



THE DEVELOPER'S CONFERENCE

Software Seguro
Na prática a Teoria é Diferente

Declarações

- › Todo conteúdo aqui apresentado diz respeito à minha própria opinião, ficando isenta toda empresa e/ou organização para qual eu trabalhe, represente ou preste serviços, de qualquer responsabilidade sobre o conteúdo aqui apresentado.
- › As opiniões apresentadas não correspondem a verdade, ficando restritas ao pensamento do autor.
- › As informações aqui apresentadas, quando citada a fonte, foram obtidas a partir de pesquisas pessoais, não científicas, de minha autoria, mas porém, não são da minha propriedade.
- › A cópia ou reprodução do conteúdo apresentado, devem ocorrer, somente com a expressa autorização do autor.



Mercado de Software

PRINCIPAIS INDICADORES DO MERCADO BRASILEIRO DE SOFTWARE E SERVIÇOS – 2016 (US\$ MILHÕES)

Main Brazilian Software and Services Market Indicators – 2016 (US\$ million)



THE
DEVELOPER'S
CONFERENCE

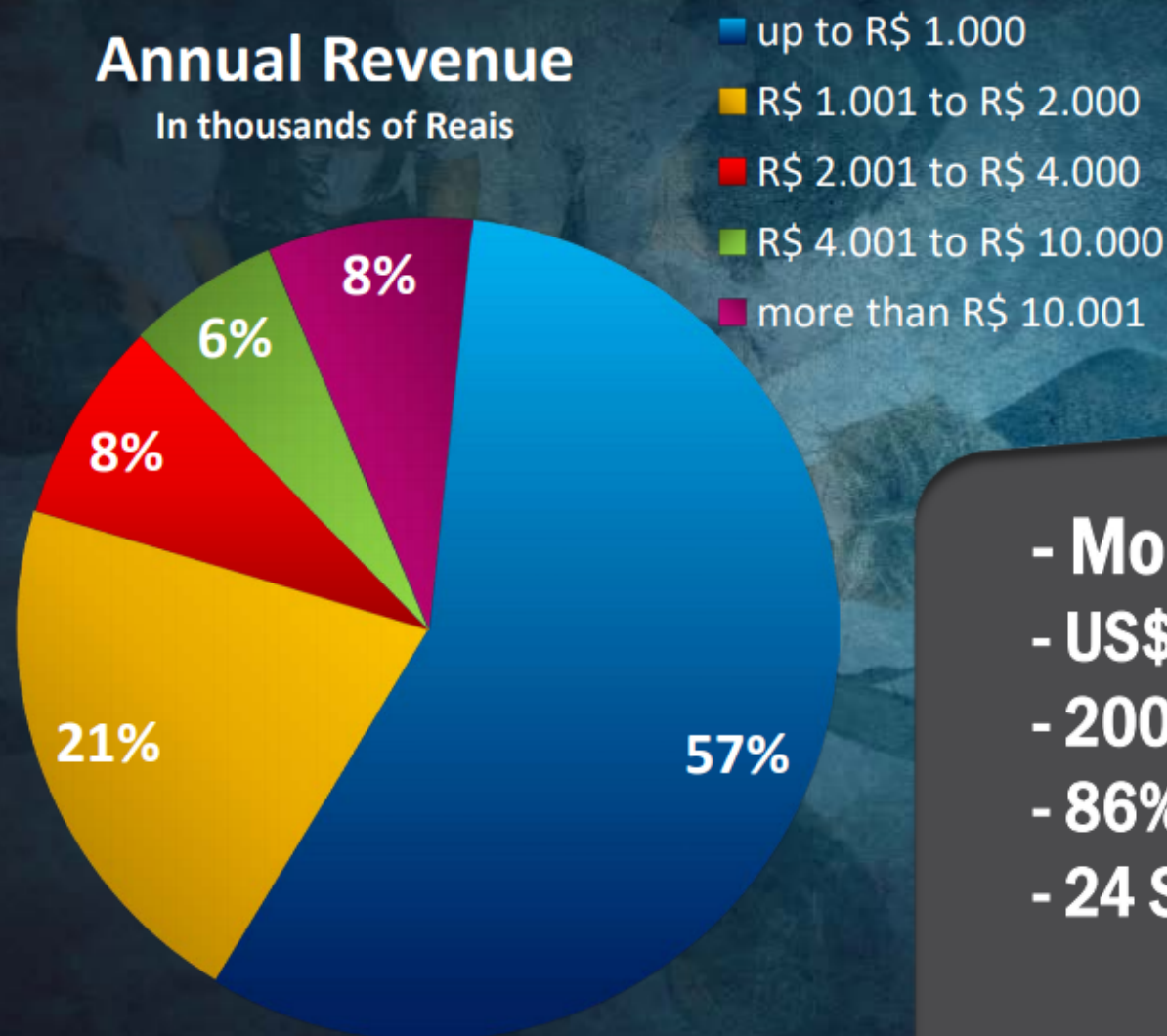


Fonte: Mercado Brasileiro de Software: Panorama e Tendências, 2017. 1ª Ed – São Paulo – ABES – 2017.

