AppSec

É para os brabos!

Tiago Zaniquelli

- Pai/Marido!
- Especialista em AppSec;
- Analista de Segurança na Conviso;
- Entusiasta:
  - Segurança da Informação;
  - Desenvolvimento;
  - Agilidade.

Agenda da palestra

- O que é Segurança de Aplicações (AppSec)?
- AppSec segundo SAMM
  - Governança
  - Design
  - Implementação
  - Verificação
  - Operação

O que é segurança de aplicações?

SDLC x S-SDLC


Ciclo de vida do desenvolvimento de software (SDLC)
Requisitos
Design
Desenvolver
Testar
Implementar
Ciclo de vida do desenvolvimento de software seguro (S-SDLC)
Requisitos de segurança
Modelagens de Ameaças e Revisão de Arquitetura
Análise Estática e Desenvolvimento Seguro
Revisão de Código e Testes de Segurança
Implementação e Manutenção

Mas isso não seria
DevOps ou DevSecOps?

O que não é AppSec?

- Ferramentas
- Frameworks
- Pentest
- Bug Bounty

OWASP e seus principais projetos

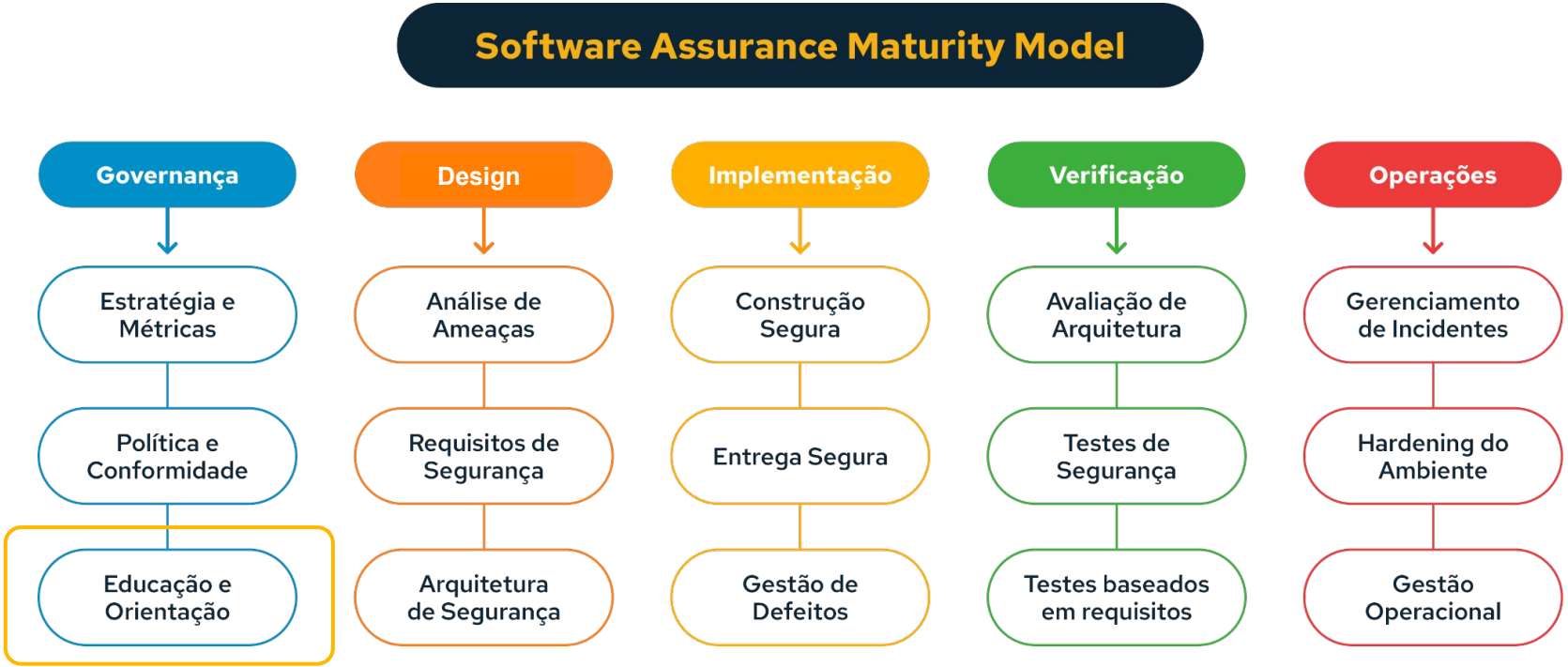
Open Worldwide Application Security Project

