Security & Risk Management

Vulnerabilidades em Aplicações Web

Luiz F Callado
Senior Deployment Specialist/Mentor
IBM Rational Latin America
callado@br.ibm.com

19 de Maio de 2009

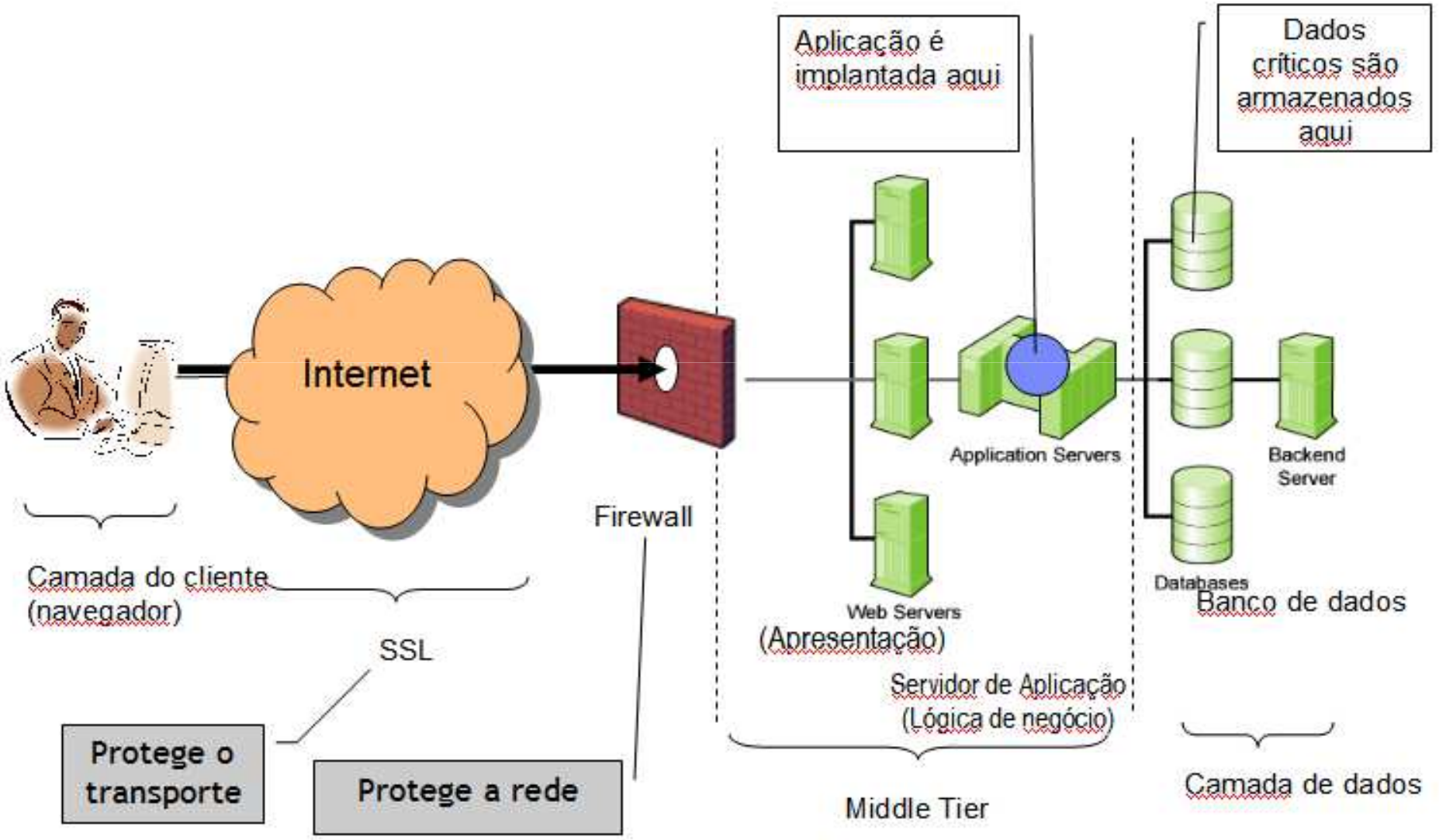
Agenda

- Introdução
- Ameaças na Web
- Porque segurança em aplicações web é prioridade?
- Ataques por categoria
  - Ataques de SQL Injection
- Principais causas de vulnerabilidades
- O Mito: Nosso site está seguro?
- A Realidade: Segurança e gastos estão desequilibrados
- Solução IBM: Hacker Ético + AppScan

Introdução

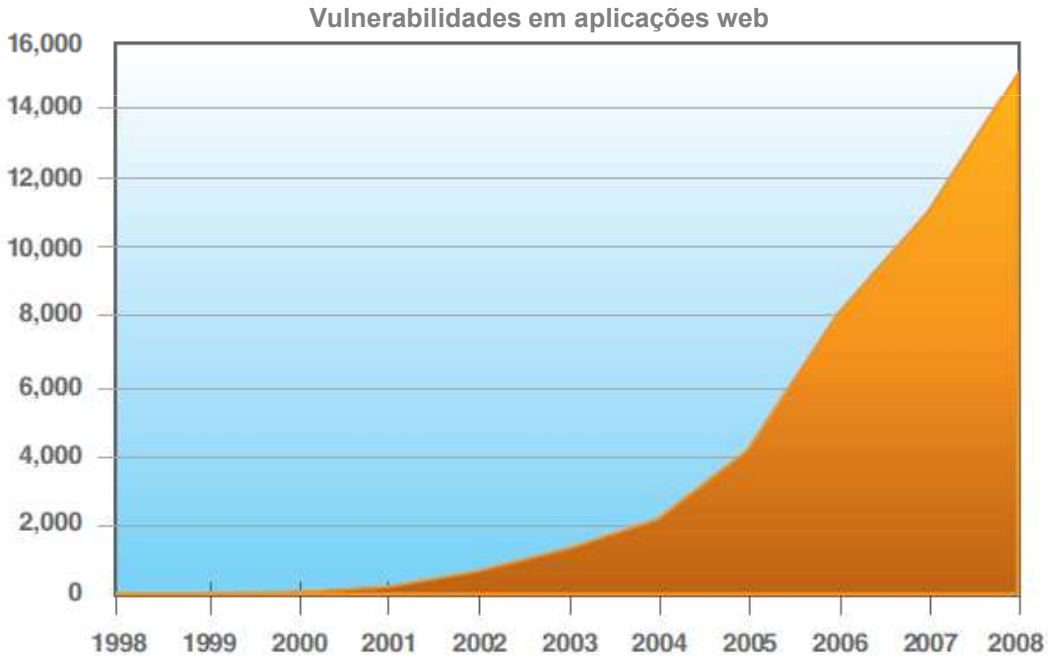
- Inicio dos anos 90
  - Surgimento do protocolo HTTP (Hypertext Transfer Protocol)
  - Maior parte das páginas eram estáticas
  - Sem muita interação com o usuário
  - **Alvo de ataques:**
    - **sistemas operacionais, ftp, banco de dados...**
- Web 2.0
  - Conceito usado pela primeira vez em 2004
  - Novos paradigmas
  - Conteúdo colaborativo
  - Personalização
  - A Internet como plataforma
  - Novas tecnologias
    - AJAX
    - XML
    - RSS
    - Flash
  - **Alvo de ataques:**
    - **servidores web, aplicações web, navegador...**