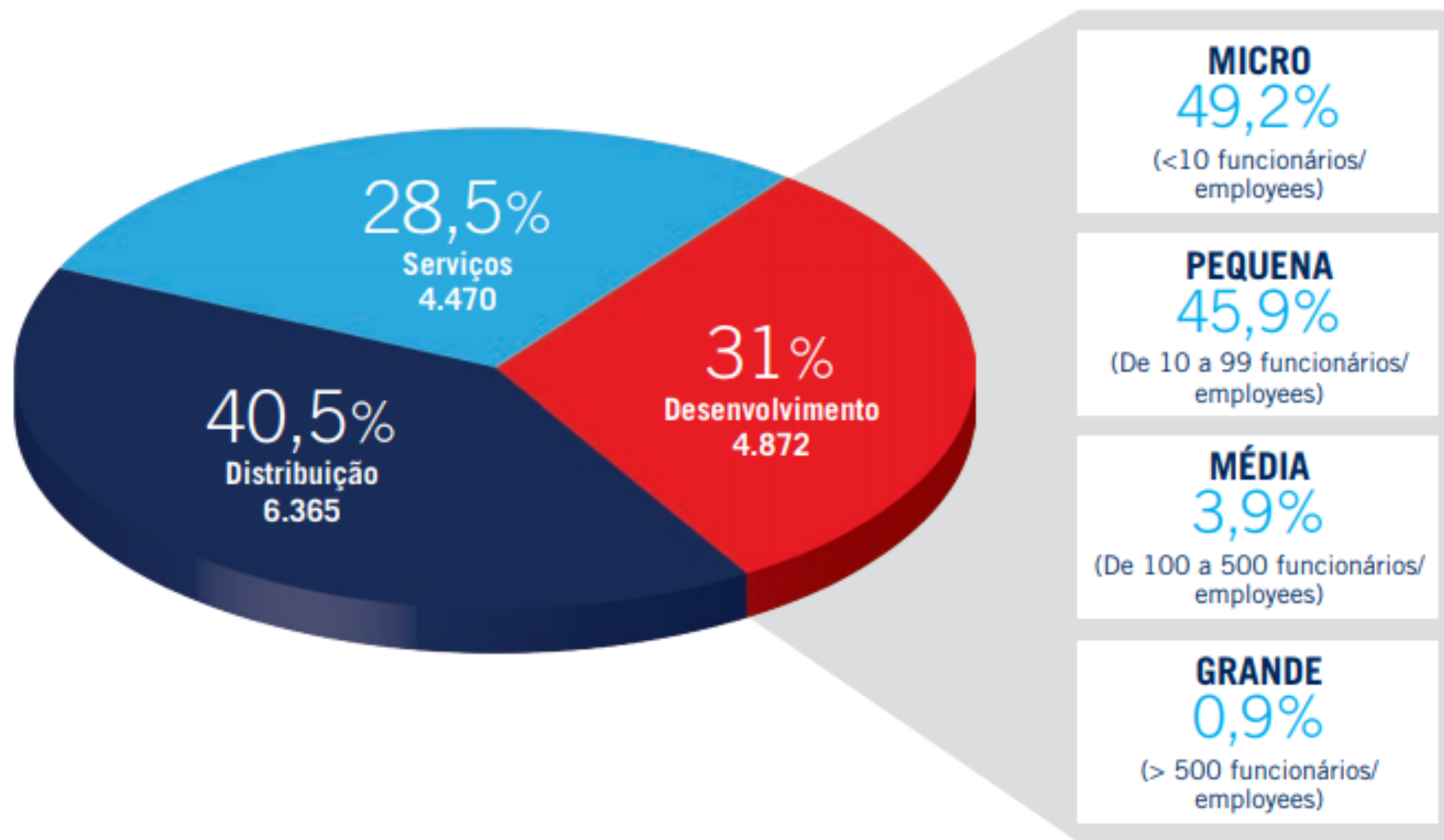
AFFILIATES PROFILE

Annual Revenue

In thousands of Reais



- More than 2000 Affiliates (*)
- US\$ 20 billion in Revenue
- 200.000 direct jobs
- 86% of Micro and Small Business
- 24 States



Fonte: Mercado Brasileiro de Software: Panorama e Tendências, 2017. 1ª Ed – São Paulo – ABES – 2017.

Mas viemos aqui para falar de
segurança...



CISO

Pentester

Vamos Refletir...

Software Seguro...



Feature ou Qualidade?

O que valoriza um Software?

Atender os Requisitos ou
Seguir requisitos de
Segurança?

O que valoriza um Desenvolvedor?

Experiência na Linguagem?

Múltiplos Conhecimentos?

