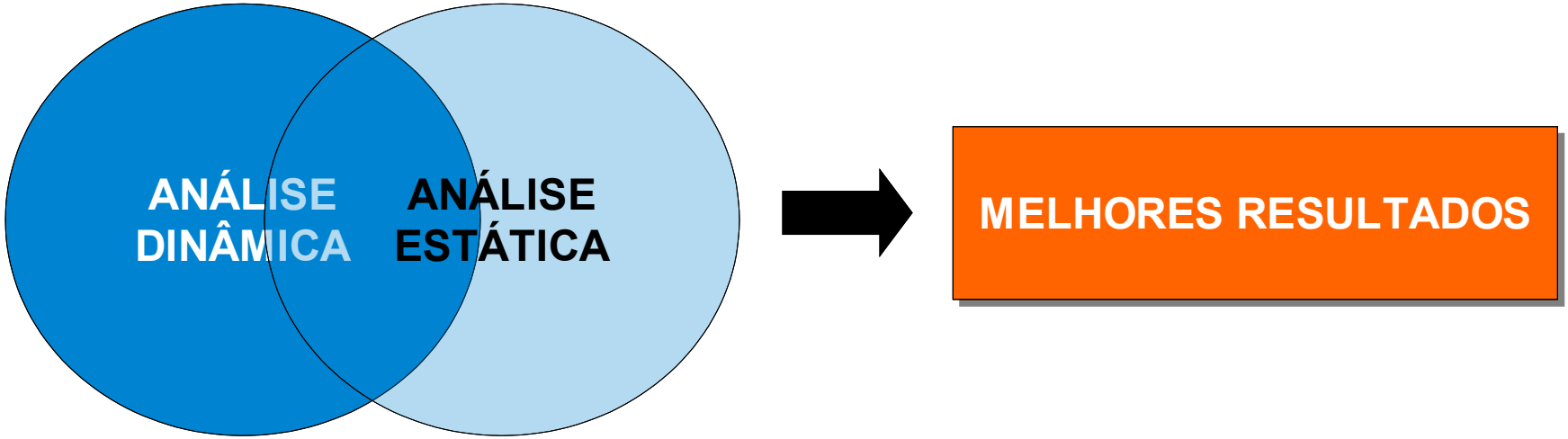
- Cobertura do código
  - Limitado ao código disponível
  - Mais do que validações HTTP
  - Suporte parcial a componentes
  - Requer suporte especial para diferentes linguagens/ frameworks
  - Não requer aplicação implementada
  - Aproximação
  - Problemas com implantação/ integração

E agora?
Analise estática ou dinâmica?

Tomando a decisão

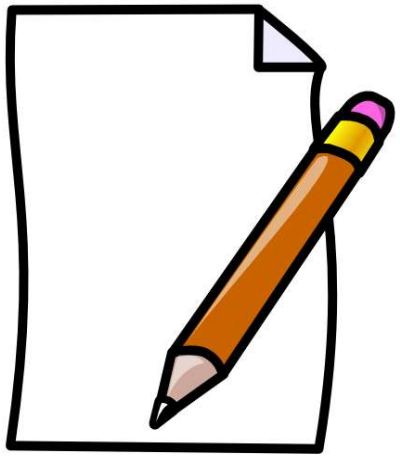
- Depende de algumas variáveis
  - Orçamento
  - Tempo
  - Tecnologia
  - Abilidade (*Skill*)
- Implicações em processos
  - Quem será o responsável por executar as ferramentas?
  - Qual a periodicidade?
  - O que será feito com os resultados?
- Nossa experiência diz que:
  - Analistas de segurança preferem ferramentas de análise dinâmica
  - Desenvolvedores preferem ferramentas de análise estática

Conclusão



Tomem nota!

- Ferramentas são importante, porém uma parte da solução
- Se tempo e custos não fossem uma barreira para as organizações, certamente análise manual seria a melhor opção
- Inteligência humana não pode ser automatizada



Soluções IBM

- A IBM é hoje o único fornecedor no mercado capaz de oferecer o melhor dos dois mundos:
  - Ferramentas:
    - Rational AppScan Standard Edition (análise dinâmica)
    - Rational AppScan Source Edition (análise estática)
  - Serviços:
    - Application Security Assessment (análise dinâmica)
    - Application Source Code Security Assessment (análise estática)
- IBM MSS

Obrigado!

Thiago Canozzo Lahr
Security & Privacy Consultant
IBM Security Services
tclahr@br.ibm.com

Luis Fernando M. Callado
Senior Deployment Specialist/Mentor
IBM Rational Latin America
callado@br.ibm.com