Estrutura de Uma Aplicação Web



Ameaças na Web

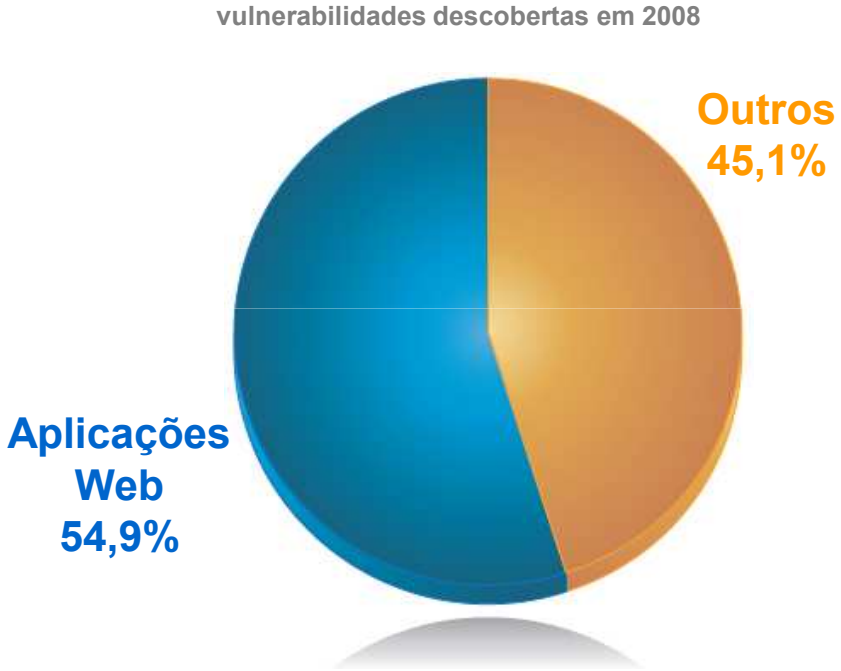
- O número de novos sites maliciosos criados no 4Q2008 superou em 50% o número total visto em 2007
- Aplicações web são consideradas alvos “rentáveis” para criminosos construirem redes de robôs (*botnet*) maliciosos
- Aplicações web tem se tornado o “calcanhar de Aquiles” das empresas de TI. Aproximadamente **55% das vulnerabilidades** descobertas em 2008 afetam aplicações web
- 74% das vulnerabilidades em aplicações web descobertas em 2008, não possuiam pacote de correção disponível até o final de 2008



Fonte: X-Force 2008 Annual Trend & Risk Report

Porque segurança de aplicações web é prioridade?

- O número de vulnerabilidades vem aumentando em comparação aos anos anteriores
- Porcentagem de vulnerabilidades de risco **alto** continua crescendo, e 40% das vulnerabilidades descobertas hoje são consideradas de risco **crítico** ou **alto**
- Requisito **PCI** DSS Seção 6.6 – Garantir que todas aplicações com interface web estão protegidas contra ataques conhecidos



Fonte: X-Force 2008 Annual Trend & Risk Report

Os ataques virtuais causam perdas bilionárias nos EUA.

23/01/2006 - 08h16

Ataques virtuais dão prejuízo de US$ 67 bi aos EUA

da **Folha Online**

Os Estados Unidos perderam, no ano passado, cerca de US$ 67,2 bilhões como conseqüência de crimes virtuais. A informação foi divulgada na última semana pelo FBI (polícia federal norte-americana) e tem como base uma pesquisa realizada com 2.066 empresas norte-americanas.

Cerca de 90% destas organizações disseram ter sofrido problemas de segurança com seus computadores nos últimos 12 meses --um quinto delas afirmaram ter sido atacadas 20 ou mais vezes durante o período.

A importância é tamanha que até o governo está procurando orientar os consumidores...

Ministério do Desenvolvimento, Indústria e Comércio Exterior

Destaques do governo

PORTAL DO CONSUMIDOR
Portal de Informações para o Consumidor

Serviços | Biblioteca | Contato | Parceiros | Mapa do Site

Procurar por notícias: Buscar

Notícias

Internet: ataques de phishing causam roubo de senhas e prejuízos para o consumidor
26/12/2007

SÃO PAULO - Perder dinheiro por conta de ataques digitais que roubam números e senhas de contas bancárias e cartões de crédito é preocupação de muitos brasileiros. O principal golpe de roubo na internet é o phishing que, de acordo com pesquisa do Gartner, gerou prejuízo de mais de US$ 3,2 bilhões somente nos Estados Unidos.

A técnica consiste em enviar ao usuário e-mails com mensagens atrativas, como "Tire seu nome do cadastro de inadimplentes" ou "Veja as fotos da festa de sexta-feira" que, ao serem clicadas, realizam o download de um software no computador.

Ocorrência
Em todo o mundo, são enviados diariamente quase 8 milhões de e-mails com a modalidade de fraude. O Brasil e os Estados Unidos estão os países com maior ocorrência desse tipo de ataque.

Um levantamento da empresa de tecnologia Unisys, feito com 1,5 mil brasileiros, comprovou que 94% temem as ameaças virtuais, sendo que 79% afirmaram que se sentem extremamente preocupados com os ataques.

Já a pesquisa do Gartner aponta que, somente nos Estados Unidos, 3,6 bilhões de pessoas sofreram ataques phishing em 2007.

De 4.500 usuários entrevistados, 3,3% afirmaram terem recebido e-mails phishing em 2007. No ano passado, esse índice era de 2,3%. Estima-se que, por golpe, sejam roubados US$ 886.

Segurança
Para o especialista em segurança digital, Sérgio Leandro, o roubo de identidade pela web é uma fraude que tem crescido no Brasil, pois, a cada dia, aumenta o número de pessoas com acesso à internet e, conseqüentemente, o número de transações bancárias *on-line* e compras virtuais.

Para fugir destes golpes, o especialista dá algumas dicas:

- Nunca faça downloads de software desconhecido a partir de e-mails que não reconhece;
- Procure sempre digitar o endereço URL da página web que pretende acessar. A fraude por phishing utiliza links que, de forma camuflada, encaminham o usuário para falsos sites dos bancos. É sempre mais seguro digitar o endereço do banco diretamente no browser, para garantir que está no site legítimo;
- Sempre que receber um e-mail suspeito, não abra arquivos anexos nem clique nos links;
- Cheque se o cadeado do site realmente refere-se à identidade apresentada;
- Dados bancários ou de cartões de crédito só devem ser enviados se o comprador iniciou uma negociação. Empresas sérias nunca solicitam dados de confirmação e muito menos senhas. Estas são pessoais e intransferíveis;
- Ao comprar pela internet, jamais passe dados pessoais ou financeiros por e-mail. De novo, empresas confiáveis solicitam essas informações no próprio site, informando claramente os aspectos de segurança e condições comerciais.

Fonte: Infomoney

Foco no Roubo de Informações

Invasão de sistema expõe dados de 310 mil

Classificação: OOOOO / 0

Fraco ◯ ◯ ◯ ◯ ◉ Bom Avaliar

14-Abr-2005

Uma investigação interna na divisão LexisNexis da editora e provedora de informações Reed Elsevier descobriu evidências de que cerca de 310 mil pessoas podem ter seus dados pessoais expostos. Segundo a empresa, indivíduos não autorizados tiveram acesso ao banco de dados com informações como o seguro social e os números das carteiras de habilitações de seus clientes.
Em um comunicado, a empresa afirmou que foram 59 incidentes de s
ocorridos em seus sistemas. Inicialmente, 30 mil clientes tiveram seu
roubados, e desta vez, outros 280 mil nomes também podem estar

No golpe, os invasores utilizaram senhas e nomes de clientes legítim
ganhar acesso aos dados pessoais.

