DevSecOps

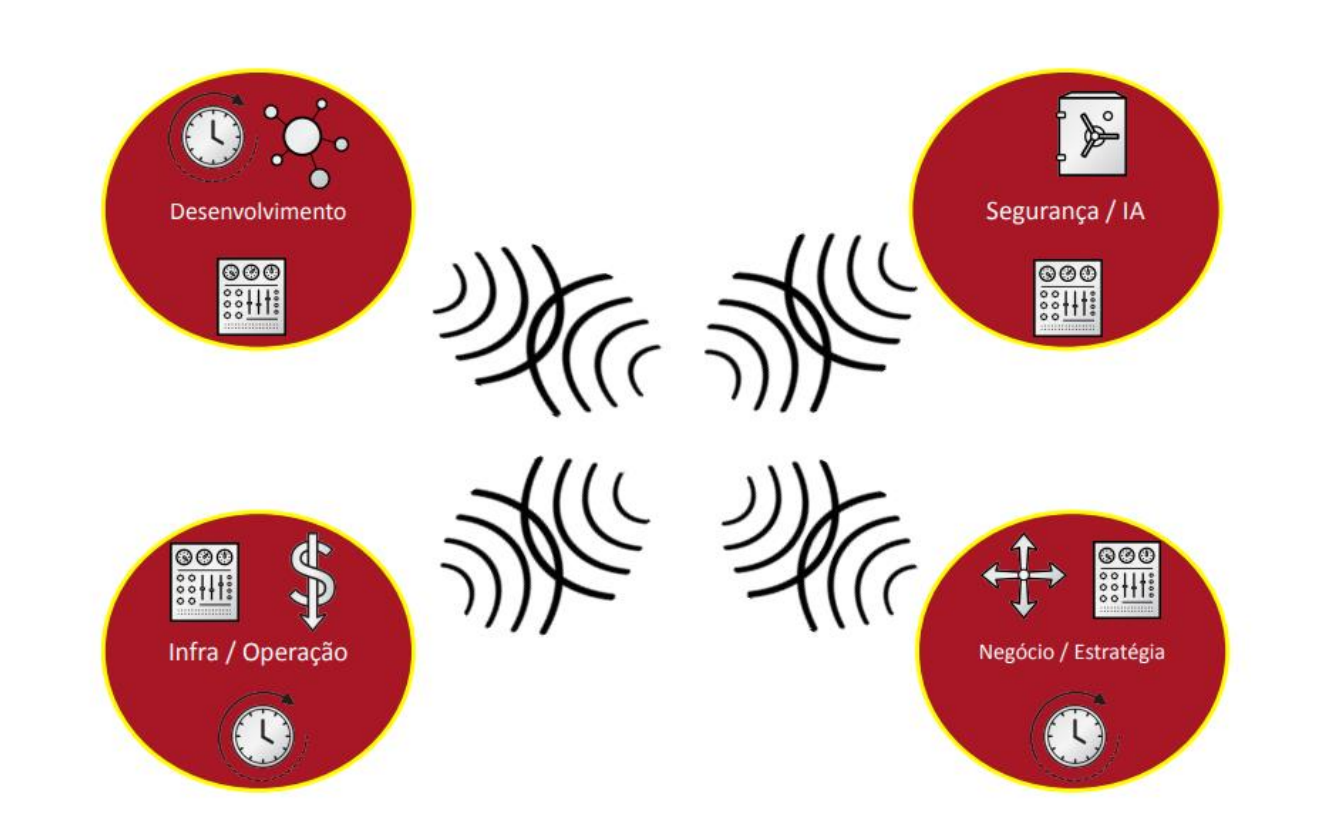
Professor Vitor Kessler

Introdução

- Sem DevSecOps:
  - A segurança era 'acrescentada' ao software no final do ciclo de desenvolvimento.
  - Atualizações de software eram liberadas apenas uma ou duas vezes por ano.
  - Com metodologias ágeis, segurança virou um gargalo.

