



KPIs e Métricas para AppSec





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.





↘ Somos
especialistas
em    ***
Pentest e
Cibersegurança.





Primeiro,
o mais
importante...



Rebeca Andrade sendo reverenciadas por Simone Biles e Jordan Chiles
(Foto: Jack Gruber-USA TODAY Sports)



↘ “O sucesso é alcançado
através de **métricas precisas** e
KPIs, baseados em **dados** e **análise**
contínua.”





Mas o que significa
“**sucesso**”
quando falamos de
Segurança de Aplicações?



Medir o sucesso do seu programa de segurança

- **É essencial para gerenciar riscos** e aprimorar o programa ao longo do tempo;
- **Poucas empresas entendem** seus próprios processos;
- **As mesmas perguntas permanecem:**
 - Como a equipe sabe onde está?
 - Como criar prioridades certas?
 - Como justificar ou validar investimentos?
 - Como transmitir o impacto?

↳ Desempenho e eficiência

- **Mais entradas e métricas são necessárias** à medida que o desempenho melhora;
- Monitore o que importa e garanta investimentos adequados para **atingir seus objetivos.**



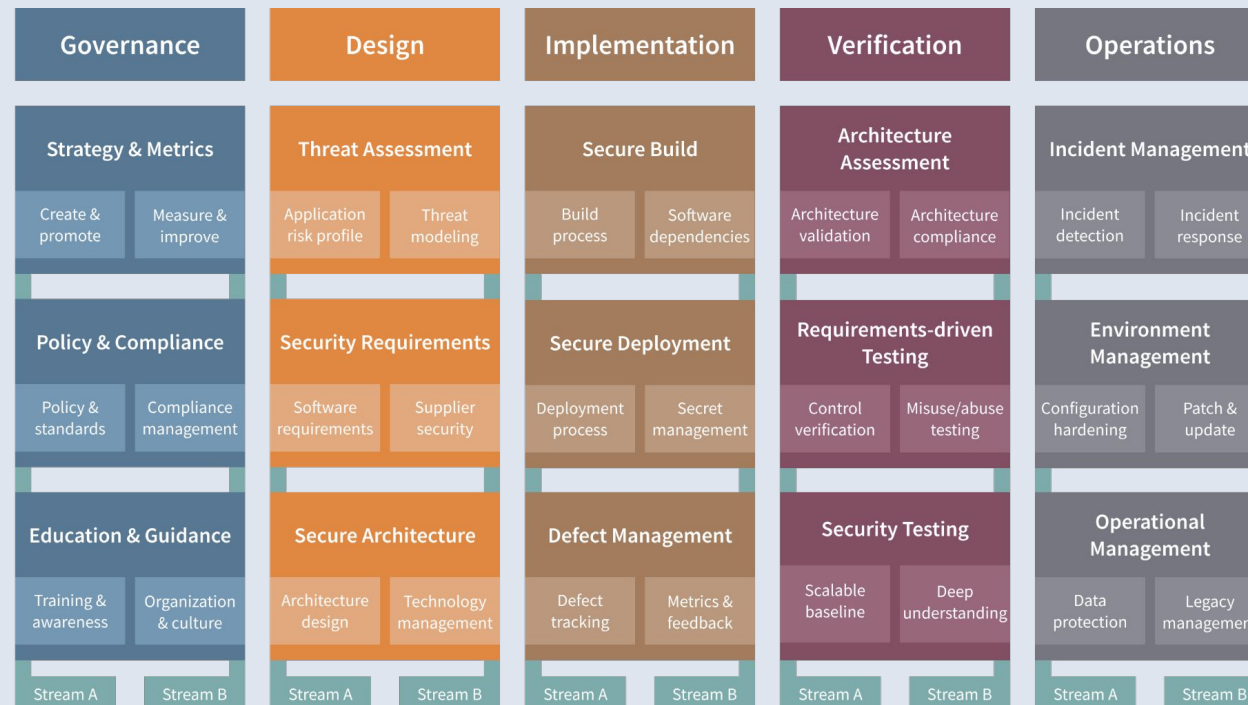


Sucesso vai depender do propósito em si

- **Objetivo da Segurança de Aplicações:** garantir a segurança dos sistemas de software, evitando consequências adversas.
- **Principais metas:**
 - Equilibrar risco e custo.
 - **Aumentar a maturidade com OWASP SAMM.**