A LexisNexis é proprietária da Seisint, empresa que mantém em seu
de informações com dados pessoais de cidadãos norte-americanos,
segurança social, históricos de crédito e registros criminais.

A empresa divulgou nos últimos anos os dados que mantém no siste
Terrorism Information Exchange), programa que compartilha os dad
autoridades norte-americanas.

Depois do incidente, a LexisNexis informou que vai reforçar seus sis
News Service, EUA

0 Pontos

Subir

07/01/2006 - 16h01

Piratas concentram foco no roubo de informações

JULIANA CARPANEZ
da **Folha Online**

Nada de apagar arquivos, travar programas ou alterar dados. Um estudo global da empresa britânica de segurança Sophos mostra que o foco dos piratas virtuais está cada vez mais voltado para o roubo de informações --o objetivo final destas ações são os ganhos financeiros. Em 2005, os programas que repassam dados de micros infectados a pessoas mal-intencionadas (pragas conhecidas como cavalos de tróia) responderam por 62% das infecções.

No Brasil, o padrão se mantém, segundo dados do Cert.br (Centro de Estudos, Respostas e Tratamentos de Incidentes de Segurança no Brasil), um dos braços do Comitê Gestor da Internet no Brasil.

Em 2005, as tentativas de fraudes virtuais no país aumentaram 579% em relação ao ano anterior. No ano passado, quando o centro recebeu 68 mil notificações sobre incidentes, 27.292 (ou 40%) referiam-se a tentativas de fraudes virtuais. Já em 2004, elas responderam por apenas 4.015 dos 75.722 problemas reportados (5,3% do total).

Os clientes de muitas empresas estão sofrendo com os ataques...

Arquivo

Ataques de phishing causam prejuízos de 2,8 mil milhões de dólares nos Estados Unidos

Publicado por Casa dos Bits às 10.22h no dia 13 de Novembro de 2006 | 0 comentários

A- A+

No último ano, os indivíduos com rendimentos superiores a 100 mil dólares receberam uma média 112 ataques de *phishing* por *email* contra apenas 74 registados entre aqueles que ganham menos, mostram os dados da Gartner.

As mensagens fraudulentas são enviadas por fontes supostamente seguras, que utilizam *links* para *sites* - muitas vezes de bancos - para roubar informações confidenciais aos utilizadores.

Os que mais recebem estas mensagens são também os que mais perdem com estes ataques. A média é de 4,36 mil dólares por utilizador, enquanto os que obtêm rendimentos inferiores perdem perto de 1,24 mil dólares.

O relatório diz que 109 milhões de adultos norte-americanos foram sujeitos a ataques de *phishing* este ano, contra os 79 milhões registados há dois anos. A média do prejuízo por pessoa este ano é de 1,244 mil dólares enquanto, no ano passado, os valores roubados não iam além dos 257 dólares por pessoa.

Outro dos dados negativos referidos pela consultora é que, apesar dos números aumentarem, existe um que, pelo contrário, diminuiu: a taxa de recuperação do dinheiro roubado. Este ano apenas 54 por cento dos valores voltaram a ser repostos, contra 80 por cento em 2005.

Em 2006 os prejuízos globais devem chegar aos 2,8 mil milhões de dólares nos Estados Unidos, refere a Gartner, salientando que as estratégias utilizadas pelos criminosos são cada vez mais apuradas e difíceis de detectar.

E os seus clientes também estão preocupados com isso...

BANCO DE NOTÍCIAS

Roubo de informações é o maior medo de 26% dos usuários

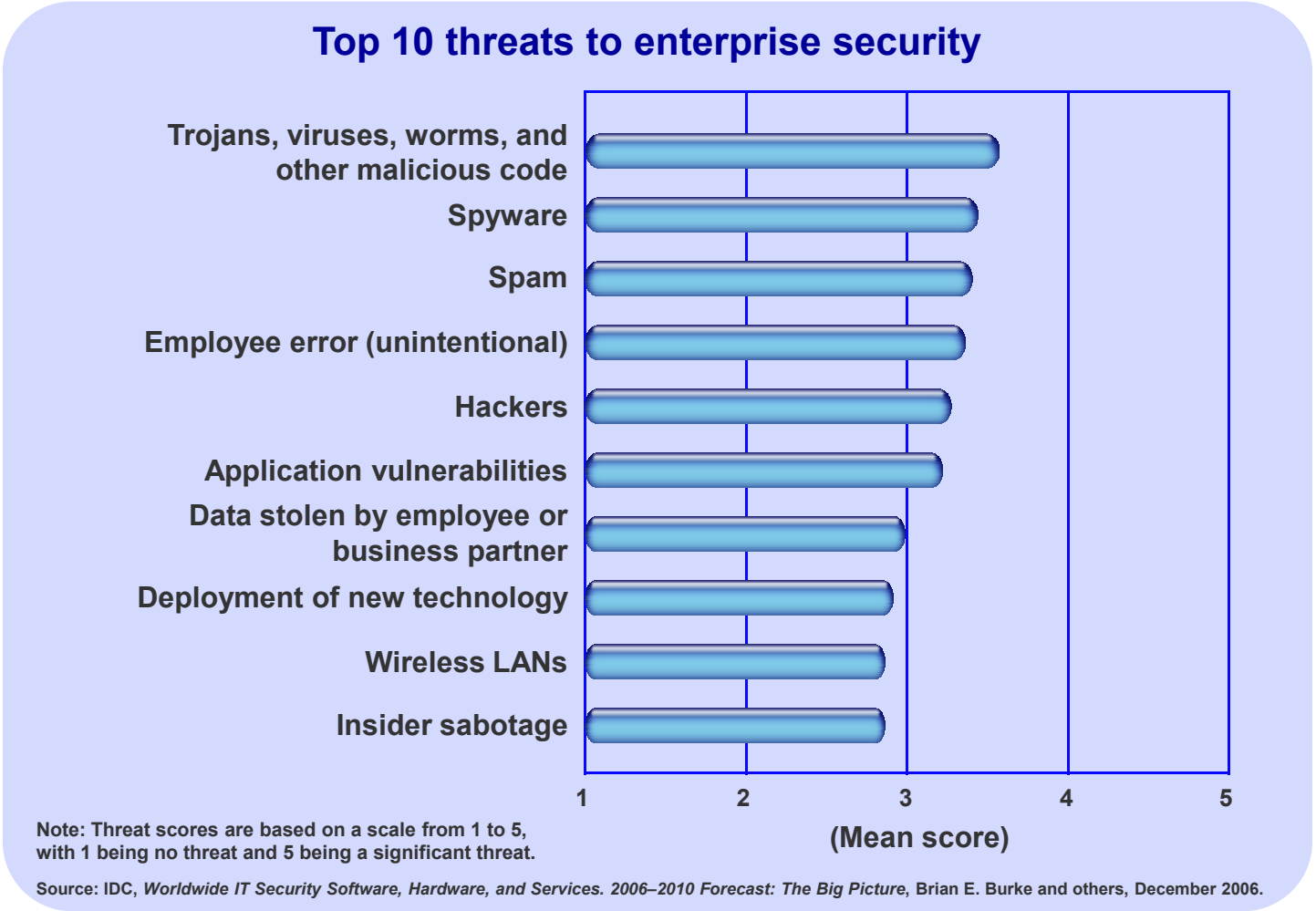
Data: 2006/07/10
Fonte: Módulo Security Magazine

