VANTICO

vantico.com.br

AppSec e **Segurança Ofensiva** lado a lado

Quem sou eu

Analista de Segurança na Fiotec/Fiocruz;

Tecnólogo em Análise e Desenvolvimento de Sistemas;

Mestre em Ciências pela USP;

Cofundador do Hack In Rio, voluntário da Codecon e demais comunidades de tecnologia.

VANTICO

vantico.com.br

↘ Somos especialistas em *** Pentest e Cibersegurança.

↘ Como se constrói software hoje em dia?

Contexto para o **desenvolvimento de software**

Práticas antigas ainda são comuns

Desenvolvimento de **Software em cascata (Waterfall)** junto com modelo ágil;

Esforços para manter **ciclos de atualizações menos longos**, na busca da geração contínua de valor;

Falta de colaboração e integração

DevOps tratado mais como **tecnologia de CI/CD** do que cultura de integração e processos;

Apesar do uso de diversas tecnologia**, persistem problemas de comunicação** entre diferentes equipes;

Desafios das novas tendências

Uso de **inteligência artificial e amplas automações**;

Aumento do uso de **microsserviços, cloud computing, containers, plataformas low-code** etc.

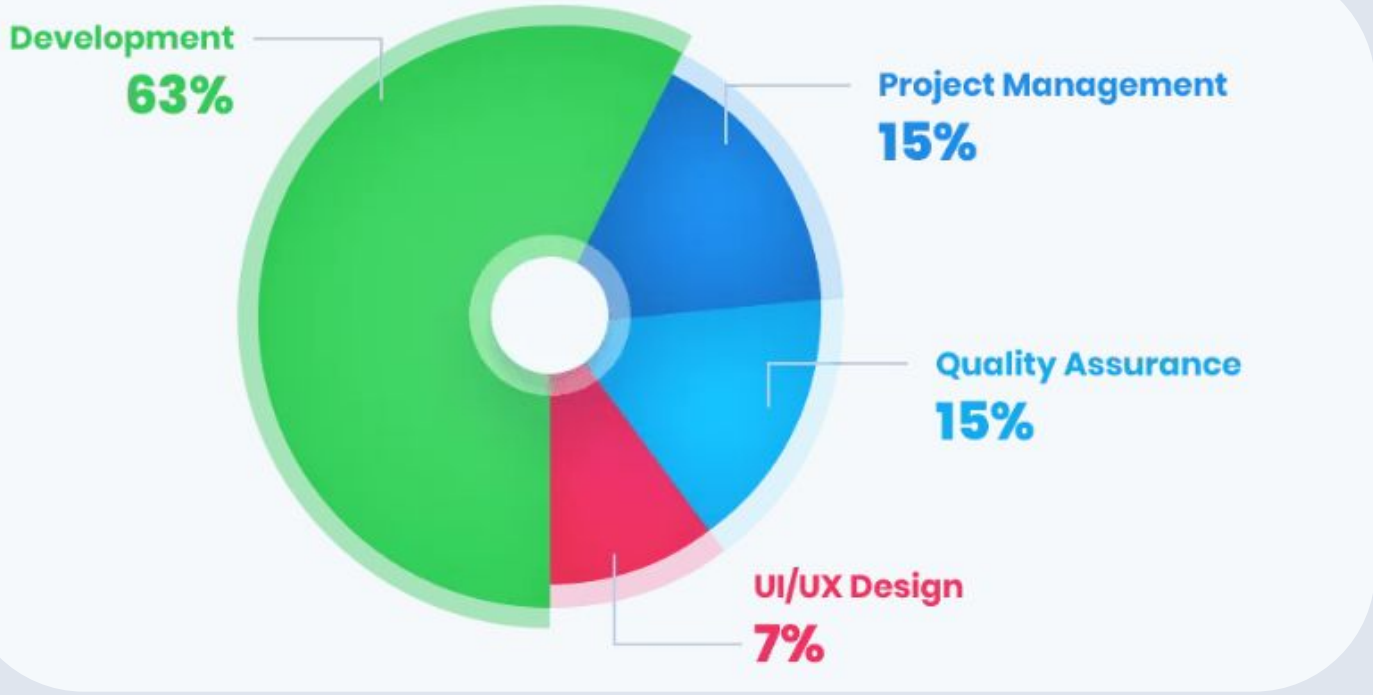
Segurança de Aplicações no contexto atual↘