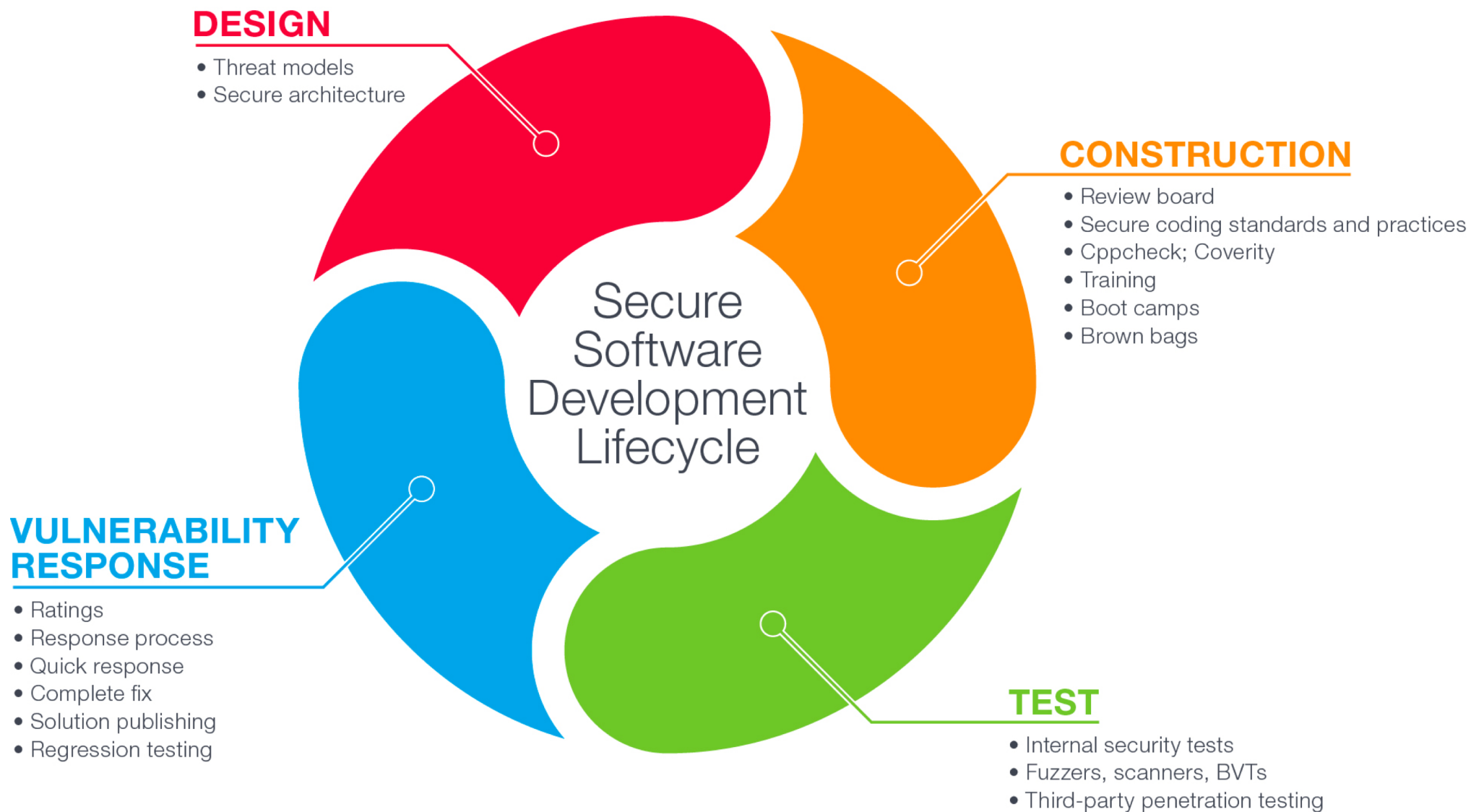
Desenvolvimento Seguro?

Quem deve propor Software Seguro?



Desenvolvedor?
Empresa?
Cliente/Usuário?