(da Redação)

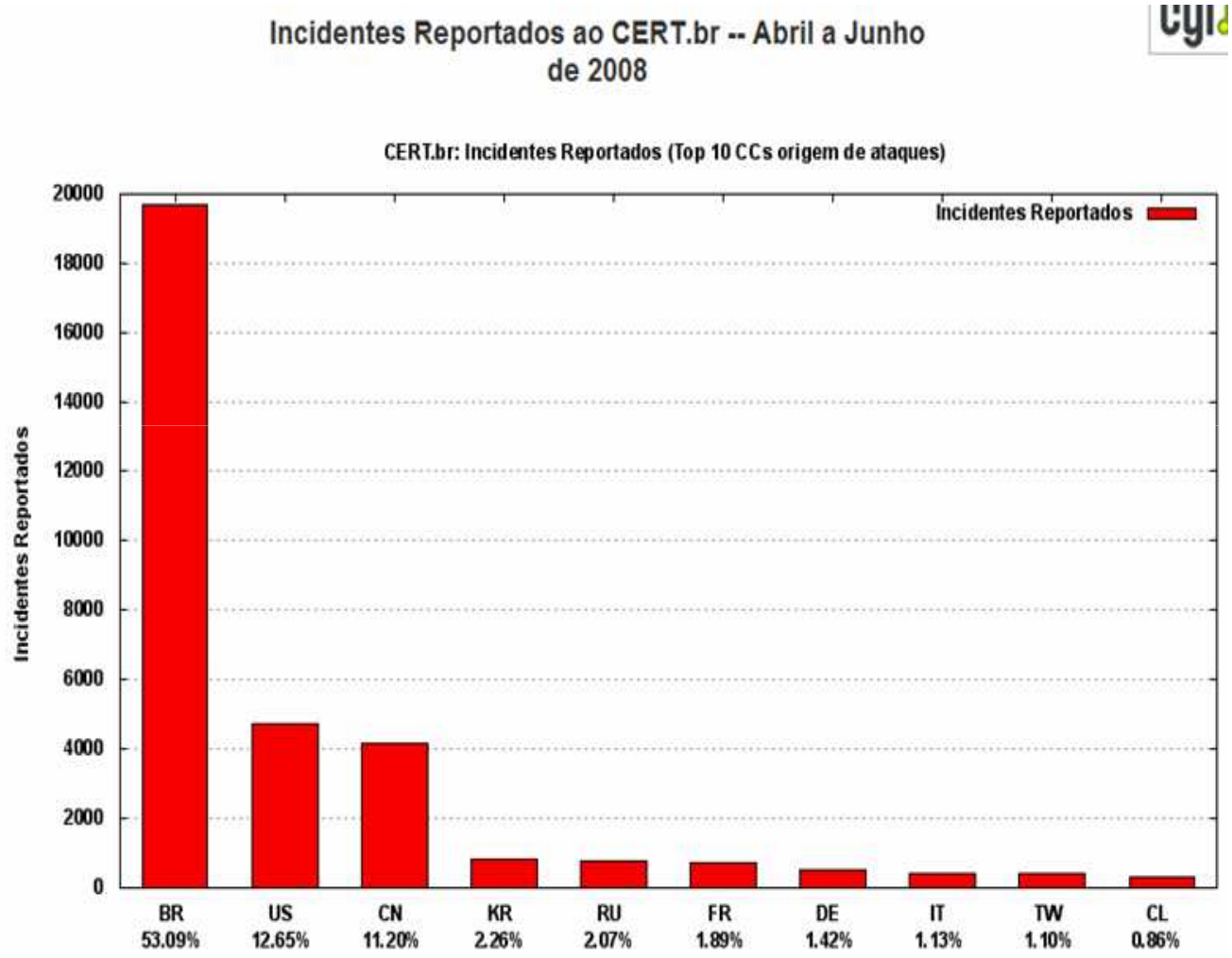
Um estudo da União Internacional de Telecomunicações (UIT), órgão da ONU, anunciou que o maior temor de 26% dos usuários é terem suas informações pessoais roubadas. A pesquisa concluiu que o medo de ameaças como spywares, phishing scans e spams é o maior obstáculo para o desenvolvimento de uma sociedade informatizada.

O estudo revelou ainda que 64% dos entrevistados deixam de fazer algo na web por preocupações com a Segurança da Informação. Além do roubo de dados pessoais, um quarto dos usuários teme vírus e worms, 19% possuem medo de spywares e 13% de fraudes como phishing scan.

Considerando as estatísticas dos principais problemas de Segurança, temos:



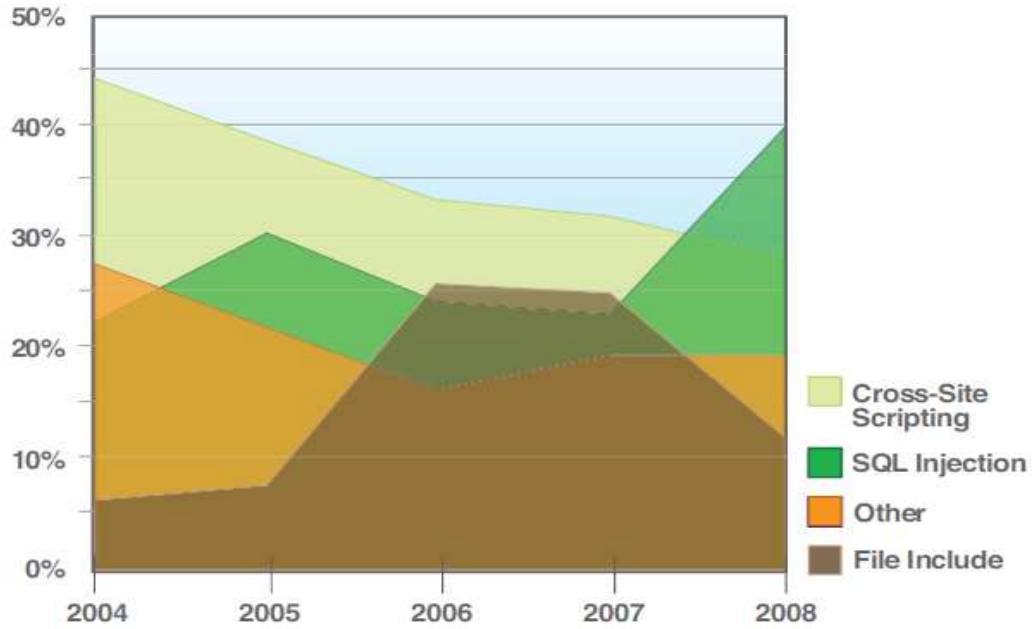
Total de incidentes reportados ao CERT.BR por ano



Ataques por categoria

- As 3 vulnerabilidades que mais aparecem em aplicações web são:
  - **SQL Injection**
  - **Cross Site Scripting (XSS)**
  - **File Include**

- Em 2008, as falhas relacionadas ao *SQL Injection* aumentaram mais do que o dobro do ano anterior, ultrapassando o número de ataques de *Cross Site Scripting (XSS)*