OWASP SAMM



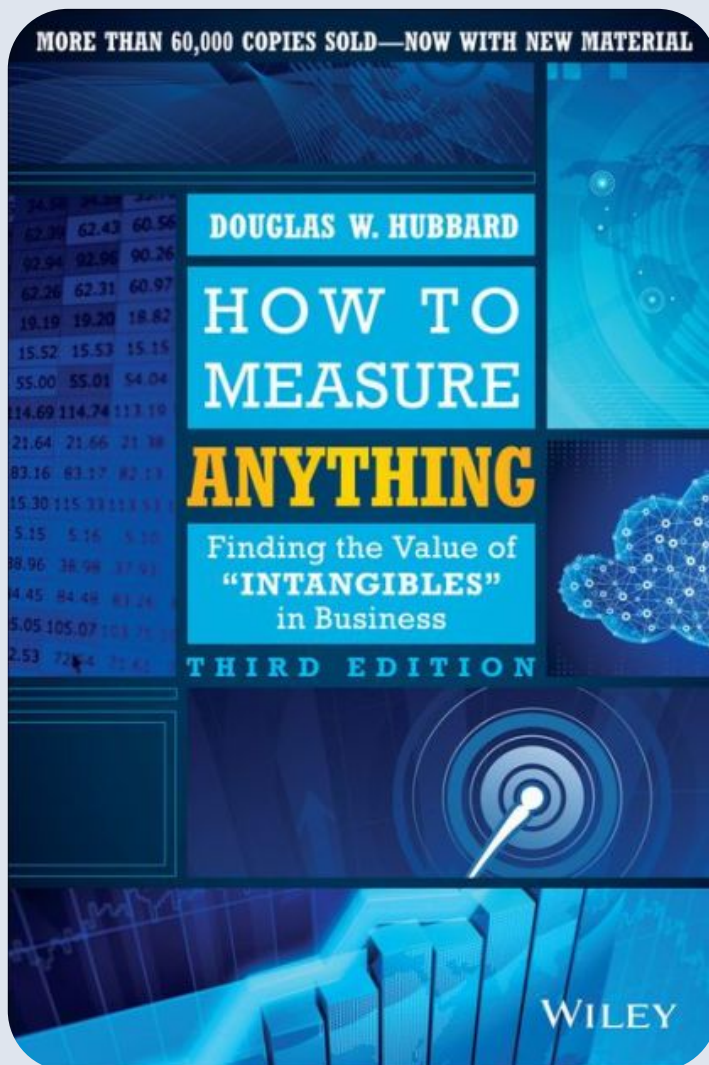
Key changes in OWASP SAMM v2. OWASP, 2024.





 “*Você não pode melhorar o que não pode medir*”. Mas, então, o que realmente significa **medir**?





Livro: How to Measure Anything Workbook

Métricas e KPIs

- **Métricas são medidas quantitativas** usadas para avaliar, comparar ou acompanhar o desempenho de uma empresa, departamento ou processo.
- **Os KPIs são indicadores importantes para o seu negócio e o seu objetivo**, enquanto uma métrica é apenas algo a ser medido.
- Auxiliam a **explicar numericamente o resultado de ações do negócio**.

Mapeamento
da Superfície de
Ataque
=
Inventário de
ativos
=
Gestão de Ativos
e Risco



↘ Métricas

- Exemplo:

Número de Vulnerabilidades Detectadas:

Quantidade total de vulnerabilidades identificadas em um período específico.

- **São úteis para monitorar e identificar problemas**, mas não necessariamente indicam o desempenho em relação a objetivos estratégicos.

↘ KPIs

- Exemplo:

Redução de Vulnerabilidades Críticas:

Percentual de redução de vulnerabilidades críticas ao longo do tempo.

- **Ajudam a medir o progresso em direção a metas específicas** e são usados para avaliar o sucesso das iniciativas de segurança.





Fonte, metodologia, automação e orquestração




DevSecOps Pipeline

- **Considerar fonte de dados, origem e metodologia** na coleta para métricas;
- **Implementar processos automatizados** para garantir consistência e reduzir erros humanos;
- **Garantir que os dados coletados sejam precisos e confiáveis;**
- **Orquestração para integrar e coordenar dados de diferentes ferramentas** de segurança para cobrir todas as etapas do ciclo de vida do desenvolvimento;
- **Desduplicação para eliminar dados duplicados** para manter a integridade das informações.