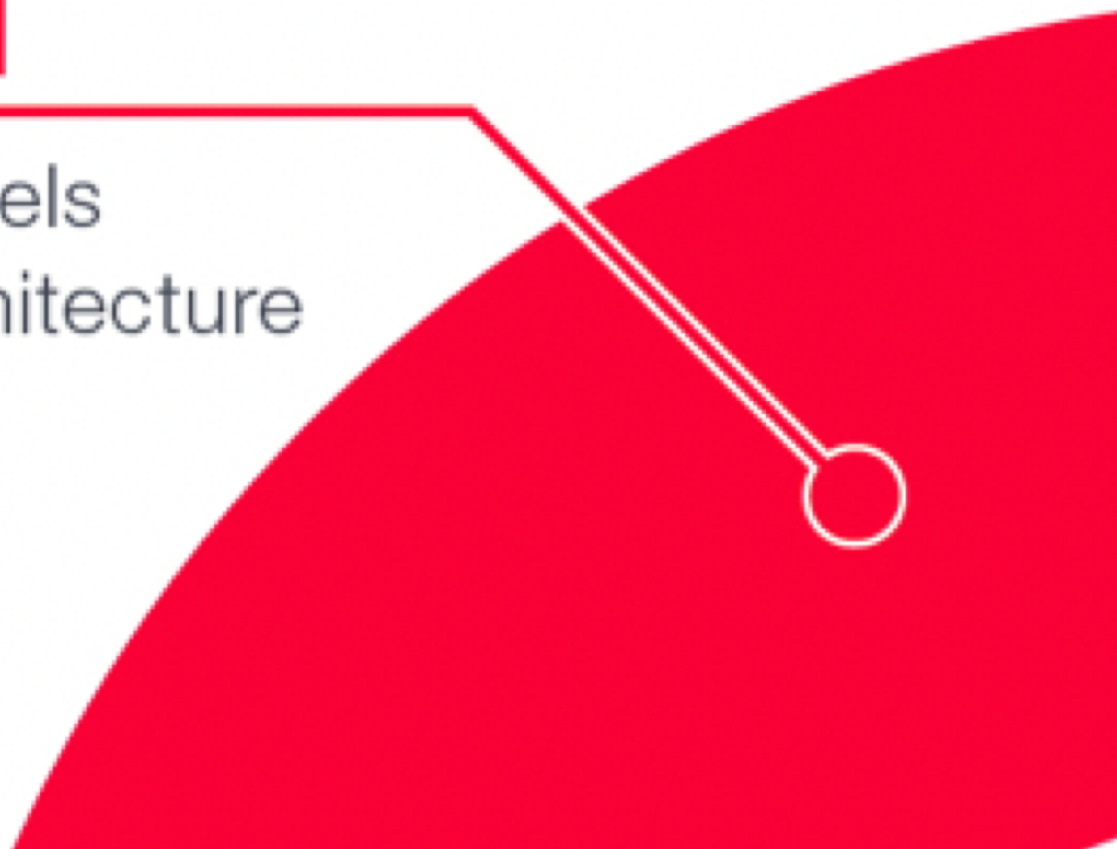
Software Security





DESIGN

- Threat models
- Secure architecture



Modelos de Ameaças

- › Acesso indevido = autenticação e autorização
 - › Proteção contra Brute Force
 - › Política de Senha
 - › Granularidade de Permissões
 - › Ataques dentro da aplicação (Top 10 Owasp)
- › Vazamento de Informações
 - › SQL Injection
 - › XSS
 - › etc
- › Rastreabilidade = logs

Arquitetura

- › Comum preocupar-se com a Arquitetura e Infra da Aplicação na Cloud...
- › Mas e a Arquitetura de Segurança no Design?
- › Criptografia é considerada?

E as obrigações legais?

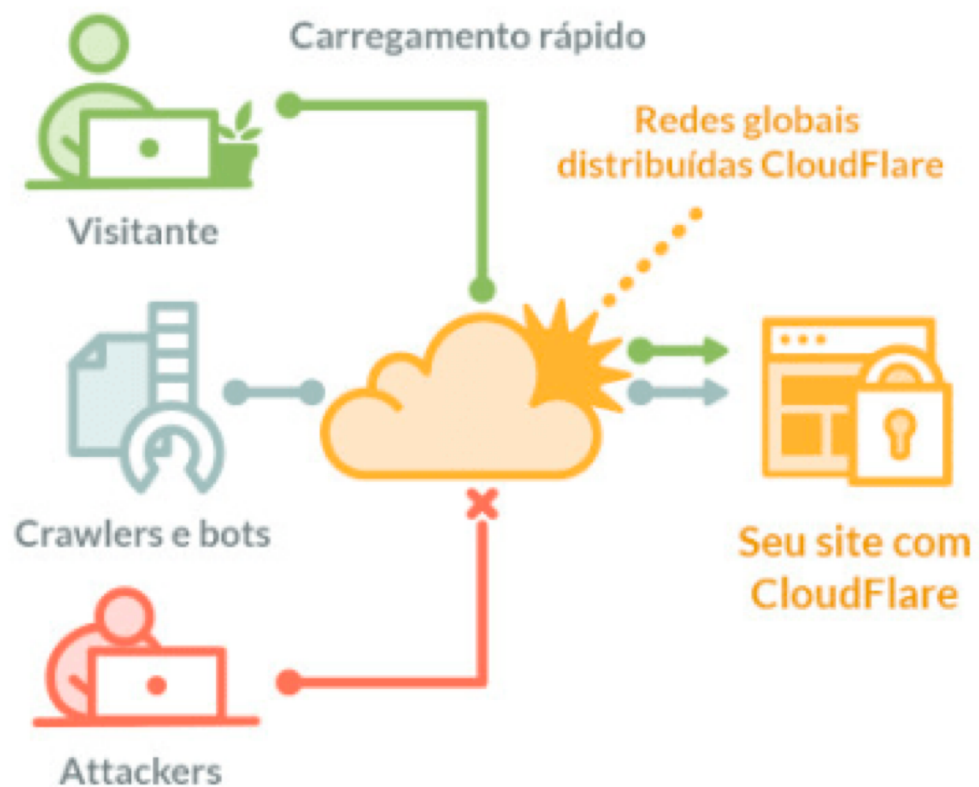
- › LGPD e/ou GDPR
 - › Criptografia
 - › Onde vai armazenar – brasil ou exterior?
 - › Isso é considerado?