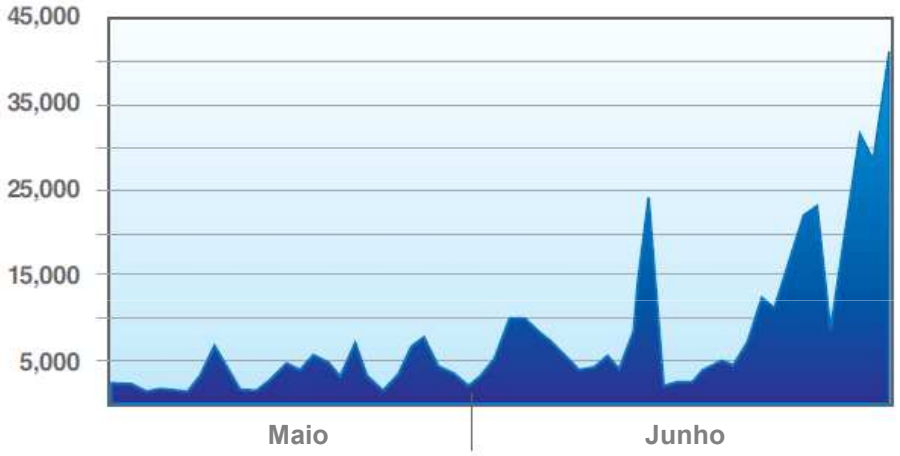
Fonte: X-Force 2008 Annual Trend & Risk Report

Entendendo melhor XSS e SQL Injection

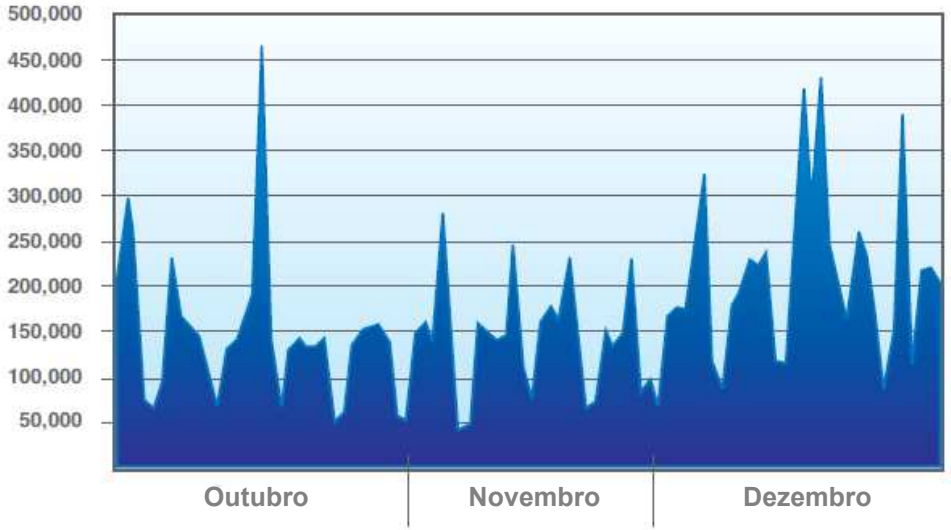
- XSS (Cross Site Scripting)
  - Cross Site Scripting -> Induzir o browser do usuário a executar um script malicioso dentro do contexto de um site confiável.
  - A exploração bem sucedida deste ataque permite ao hacker embutir um código malicioso (na forma de Javascript ou VBScript) em campos de entrada, os quais são inseridos de volta para a resposta do servidor. Isto permite ao hacker a execução de um código arbitrário em um usuário desatento que tenha acesso permitido ao site escolhido como vítima.
- SQL Injection
  - Algumas aplicações não validam as entradas de usuários permitindo que hackers executem comandos diretamente no banco de dados de uma aplicação. Este ataque permite ao hacker alterar valores do SQL, concatenar declarações SQL, adicionar chamadas de função e procedimentos de armazenagem para uma declaração, entre outras ações.
  - O sucesso na exploração deste ataque poderia resultar no acesso não autorizado aos dados, manipulação de registro e no comprometimento geral do servidor.

Ataques de *SQL Injection*

- A quantidade de ataques manuais e automatizados *(botnets)* usando *SQL Injection* teve um aumento significativo no final de 2008



Fonte: X-Force 2008 Annual Trend & Risk Report



Fonte: X-Force 2008 Annual Trend & Risk Report

Principais causas de vulnerabilidades

Principal Causa → **Usuários podem submeter dados de entrada arbitrários**

- **Principais sinais de problemas:**
  - Imaturidade em segurança
  - Desenvolvimento *in-house*
  - Percepção de simplicidade
  - Restrições de recursos e tempo
  - Mau uso de tecnologias

"64% dos desenvolvedores não tem confiança na sua própria capacidade de escrever código de aplicações seguras."

Microsoft Developer Research

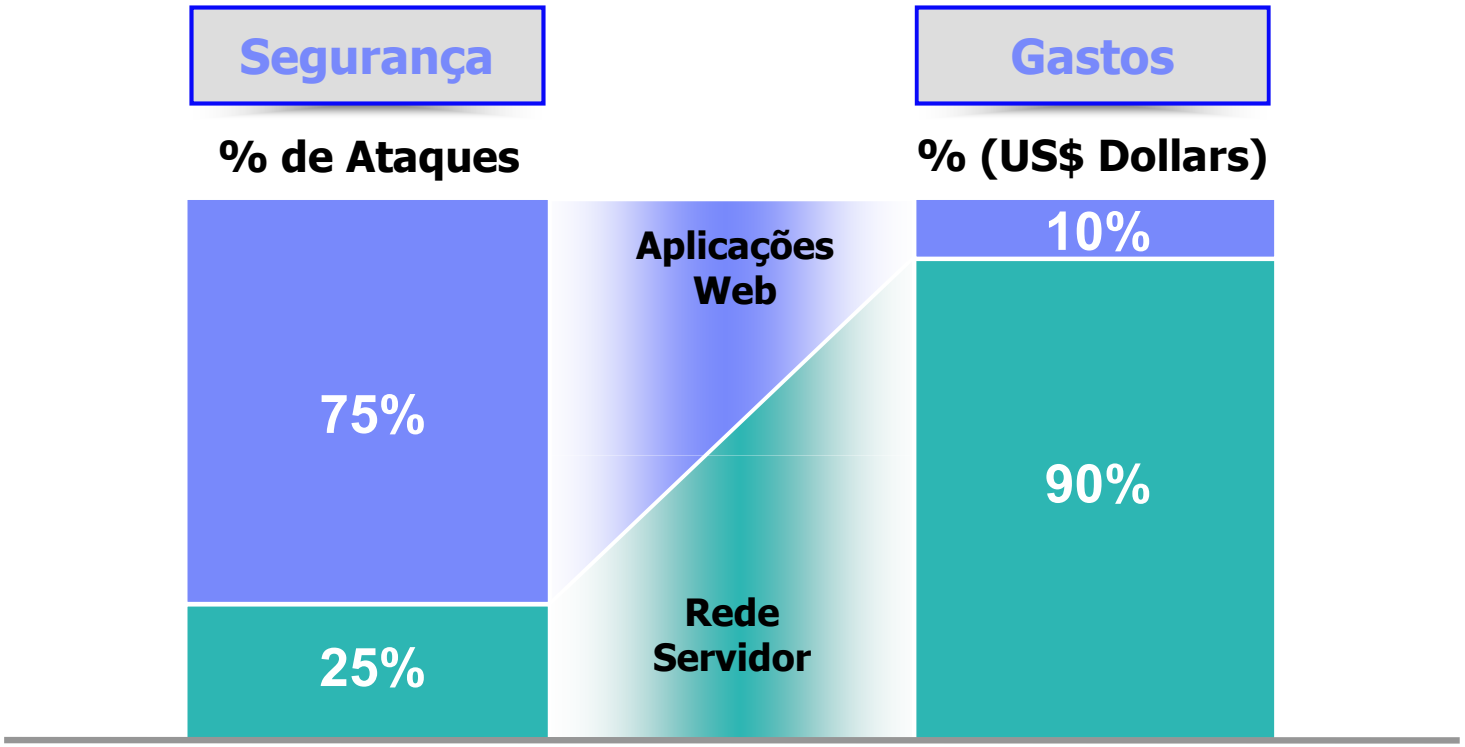
O Mito: Nosso site está seguro?