 **“Métricas são usadas para contar uma história e justificar uma ação, como o aumento do orçamento de segurança, e argumentar a favor de mudanças”**

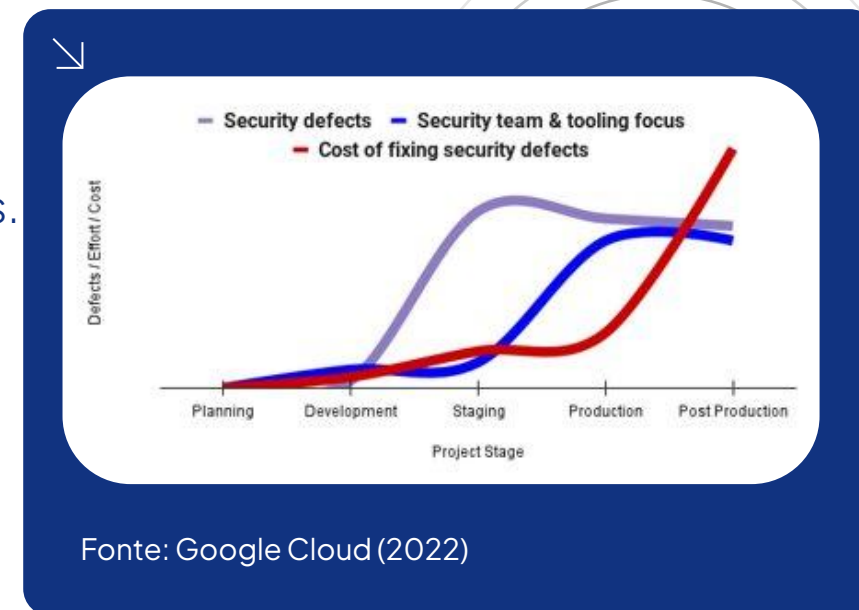
(OWASP, 2024).





Métricas de SLDC conforme a OWASP

- **Importância das Métricas:** melhoram a maturidade da segurança ao medir o progresso nas metas definidas.
- **Úteis para apresentar à gerência,** destacando lacunas e justificando recursos.
- **Medição ao Longo do Tempo:** mostram **tendências** trimestrais.
- **Indicam a direção desejada** e atividades que causaram mudanças significativas.
- **Fase do SDLC: Identificar problemas de segurança cedo** no ciclo de desenvolvimento é mais econômico.
- **Focar nas metas de maturidade** para detectar problemas precocemente.
- **Tempo de Resposta e SLA:** indicadores críticos da agilidade em responder a incidentes de segurança.





↘ Tipo de Métricas – Design – Modelagem de Ameaças

- Número de aplicações que possuem um perfil de risco definido;
- Número de modelos de ameaças ou atividades de modelagem de ameaças realizadas;
- Número de ameaças identificadas em modelos de ameaças;
- Tempo para revisar e mitigar ameaças durante o design;

KPIs (Indicador-Chave de Desempenho)

- Percentual de componentes críticos do sistema que foram analisados em uma modelagem de ameaças.
- Percentual de aplicação com requisitos de segurança definidos.
- Tempo médio necessário para mitigar as ameaças identificadas na fase de design.
- Percentual de equipes de desenvolvimento que integram práticas seguras desde o design.
- Percentual de redução de vulnerabilidades críticas detectadas após a fase de design (durante a implementação ou testes) devido às correções feitas no design.





↘ Tipo de Métricas – Desenvolvimento – Revisões de Código

- Número de revisões de código realizadas;
- Número de descobertas nas revisões de código;
- Tempo para revisar e mitigar as vulnerabilidades identificadas durante as revisões de código;

KPIs (Indicador-Chave de Desempenho)

- Percentual de revisões de código que incluíram verificações específicas de segurança em relação ao total de revisões;
- Média de vulnerabilidades de segurança detectadas por revisão de código.
- Tempo médio necessário para corrigir vulnerabilidades detectadas durante a revisão de código;
- Percentual de código que passou por revisão de segurança em relação ao total de código produzido durante o ciclo de desenvolvimento.
- Percentual de pull requests rejeitados ou revisados devido a problemas de segurança identificados durante a revisão de código.