É uma organização sem fins lucrativos, internacional, cujo objetivo é melhorar a segurança de software no mundo.

Mas porque
AppSec é para os brabos?


SECURITY ATTACKS
DEVSECOPS
THE INNOCENT APP

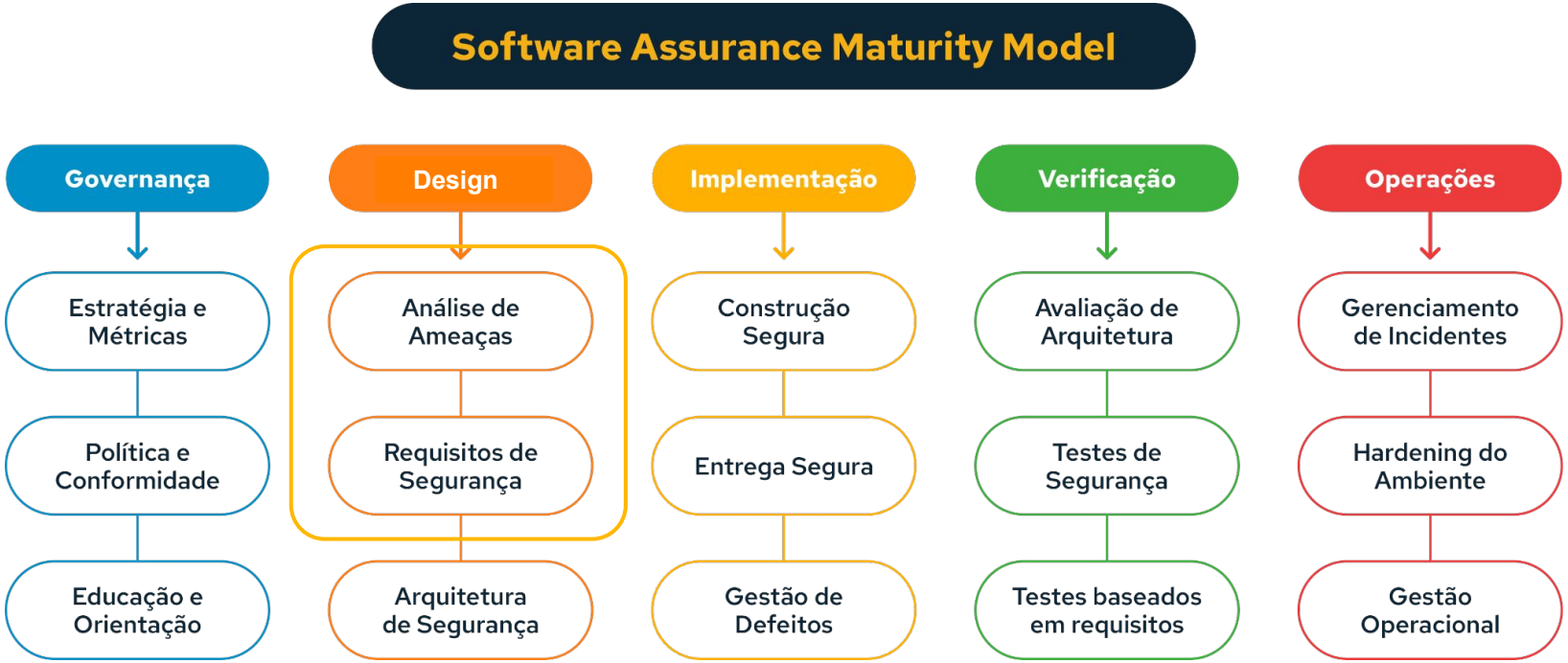
OWASP SAMM


Software Assurance Maturity Model
Governança
Estratégia e Métricas
Política e Conformidade
Educação e Orientação
Design
Análise de Ameaças
Requisitos de Segurança
Arquitetura de Segurança
Implementação
Construção Segura
Entrega Segura
Gestão de Defeitos
Verificação
Avaliação de Arquitetura
Testes de Segurança
Testes baseados em requisitos
Operações
Gerenciamento de Incidentes
Hardening do Ambiente
Gestão Operacional

O que é Security Champions?

"É um **profissional** do time de desenvolvimento que atua na **disseminação** da cultura de **desenvolvimento seguro**!"