- **Segurança continua sendo mais comum no final do ciclo de desenvolvimento;**
- **Exclusiva dos times de segurança, raramente interage com devs e demais times;**
- **Vista geralmente como “ferramentas de testes do tipo SAST”;**
- **A segurança dificilmente é considerada pelo time de Produto (requisito).**

↘ Segurança Ofensiva

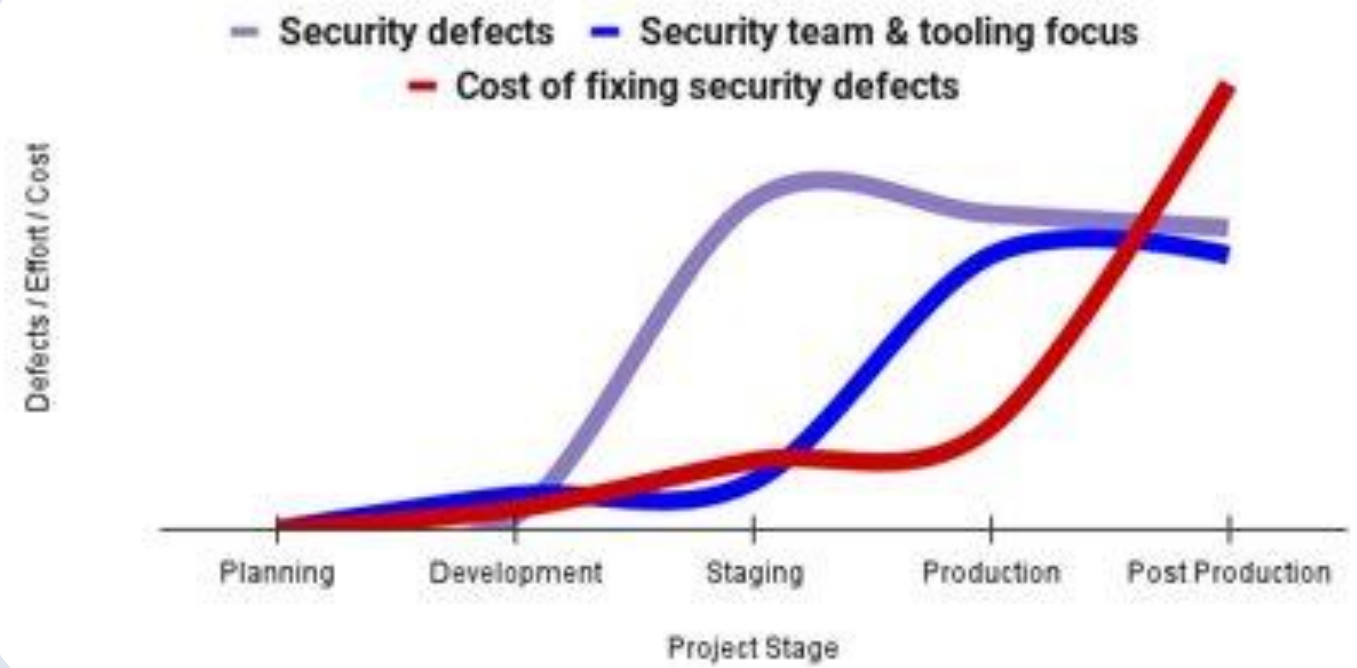
- Resumida geralmente em Pentestings individualizados em vez de um Programa de Gestão Contínua;
- Testes de Segurança Ofensiva nem sempre se comunicam com os demais testes de segurança maneira estratégica;
- Necessidade de maior gestão, integração e centralização dos resultados obtidos.