↘ Tipo de Métricas – Implantação – Testes de Segurança

- Número de descobertas de testes de invasão;
- Número de descobertas em varreduras de vulnerabilidades (AST);
- Número de vulnerabilidades corrigidas;
- Número de bibliotecas e pacotes de terceiros analisados;

KPIs (Indicador-Chave de Desempenho)

- Tempo gasto para corrigir uma vulnerabilidade e se isso atende a um SLA.
- Qual o percentual de automação dos seus projetos.
- Percentual de áreas críticas da aplicação que foram cobertas pelos testes de segurança.
- Percentual de vulnerabilidades relatadas nos testes de segurança que são falsos positivos.
- Percentual de vulnerabilidades que foram reintroduzidas após a correção.
- Percentual de vulnerabilidades detectadas por ferramentas automatizadas em relação ao total de vulnerabilidades detectadas.





↘ Tipo de Métricas – Operações – Monitoramento

- Número de incidentes ocorridos em um período de 3 meses;
- Tempo decorrido entre a descoberta do incidente e sua solução;
- Quantidade de aplicações cobertas por um plano de incidentes;
- Número de sistemas desatualizados/legados;
- Quantidade de tentativas de ataque ou acesso não autorizado que foram bloqueadas automaticamente pelos sistemas de segurança em um período de tempo.

KPIs (Indicador-Chave de Desempenho)

- Tempo médio de resolução de incidentes de segurança, desde a descoberta até a mitigação completa.
- Percentual de sistemas e aplicações atualizados com patches de segurança no último trimestre.
- Percentual de incidentes de segurança detectados por ferramentas e processos de monitoramento proativo, em comparação com aqueles relatados por usuários ou após danos já causados.
- Percentual de alertas de segurança que foram identificados como falsos positivos no total de alertas emitidos.





↘ Tipo de Métricas – Cultura – Security Champions

- Número de módulos "secure by default" criados;
- Número de designs de arquitetura segura criados e fornecidos aos desenvolvedores;
- Número de Security Champions integrados;
- Número de atividades de treinamento introduzidas aos desenvolvedores;
- Número de desenvolvedores integrados em atividades de treinamento;
- Número de desenvolvedores engajados em atividades de treinamento específicas.

KPIs (Indicador-Chave de Desempenho)

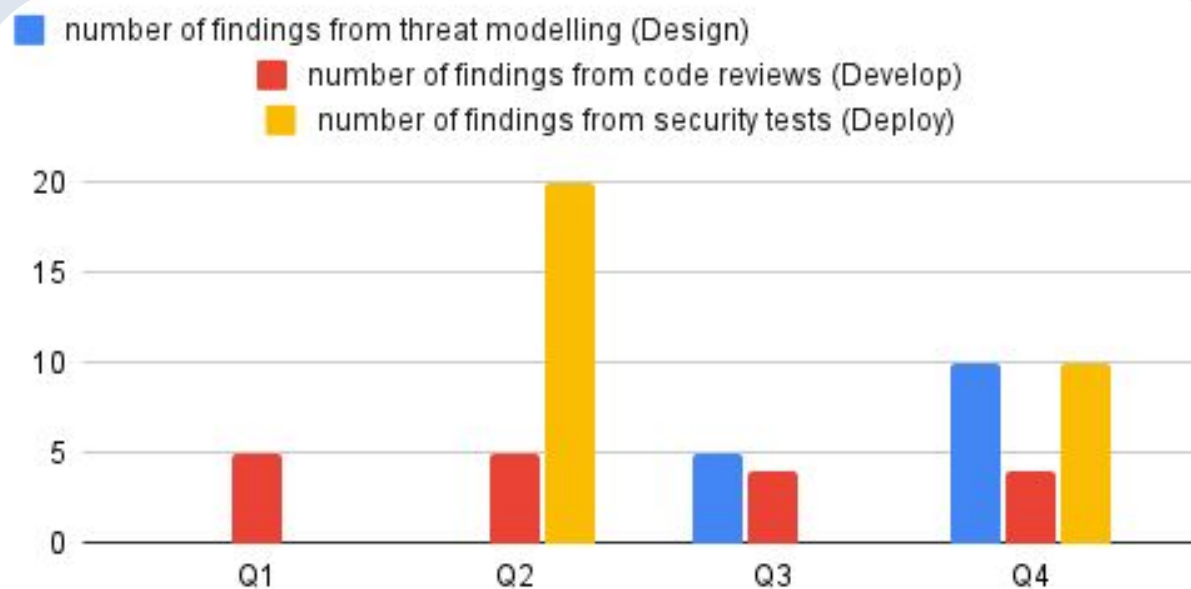
- Medir a redução percentual de incidentes de segurança em áreas cobertas por atividades de treinamento;
- Percentual de desenvolvedores que fornecem feedback positivo após o treinamento;
- Percentual de engajamento dos Security Champions nas atividades de Segurança.