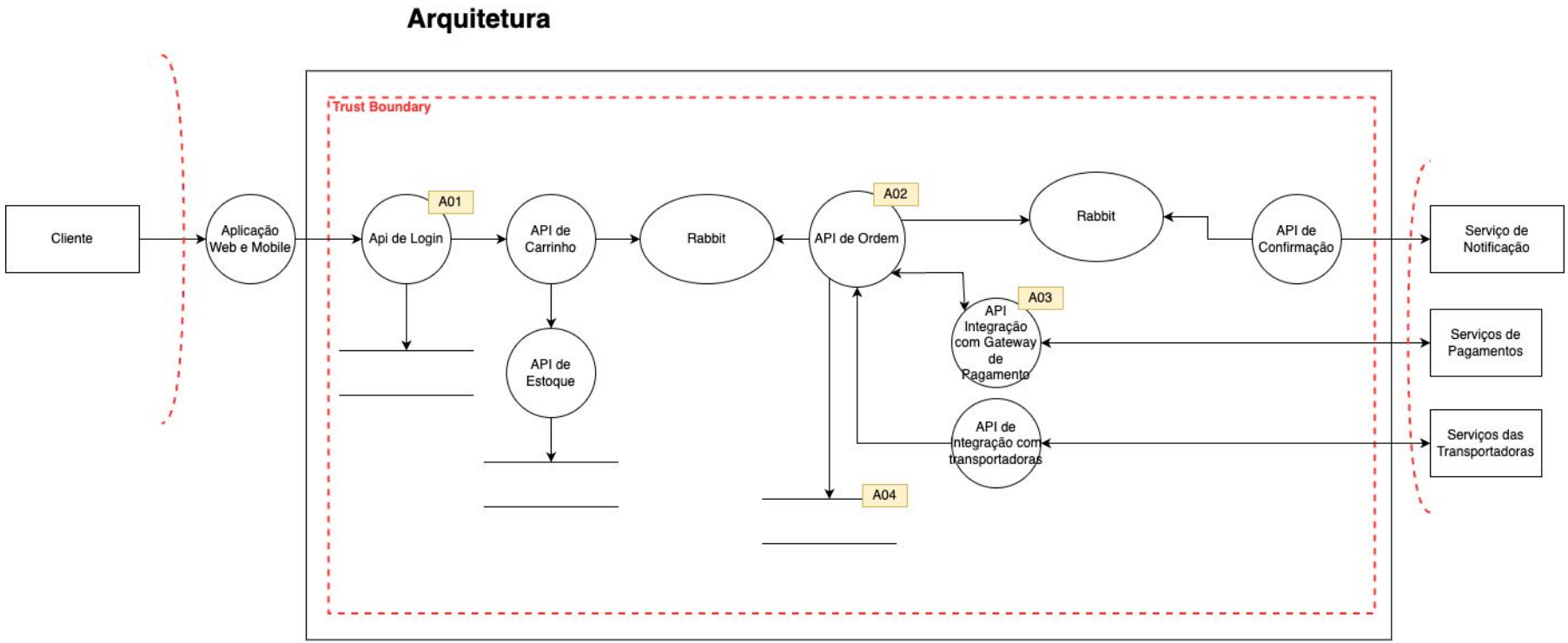
OWASP SAMM


Software Assurance Maturity Model
Governança
Estratégia e Métricas
Política e Conformidade
Educação e Orientação
Design
Análise de Ameaças
Requisitos de Segurança
Arquitetura de Segurança
Implementação
Construção Segura
Entrega Segura
Gestão de Defeitos
Verificação
Avaliação de Arquitetura
Testes de Segurança
Testes baseados em requisitos
Operações
Gerenciamento de Incidentes
Hardening do Ambiente
Gestão Operacional

O que é modelagem de ameaças?

"É uma **técnica efetiva** que ajuda a construir aplicações, sistemas, redes e serviços de **maneira mais segura**. De forma que **identifique ameaças potenciais** e **reduza riscos** estratégicos logo no início do ciclo de desenvolvimento."

Modelagem de Ameaças



Modelagem de Ameaças