Principais custos durante o **desenvolvimento de software**



Fonte: GoodCore Software, 2024.

Economize tempo e dinheiro: **Integrando a segurança durante todo o ciclo de desenvolvimento**



Fonte: Google Cloud (2022)

↘ Segurança durante todo o **ciclo de desenvolvimento**

Dados mostram que, embora a conscientização sobre a importância da segurança esteja crescendo, ainda há um longo caminho a percorrer para que a **segurança seja totalmente integrada e priorizada no desenvolvimento de software**.

↘ Aprofundando sobre
Segurança de Aplicações

Conceito de **Segurança de Aplicações**

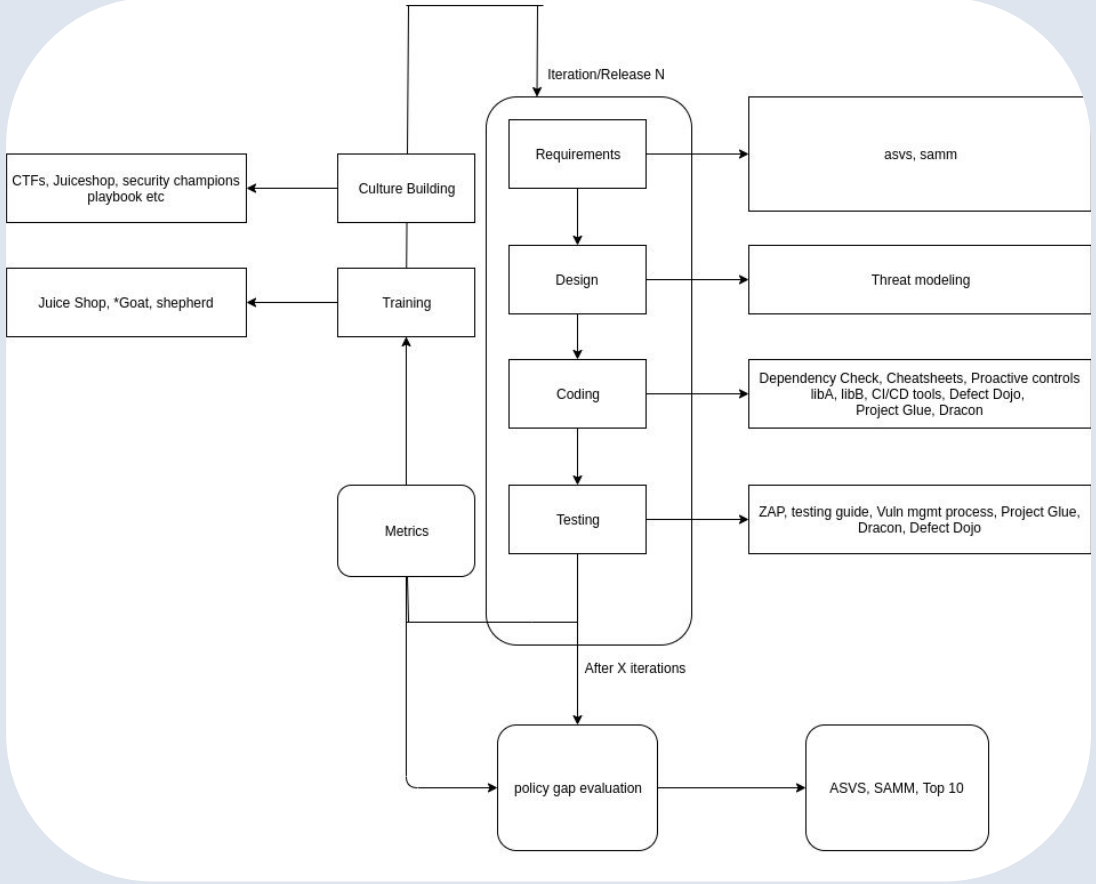
=

Segurança de Aplicações é o nome que se dá ao **processo de construir, lançar e manter aplicações seguras** – sempre por meio das melhores práticas aplicadas e integrados ao ciclo desenvolvimento.