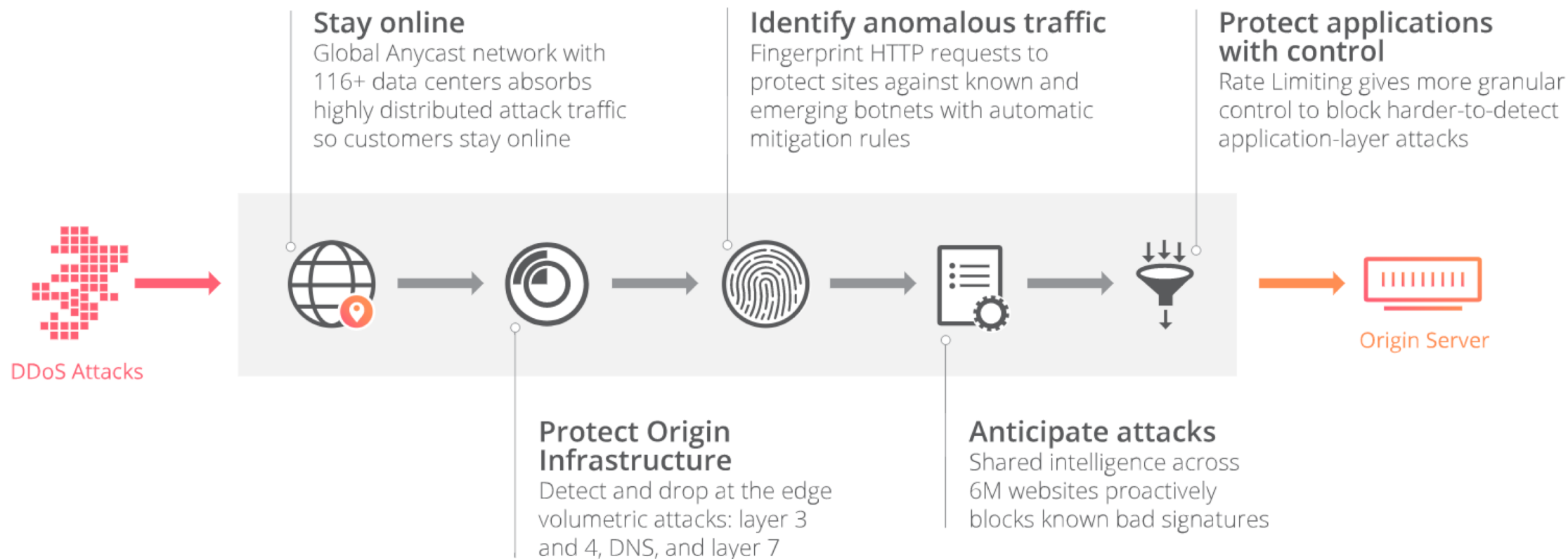


Sem Cloudflare

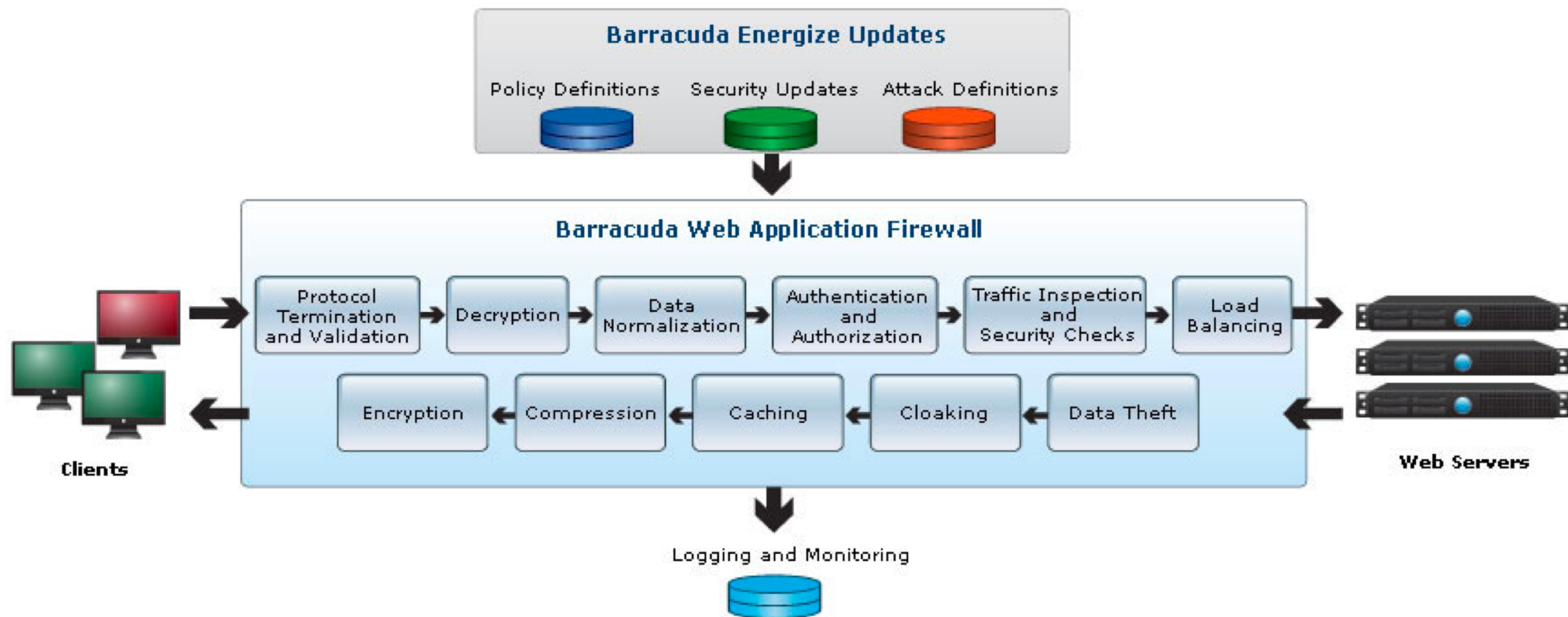


Com Cloudflare





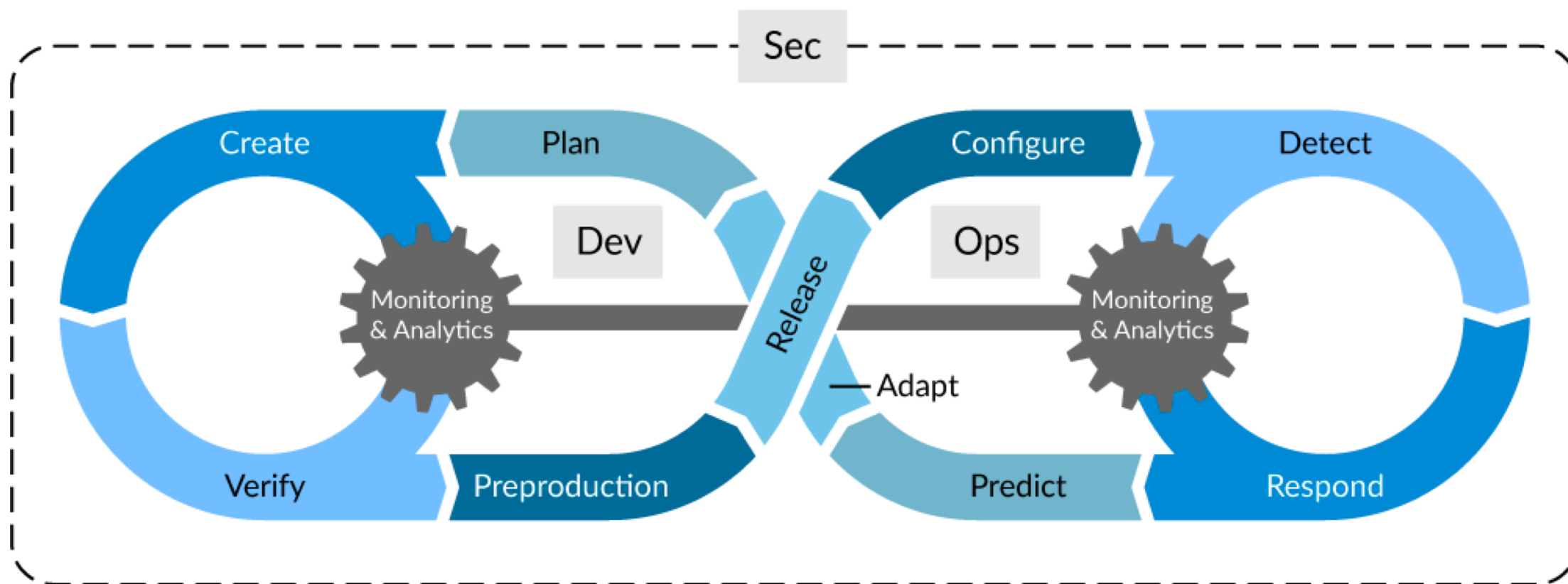
Barracuda Web Application Firewall Architecture





CONSTRUCTION

- Review board
- Secure coding standards and practices
- Cppcheck; Coverity
- Training
- Boot camps
- Brown bags