Nós temos firewalls

Nós fazemos auditoria de segurança 1 vez por semestre

Nós utilizamos network scanners

A Realidade: Segurança e gastos estão desequilibrados



75% de todos os ataques são direcionados à camada de aplicação web

2/3 de todas as aplicações web estão vulneráveis

Gartner

Estratégia

Endereçando a Segurança de Aplicações

Opções para a Segurança de Aplicações Web

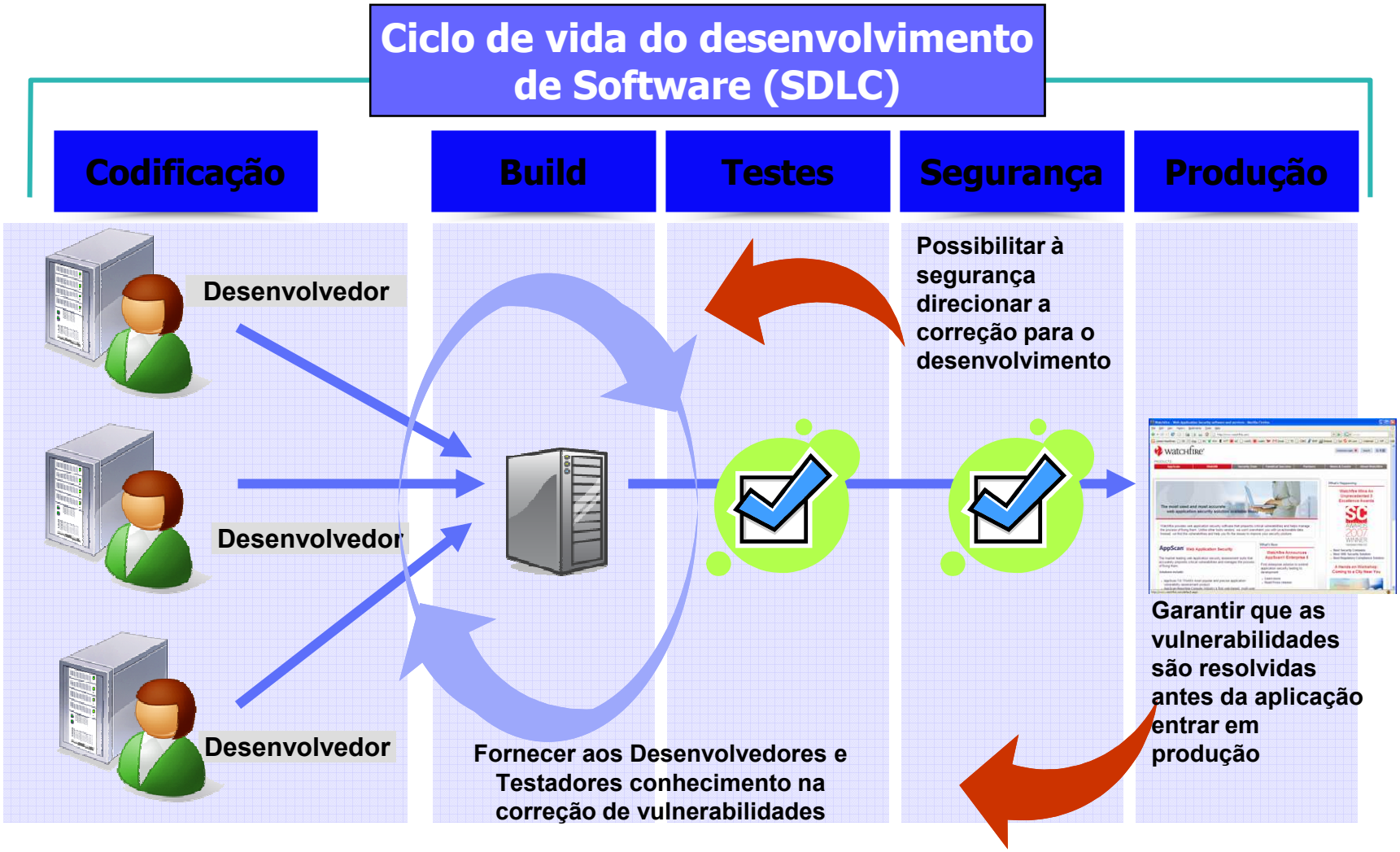
Estratégico
- Solução Corporativa
- Escalável

Tática interna
- Esforços manuals
- Ferramentas na estação de trabalho
- 2-3 Especialistas em segurança (internos)

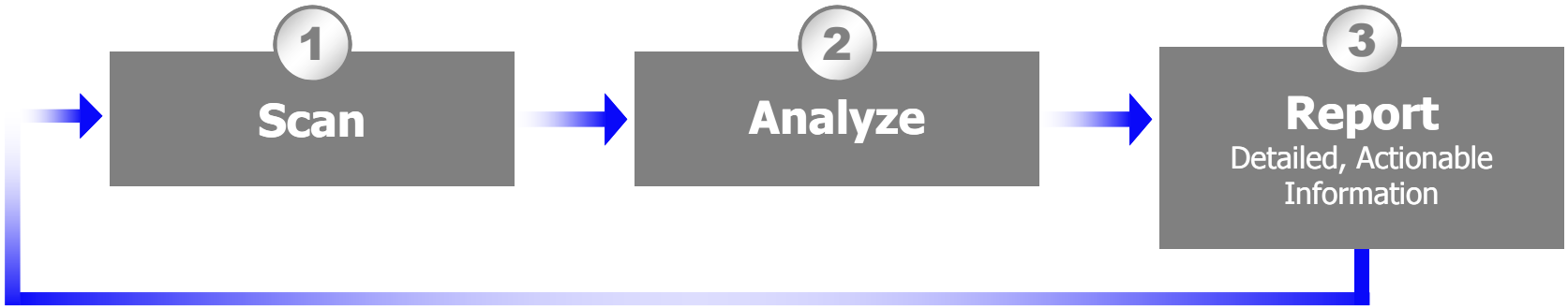
Subcontratar
- Consultores
- *"Penetration Tester"*

Não fazer nada

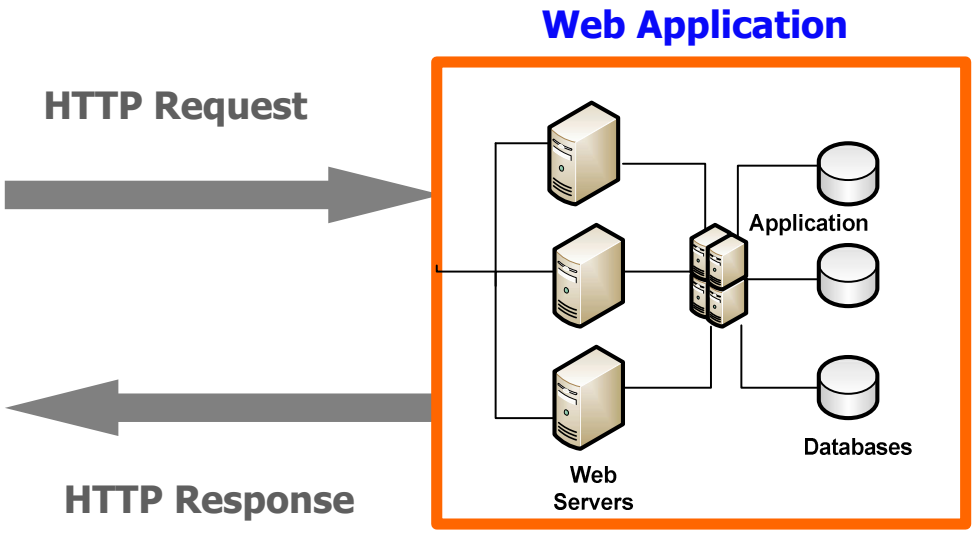
Resolver antes custa menos!