Assets		
ID	Description	
A01	API de Login	.NET 7; REST; HTTPS;OAuth2; Linux;
A02	API de Ordem	.NET 7; REST; HTTPS; RabbitMQ; Entity Framework; SQLServer 2022; Key Vault; Linux;
A03	API de Integração com Gateway de pagamento	.NET 7; REST; HTTPS; Key Vault; Criptogafia; Linux;
A04	Base de Ordens	SQL Server 2022;
A05	API de estoque	.NET 7; REST; HTTPS; Entity Framework; SQLServer 2022; Key Vault; Linux;

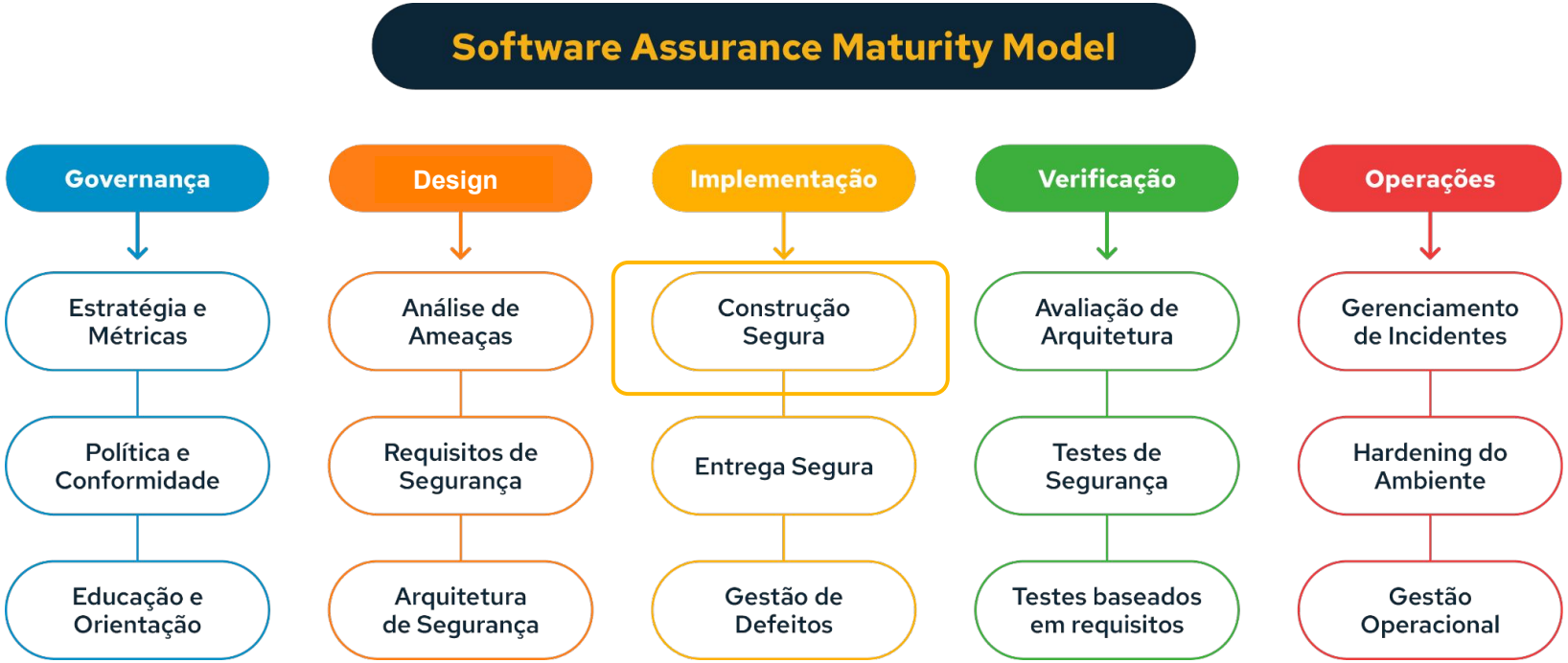
Threat Actors	
TA01	Atacante Externo (hacker, ativista, o troll, estelionatário, fraudador)
TA02	Atacante Interno (espião industrial, funcionário que cai em phishing, estelionatário, funcionário insatisfeito)
TA03	Serviços Externo (fica testando a infra, ele pode finge que é o serviço de pagamento interceptando todas as requisições)