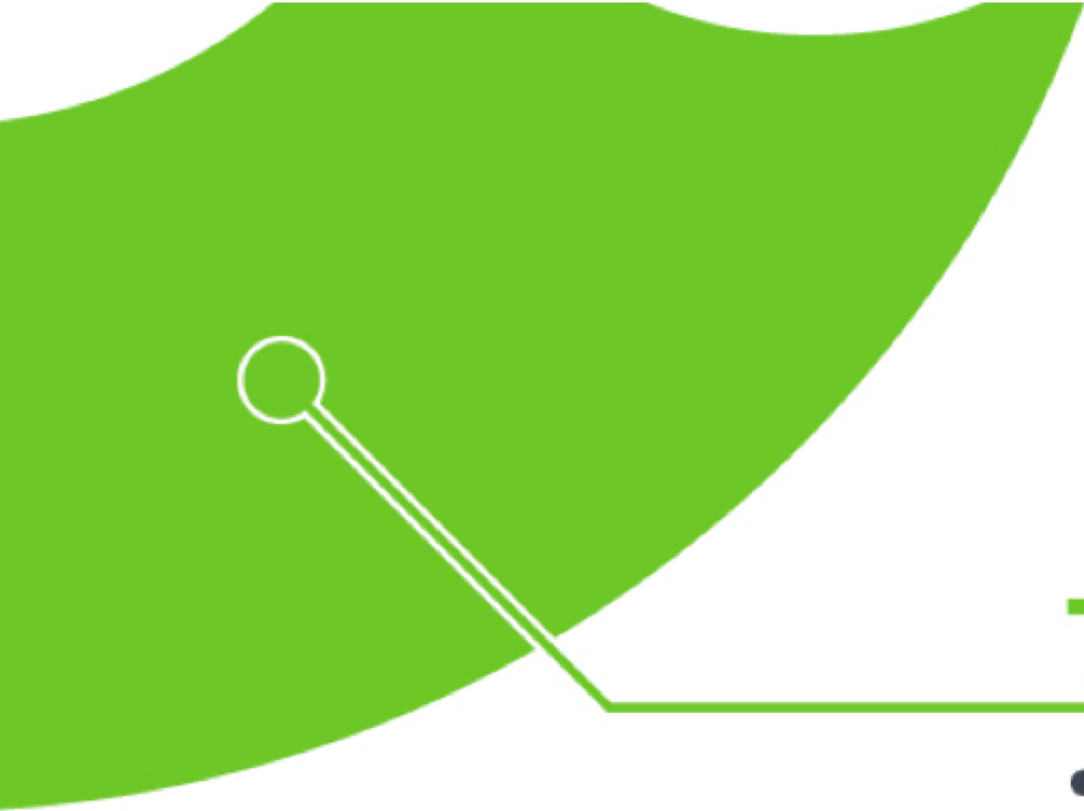


Construção

- › Todos envolvidos devem opinar sobre Segurança e Riscos e planejar as ações
- › É necessário Capacitação
 - › Iniciativa da Empresa
 - › Iniciativa do Desenvolvedor
- › Considerar ameaças e como estão sendo tratadas/protegidas
- › Criar padrões de Desenvolvimento Seguro de Código