Como funciona o Rational AppScan?

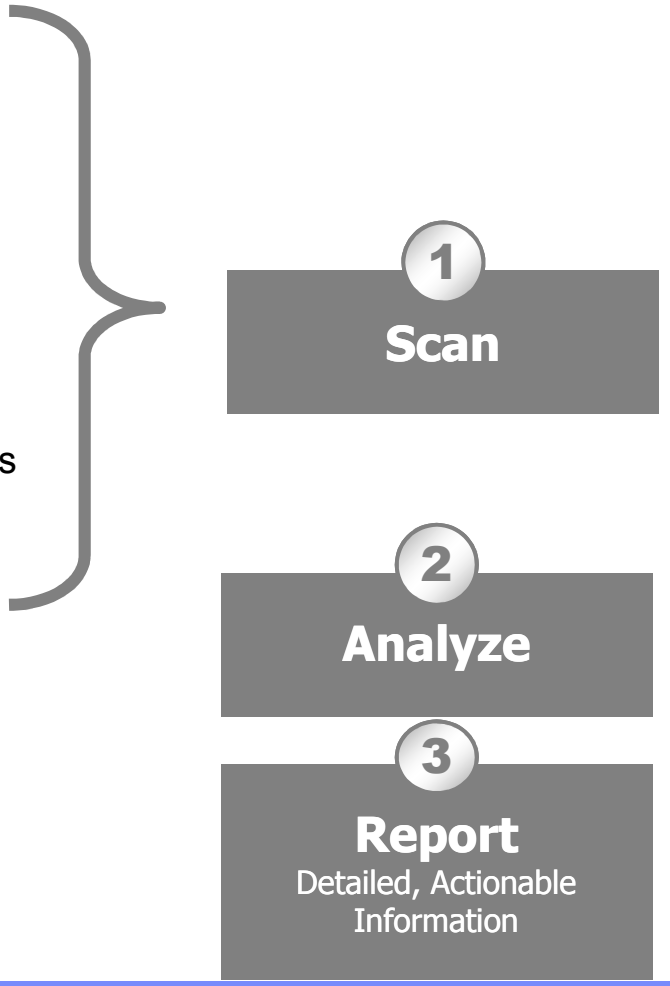


- Approaches an application as a **black-box**
- Traverses a web application and builds the site model
- Determines the attack vectors based on the selected **Test policy**
- Tests by sending modified HTTP requests to the application and examining the HTTP response according to validate rules



Visão geral do processo de testes – SCAN

1. **Identificação da aplicação a ser testada**
   - Formulário de avaliação de sistema
   - Identificação de riscos
   - Escopo do scan
     - Intrusivo / não-instrusivo
2. **Construção da configuração do scan**
   - Definição de políticas de testes
   - Crawling da aplicação (automatizado ou manual) – transações avaliadas
3. **Execução do Scan**
4. **Avaliação dos resultados**
   - Validação / Identificação de falso positivos
5. **Elaboração de relatórios**
   - +40 templates de relatórios



Exemplos de varreduras

Quick scan

- Executor: **Desenvolvedor**
- Template: Vital Few
- Aplicação: Internet Banking

- Total de URLs “scaneadas”: 114
- Total de testes efetuados: 4.902

- Tempo preparação: **5 minutos**

- Tempo execução: **16 minutos**

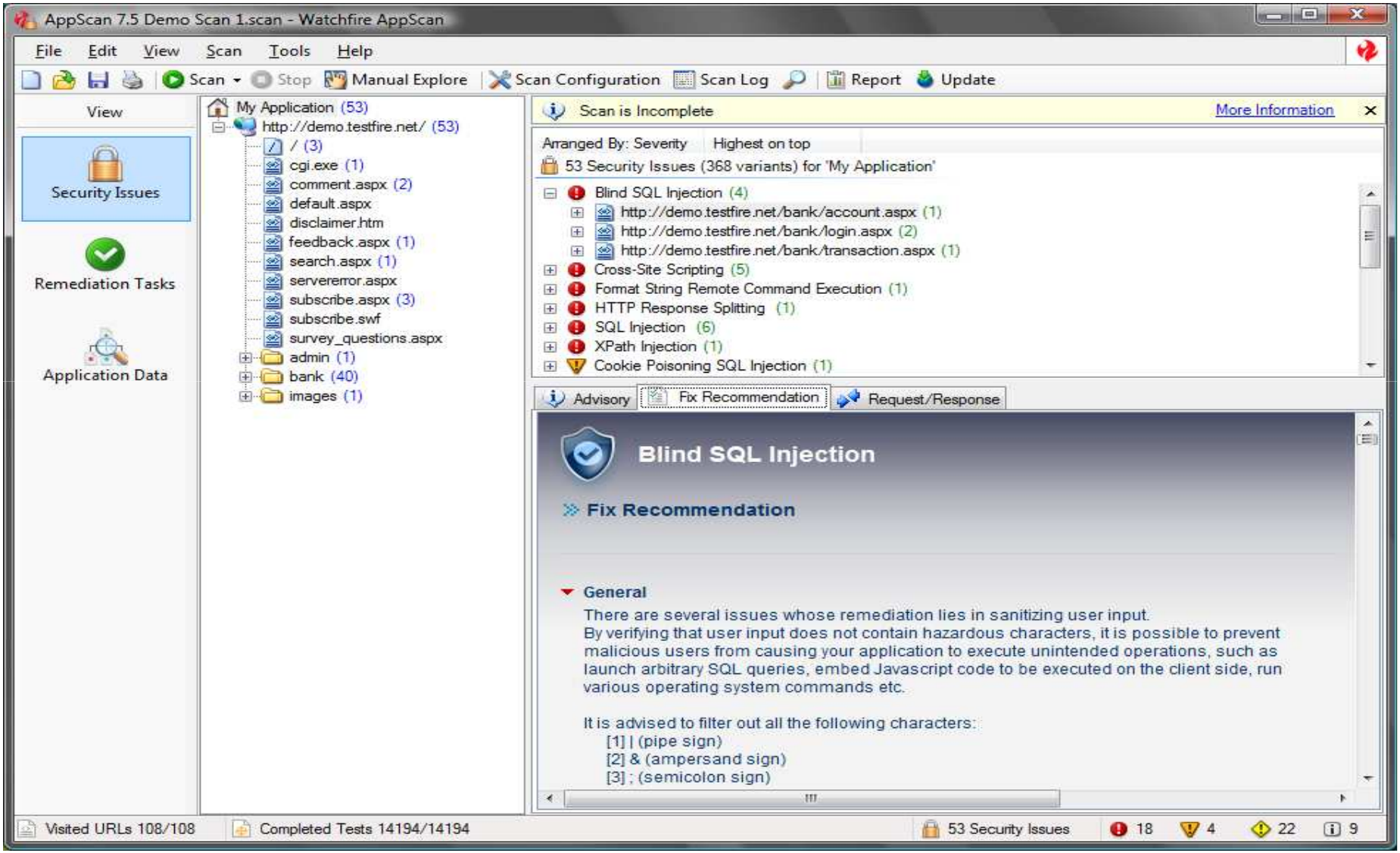
Scan padrão

- Executor: **Analista de Segurança**
- Template: Application-Only
- Aplicação: Internet Banking