Objetivos	
ID	Description
OB01	Se passar por alguém ou serviço
OB2	Conseguir informações confidenciais
OB3	Sequestro de Dados de Pagamento
OB4	Sequestro de Estoque
OB5	Indisponibilizar o sistema causando perdas financeiras

THREAT	
ID	Description
T01	Ataque de adivinhação (força bruta/password spray) para obter acesso não autorizado ao sistema
Agente de ameaça	TA01
Asset	A01
STRIDE	Repudiation / Spoofing / Elevação de privilegios / Information Disclosure

Security Controls	
ID	Description
C01	Anti bot-automation (CAPTCHA/Rate limiting)
C02	WAF (bloqueio de origens identificadas como atacantes)
C03	Implementar política de senhas segura
C04	Implementar política de rotação de senhas
C05	Implementar possibilidade de uso de segundo fator de autenticação

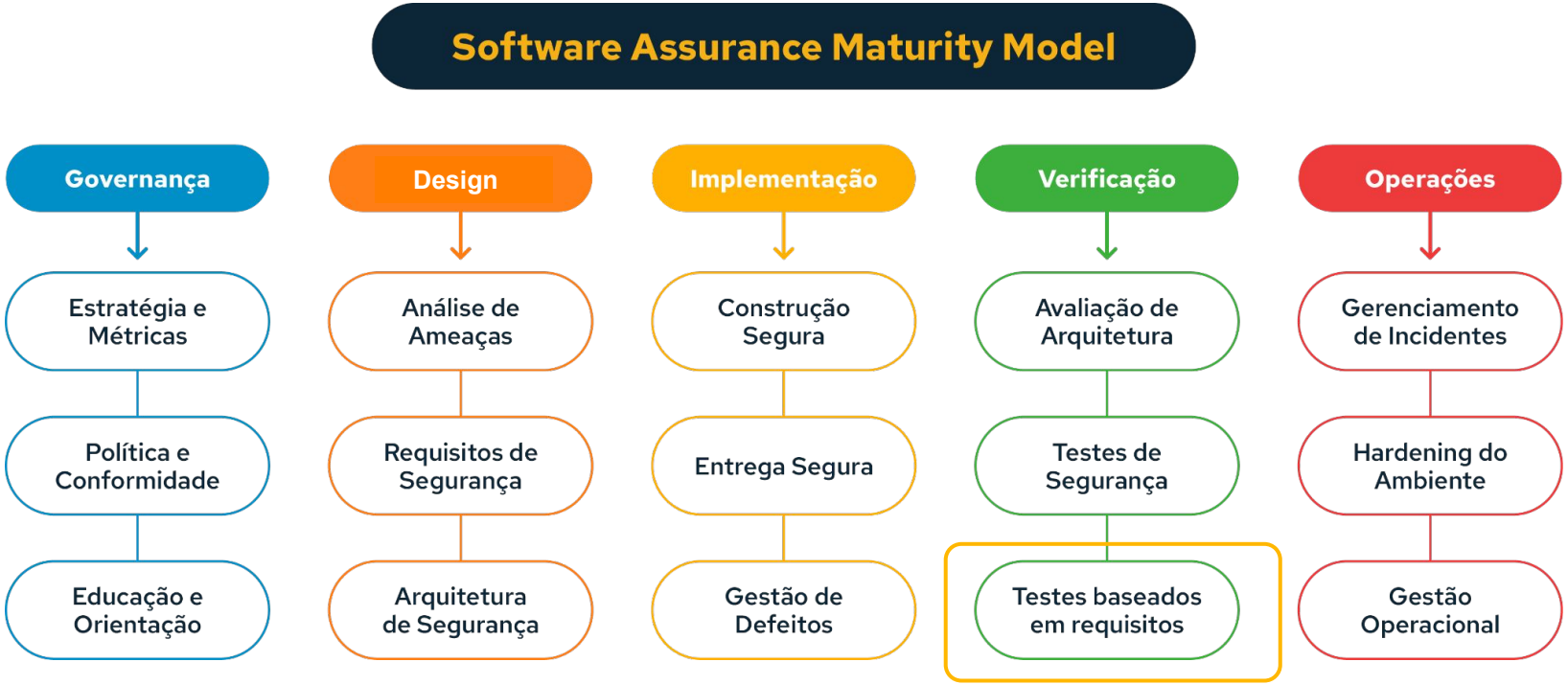
OWASP SAMM


Software Assurance Maturity Model
Governança
Estratégia e Métricas
Política e Conformidade
Educação e Orientação
Design
Análise de Ameaças
Requisitos de Segurança
Arquitetura de Segurança
Implementação
Construção Segura
Entrega Segura
Gestão de Defeitos
Verificação
Avaliação de Arquitetura
Testes de Segurança
Testes baseados em requisitos
Operações
Gerenciamento de Incidentes
Hardening do Ambiente
Gestão Operacional

O que é gestão de dependências?

"É **comum** o uso de **bibliotecas e outros componentes**, se faz necessário a **proteção e entendimento** desse uso"