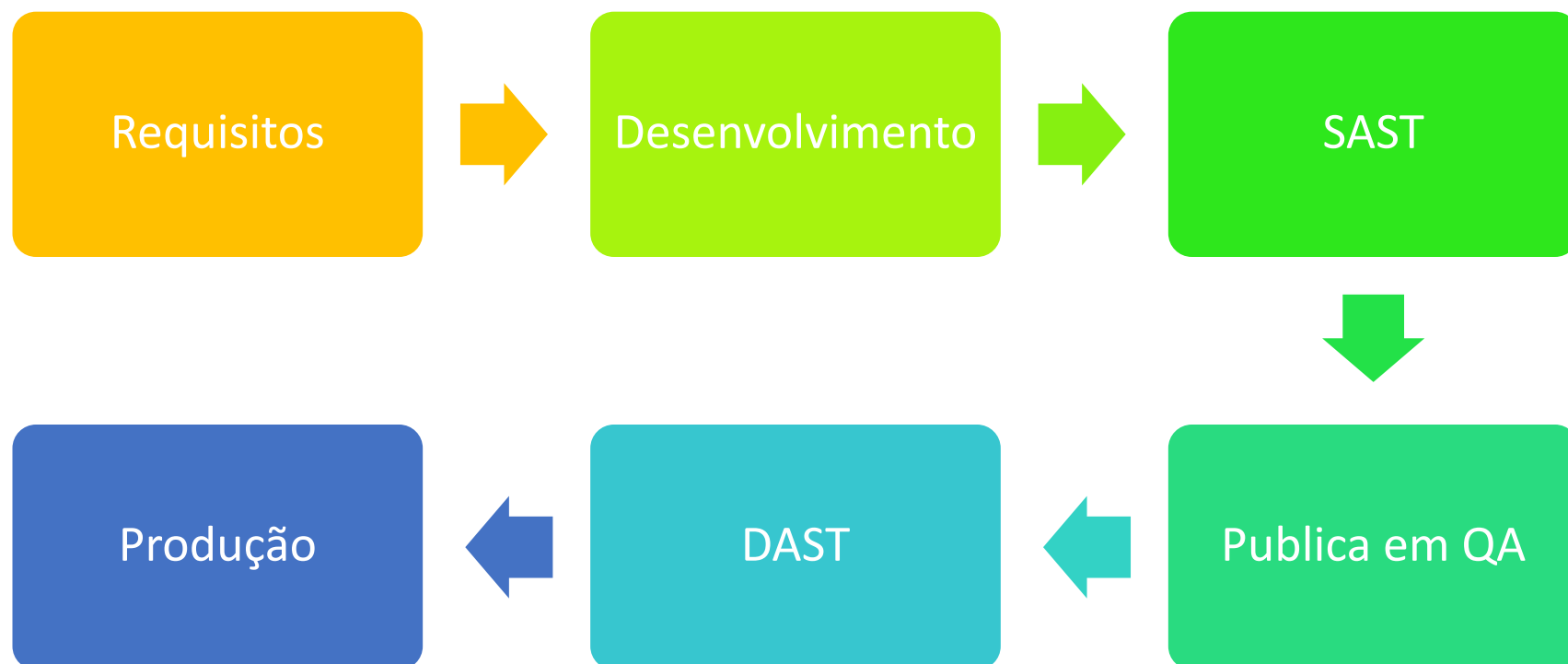
Além do SSDLC

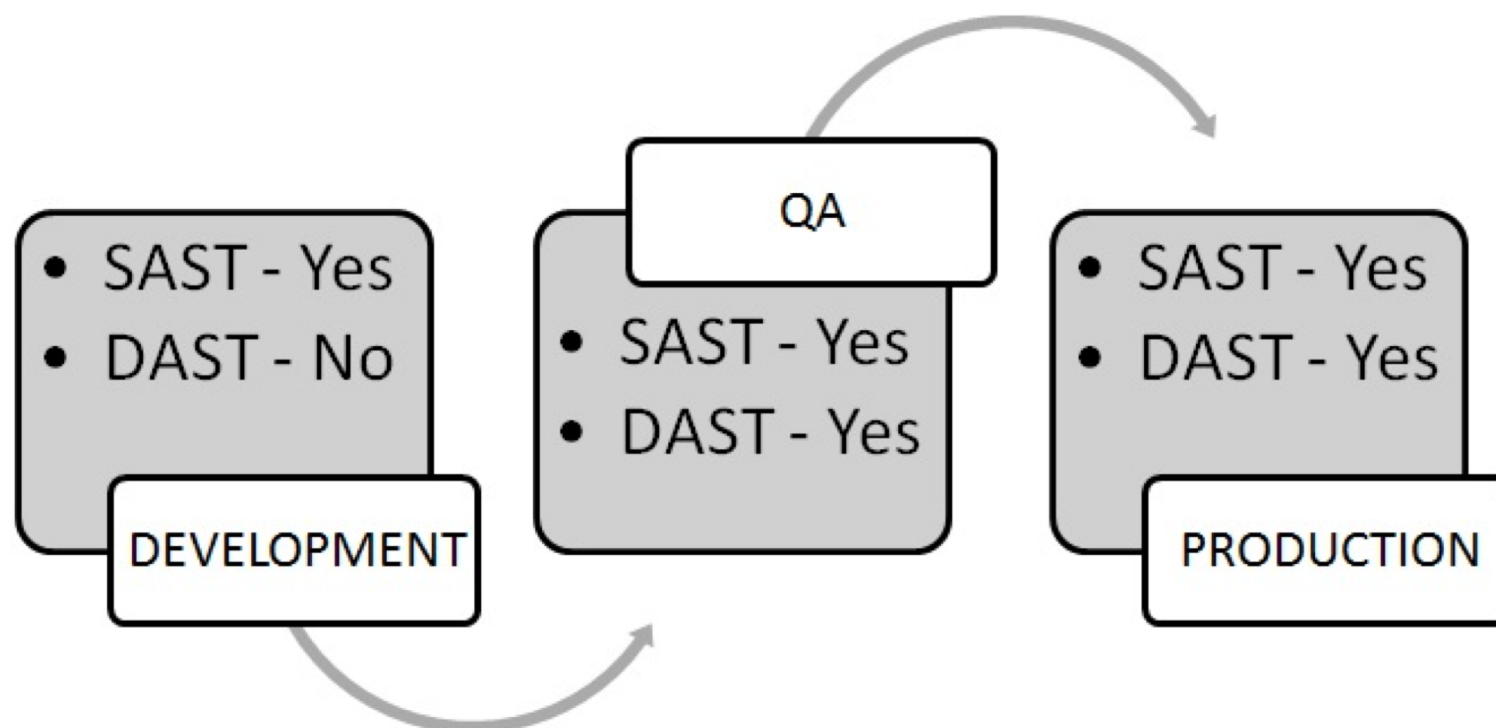
- › Serviços desnecessários abertos
- › Ambiente de testes com senha default ou sem senha
- › Manipulação de dados reais
- › Ausência de Patches / Vulnerável
- › CI Muito Permissivo



TEST

- Internal security tests
- Fuzzers, scanners, BVTs
- Third-party penetration testing







VULNERABILITY RESPONSE



- Ratings
- Response process
- Quick response
- Complete fix
- Solution publishing
- Regression testing

Resposta a Incidentes

- › Quem vai responder?
- › Qual procedimento a ser adotado em caso de Bug de Segurança?
 - › Comum ser dado tratamento igual BUGs comuns
 - › Tratam correção de bug como feature e coloca no roadmap de melhorias
- › Plano de Comunicação (Em caso de Vazamento)
 - › STAFF e Board/Investidores
 - › Autoridades
 - › Clientes

Prevenir ou Corriger?

Prevenir ou Corrigir?

- › Para cada 1000 linhas de código, em média 15 possuem problemas críticos (Departamento de Defesa dos EUA)