Exemplo de gráfico:

Número de *findings* para cada fase do SDLC ao longo do ano



OWASP, 2024.



Métricas & Indicadores essenciais em AppSec

1.

Cobertura do código testado e projetado de maneira segura

2.

Número de vulnerabilidades e sua gravidade

3.

Tempo Médio para descobrir Vulnerabilidades (MTTD)

4.

Tempo Médio para corrigir Vulnerabilidades (MTTR)

5.

Treinamento e Conscientização de Segurança

6.

Pontuação Geral de Risco





Qual(is) métrica(s) devo escolher?

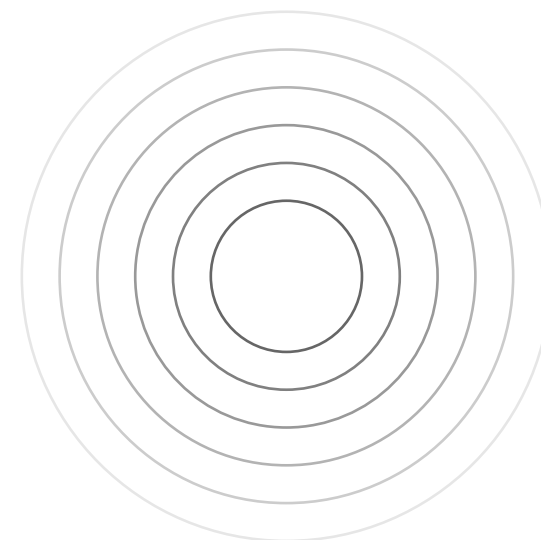
As métricas devem refletir os riscos que impactam diretamente a organização





Construindo um quadro robusto de métricas

- **Integrar métricas aos fluxos de trabalho é essencial;**
- Segundo a OWASP, **um quadro robusto de métricas** deve abordar três áreas principais:
 - **métricas de processo de segurança de aplicações;**
 - **métricas de risco;**
 - **métricas de ciclo de vida de desenvolvimento (SDLC).**
- **Perguntas que devem ser feitas para se construir um quadro de métricas** incluem:
 - "Como nossa organização está cumprindo as políticas de segurança?"
 - "Qual é o tempo médio de reparo por aplicação?"





↘ O quadro de métricas de AppSec vão te ajudar a responder perguntas como:

- Estamos fazendo **progresso** em nosso programa de AppSec?
- Nossos **investimentos** em ferramentas, pessoal e processos estão gerando resultados?
- Estamos **identificando** e **gerenciando** riscos de forma eficaz?
- Estamos **atendendo aos requisitos de conformidade** e padrões da indústria?
- Estamos **alocando nossos recursos** de forma eficiente?





Ao priorizar as métricas, mantenha em mente:

**Risco associado:**

O impacto das vulnerabilidades e incidentes no seu ambiente.

Criticidade do ativo:

O quão crítico o ativo é para o seu negócio.

Maturidade da sua equipe:

Organizações mais maduras podem focar em métricas avançadas de automação e processos.

Negócios em fase inicial devem focar em métricas mais básicas de vulnerabilidades e tempo de resposta.





Melhore o Monitoramento de **Métricas de AppSec** com Vantico





Métricas para Gestão de Vulnerabilidade



Vulnerabilidades por Criticidade



Crítica	88
Alta	0
Média	1
Baixa	2
Informativa	0

Vulnerabilidades por Status



Não Corrigido	48
Triagem	7
Re-test	8
Risco aceito	3
Corrigido	24

Tempo médio de dias para correção





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/blog)

[HTTPS://VANTICO.COM.BR/LABS](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