Segurança durante **todo o ciclo de desenvolvimento**↘

Ciclo de Desenvolvimento Seguro. OWASP, 2024.

Segurança **não precisa ser difícil** ↘



Fonte: OWASP (2024)

Principais benefícios da Segurança Integrada em todo o ciclo

- Prevenir possíveis vulnerabilidades logo no início;
- Redução de custos, economia de tempo e esforço;
- Um produto mais maduro e seguro por passar por avaliações durante todo o ciclo de desenvolvimento.

Cultura

Integração da Segurança em todas as fases do ciclo de desenvolvimento;

Aumento da conscientização e interesse sobre o tema;

A colaboração entre diferentes equipes acaba sendo fundamental.

+

OffSec

Proatividade na identificação e resolução de vulnerabilidades;

Lições aprendidas são incorporadas nos processos de desenvolvimento;

AppSec permite que as equipes de OffSec se concentrem em áreas mais críticas.

↘ Relação entre **AppSec e OffSec**

Entendendo **Segurança Ofensiva**

A Segurança Ofensiva, ou “OffSec”, envolve estratégias proativas que utilizam as mesmas táticas que os atores maliciosos usam em ataques reais para fortalecer a segurança. Isso inclui **pentesting, engenharia social, avaliações de vulnerabilidades e equipes de red team.**

Relação entre **Segurança Ofensiva e Segurança de Aplicações**

Proatividade

- Proatividade em detectar e explorar vulnerabilidades.

- Proatividade em integrar segurança desde o início do desenvolvimento (prevenção).

Foco em vulnerabilidade

- Explora vulnerabilidades em diferentes ambientes;

- Atua na conscientização e prevenção de vulnerabilidades com *secure coding;*

Gestão Estratégica

- São parte estratégica da Governança do negócio e continuidade;

- Incentiva a cultura e conscientização em segurança para todo o negócio.

Principais desafios para integrar AppSec e OffSec

Percepção do Negócio de que as áreas operam em silos

O uso de diferentes ferramentas dificulta a centralização e a visibilidade dos resultados

Os dados gerados por AppSec e OffSec são valiosos, mas muitas vezes subutilizados

↘ Conhecendo a **Plataforma Vantico**

Plataforma **exclusiva** e **metodologia** pentest as a service

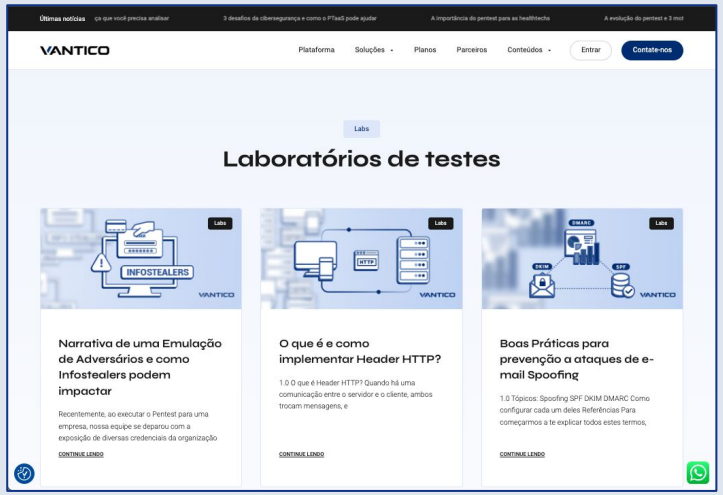
Recursos da **Vantico**

Insights do setor de nossos especialistas em segurança cibernética

Notícias e insights sobre o setor de segurança cibernética e tendências.

HTTPS://VANTICO.COM.BR/BLOG

HTTPS://VANTICO.COM.BR/LABS



Insights técnicos da Vantico

O Laboratório de testes é nossa área de P&D.

VANTICO

Vamos **transformar** os testes de segurança?

Kaique Bonato

kaique@vantico.com.br