- › Uma falha leva em média 75 minutos para ser descoberta e 6 horas para ser corrigida (Estudo realizado durante 5 anos pelo Pentágono)
- › Aplicações empresarias possuem em média, 150mil a 250 Mil linhas de código (Software Magazine)

Fonte: Barracuda Networks



Prevenir ou Corrigir?

Apenas para identificar e corrigir
código:

$15 * 150k * 1,5hrs/40 = 84$ semanas

$15 * 250k * 6hrs/40 = 562$ semanas



O que esperar então?

- › Engajamento de todos
- › Não é tendência, é realidade!
- › Associações
- › Certificações e Padrões
- › OWASP



Não custa dinheiro para começar...

OWASP: Quem são?

- › Fundação Internacional sem Fins Lucrativos para promover a Segurança no desenvolvimento de Aplicações
- › Disponibiliza gratuitamente ferramentas para testes e avaliação de segurança de aplicações, bem como manuais de testes e boas práticas para o desenvolvimento de código seguro
- › Mantém o TOP 10 OWASP
- › www.owasp.org



OWASP

Open Web Application
Security Project

\$oftware \$ecurity



› Investimento

› Dinheiro

› Dinheiro = Tempo Concentrado

› Tempo = conhecimento = maturidade = mais segurança

You get, how much you pay!