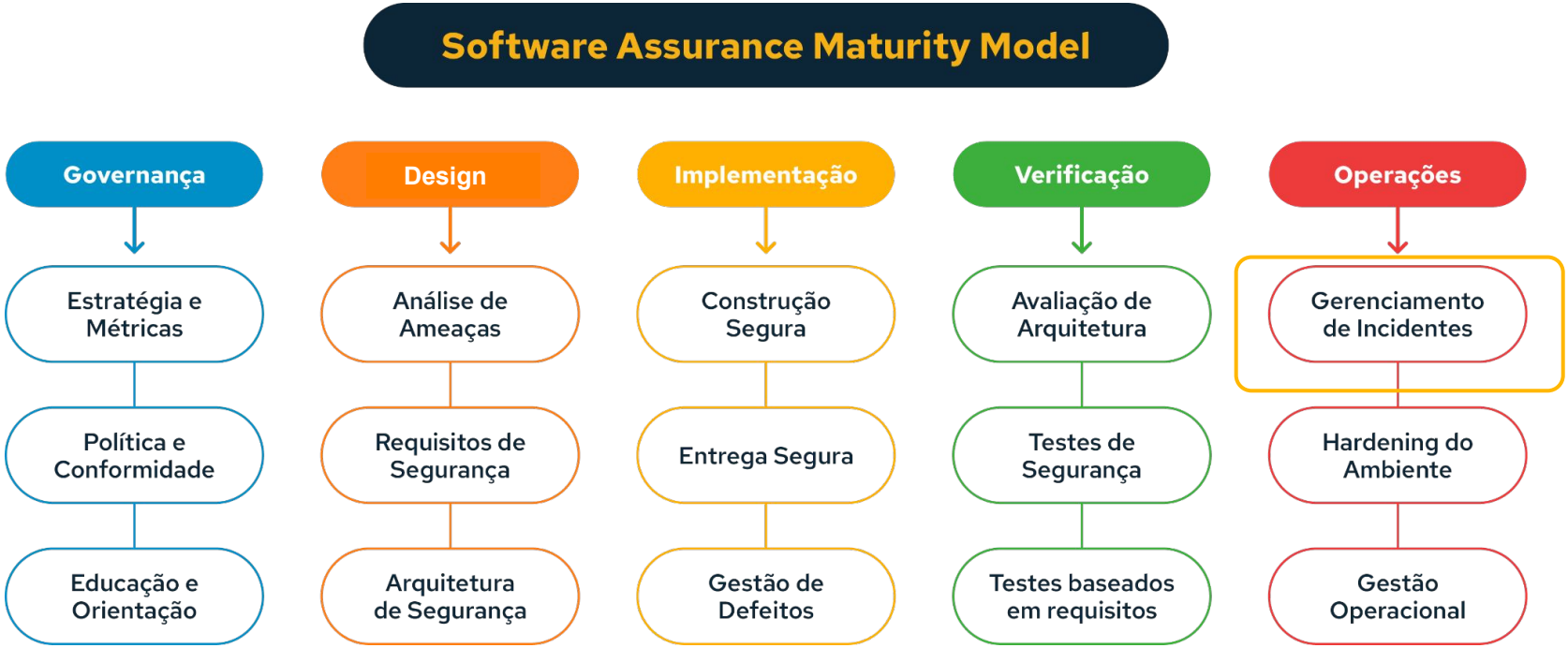
OWASP SAMM


Software Assurance Maturity Model
Governança
Estratégia e Métricas
Política e Conformidade
Educação e Orientação
Design
Análise de Ameaças
Requisitos de Segurança
Arquitetura de Segurança
Implementação
Construção Segura
Entrega Segura
Gestão de Defeitos
Verificação
Avaliação de Arquitetura
Testes de Segurança
Testes baseados em requisitos
Operações
Gerenciamento de Incidentes
Hardening do Ambiente
Gestão Operacional

O que são testes baseados em requisitos?

"Garantir que os **controles de segurança** implementados funcionem conforme o esperado e satisfaçam **os requisitos de segurança** declarados do projeto"

OWASP SAMM


Software Assurance Maturity Model
Governança
Estratégia e Métricas
Política e Conformidade
Educação e Orientação
Design
Análise de Ameaças
Requisitos de Segurança
Arquitetura de Segurança
Implementação
Construção Segura
Entrega Segura
Gestão de Defeitos
Verificação
Avaliação de Arquitetura
Testes de Segurança
Testes baseados em requisitos
Operações
Gerenciamento de Incidentes
Hardening do Ambiente
Gestão Operacional

Monitoramento e resposta a incidentes?

"Precisamos primeiro **monitorar nossa aplicação** e caso aconteça algo que **não estava previsto** precisamos ter um plano para **responder ao incidente**"

Let's empower developers to build secure applications?!

Tiago Zaniquelli

Security Analyst

https://www.linkedin.com/in/tiago-zaniquellii

zani0x03@gmail.com

twitter.com/zani0x03