- Total de URLs “scaneadas”: 156
- Total de testes efetuados: 37.200

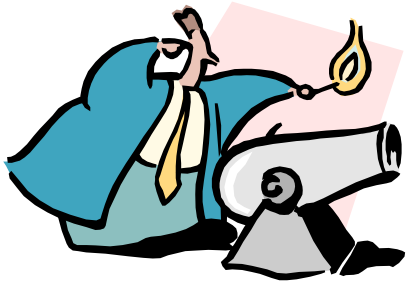
- Tempo preparação: **20 minutos**
  - Indutor de estados
  - Preenchimento de formulários
- Tempo execução: **34 minutos**

Também faz recomendações de consertos



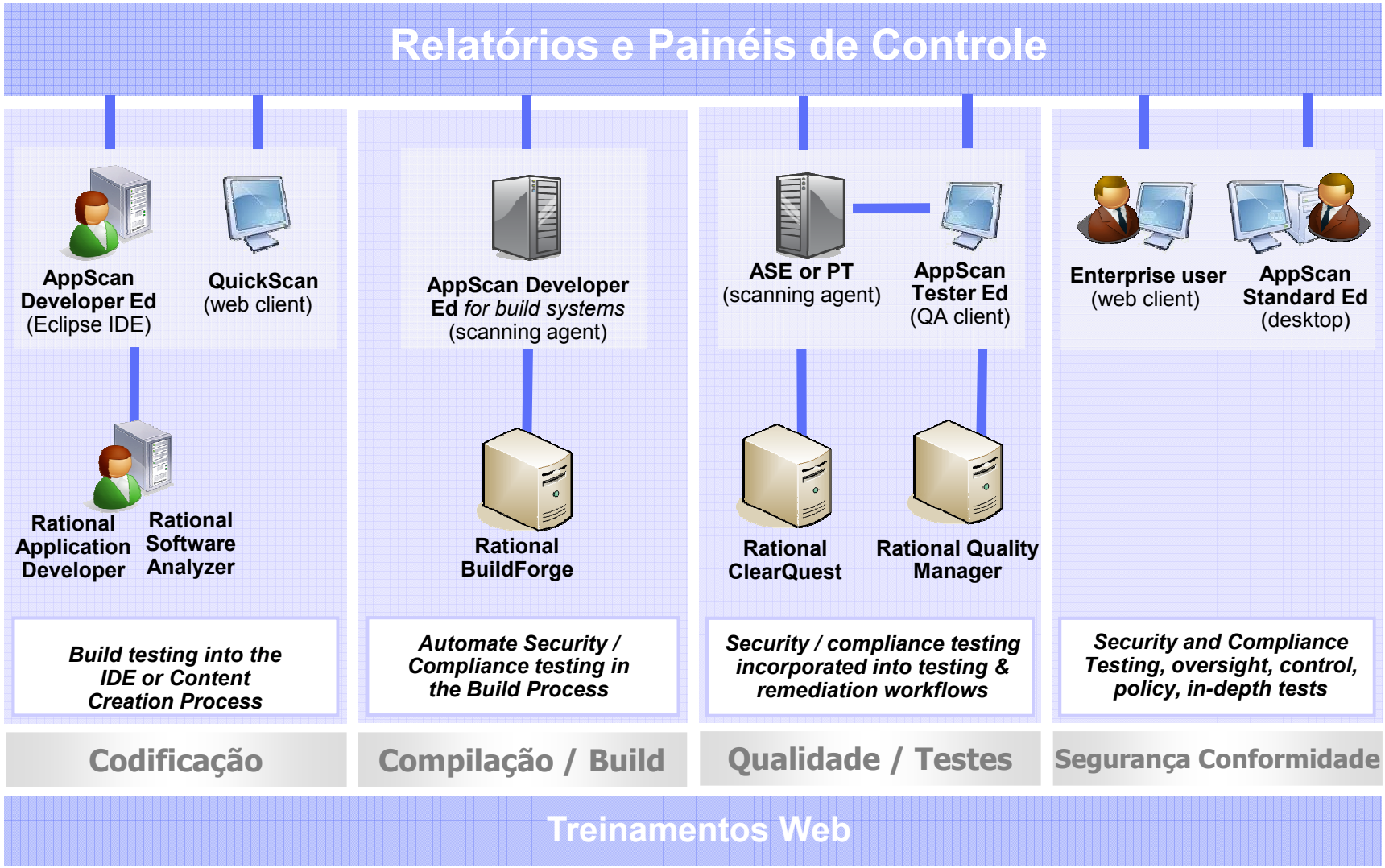
Hacker ético x Ferramenta de automação (AppScan)

- *Atuação complementar*
- *Vantagens da **ferramenta***
  - *Abrangência dos testes*
    - *Centenas de tipos diferentes de testes na base de conhecimento da ferramenta*
  - *Volume de testes executados*
  - *Cobertura da aplicação*



- *Vantagens do **hacker ético***
  - *Capacidade analítica*
  - *Compreensão dos riscos*
    - *Possibilidade de focar em testes específicos e com profundidade*

Soluções do AppScan no Ciclo de Vida de Desenvolvimento



800+ Companies [illegible] chfire

#1 in Market Share for Application Security
– Gartner & IDC

9 of the Top 10 Largest U.S. Retail Banks	8 [illegible]	[illegible]op 10 [illegible]Clinical [illegible]nies	Multiple Large Government Agencies
Bank of America – Higher Standards	Microsoft	Novartis	Veteran's Affairs
Citi	Intel	AstraZeneca	Army
JPMorgan	Nokia	Abbott Laboratories	Navy
Wells Fargo	Cisco Systems	Aventis	Air Force
Wachovia	Sony	Roche	Marines
Washington Mutual	Dell	Genentech	Social Security USA Administration
US Bank			United States Postal Service
SunTrust			

SC Magazine Awards 2007 Winner – Best S[illegible]curity Com[illegible]any

- Large, Complex Web Sites
- Extensive Customer Data
- Heavily Regulated
- High User Volume

Pergunte-se

- O que os desenvolvedores e testadores da minha organização sabem sobre segurança da informação?
- Eles têm meios de prevenir vulnerabilidades?
- Apesar de nosso investimento em segurança de rede, será que realmente estamos seguros?
- Ainda que esteja seguro hoje, tenho como garantir que não haverá falhas de segurança no futuro?

Muito Obrigado!

SEGURANÇA NÃO É UM EVENTO ÚNICO

- *Ensure Web site security and compliance - IBM Rational Web site security and Web site compliance*
  - *http://www-01.ibm.com/software/rational/offerings/websecurity/*
- IBM Internet Security Systems
  - *http://www.iss.net*
- OWASP: *How to build, design and test the security of web applications and web services.*
  - *http://www.owasp.org*

Luiz F Callado
Senior Deployment Specialist/Mentor
IBM Rational Latin America
callado@br.ibm.com