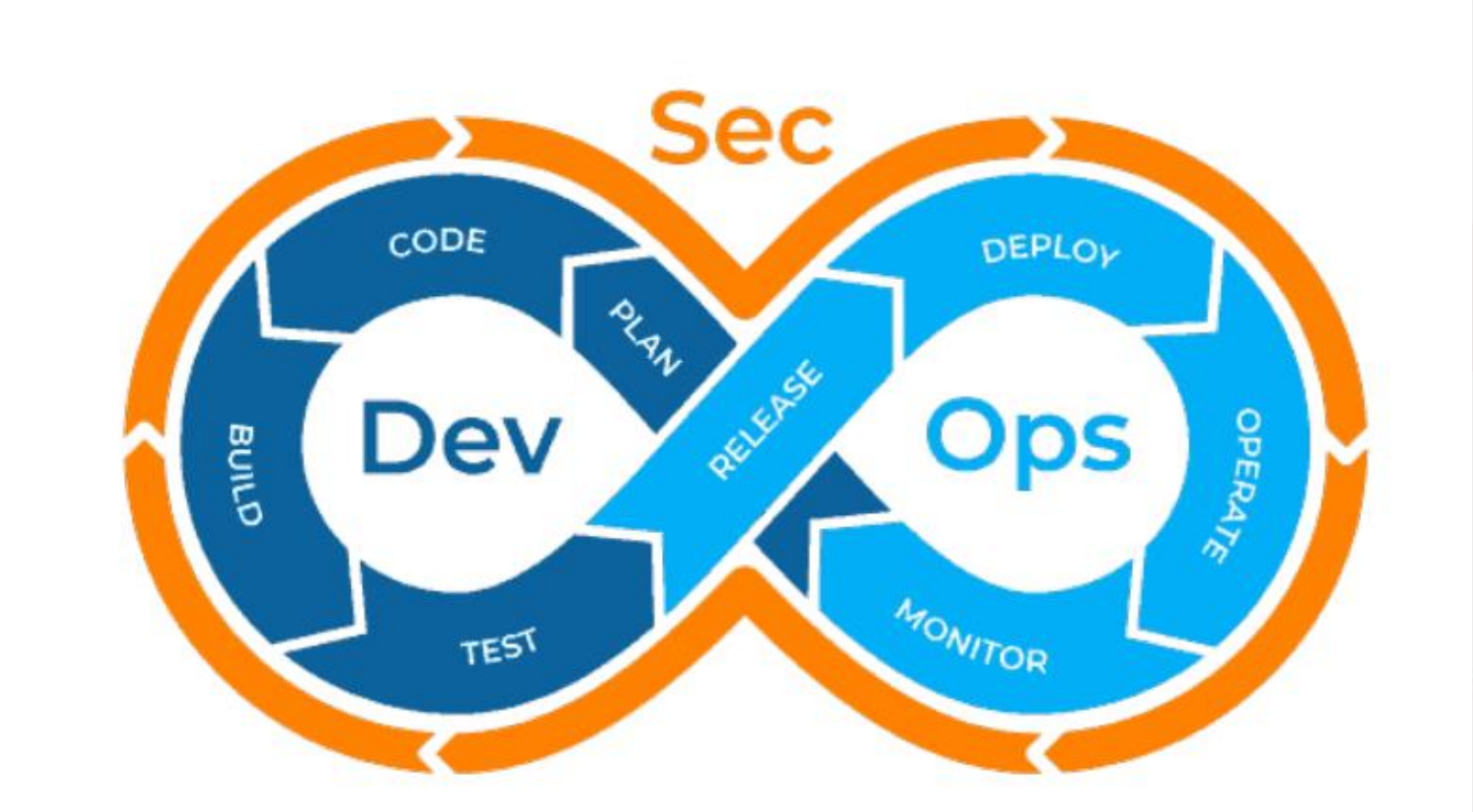
Introdução

- Com DevSecOps:



Introdução

- Com DevSecOps:

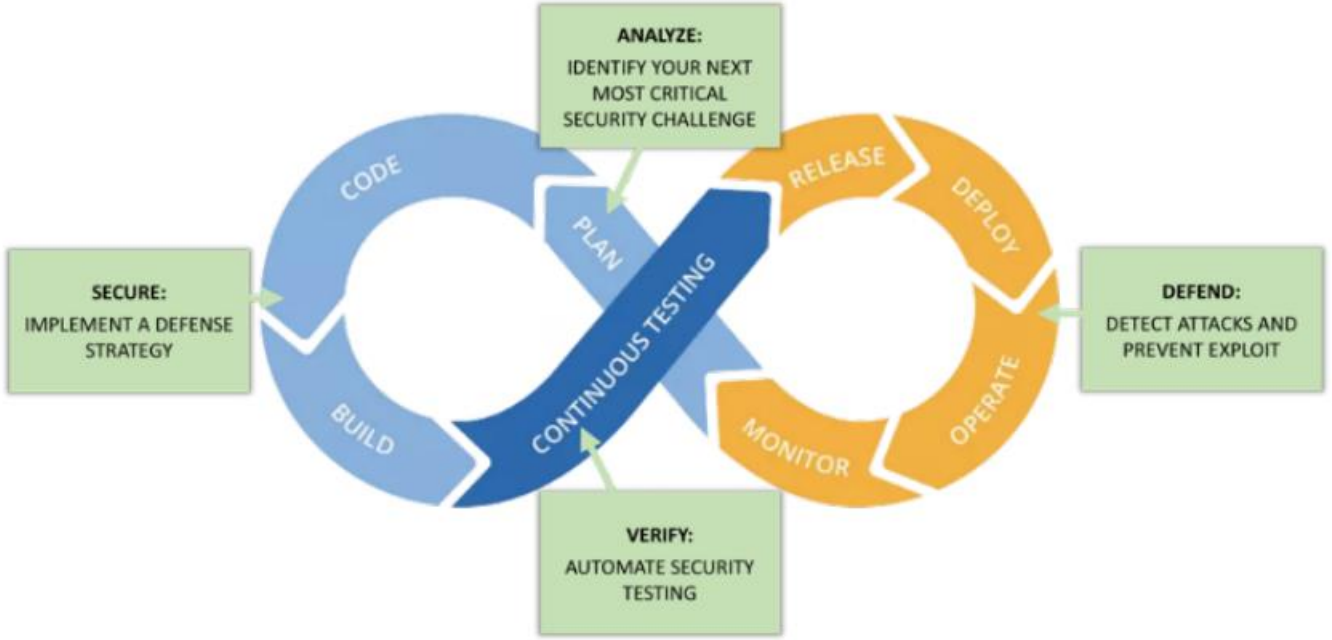


Introdução

- Desenvolvimento, Segurança e Operações.
- Incorpora a segurança em todas as fases do ciclo de vida de desenvolvimento de software.
- Permite o desenvolvimento de software seguro na velocidade do Agile e do DevOps.
- Aborda os problemas de segurança à medida que surgem, quando são mais fáceis, rápidos e baratos de corrigir.
- A segurança de aplicativos e infraestrutura é uma responsabilidade compartilhada das equipes de desenvolvimento, segurança e operações de TI.

Introdução

- Implantando DevSecOps:

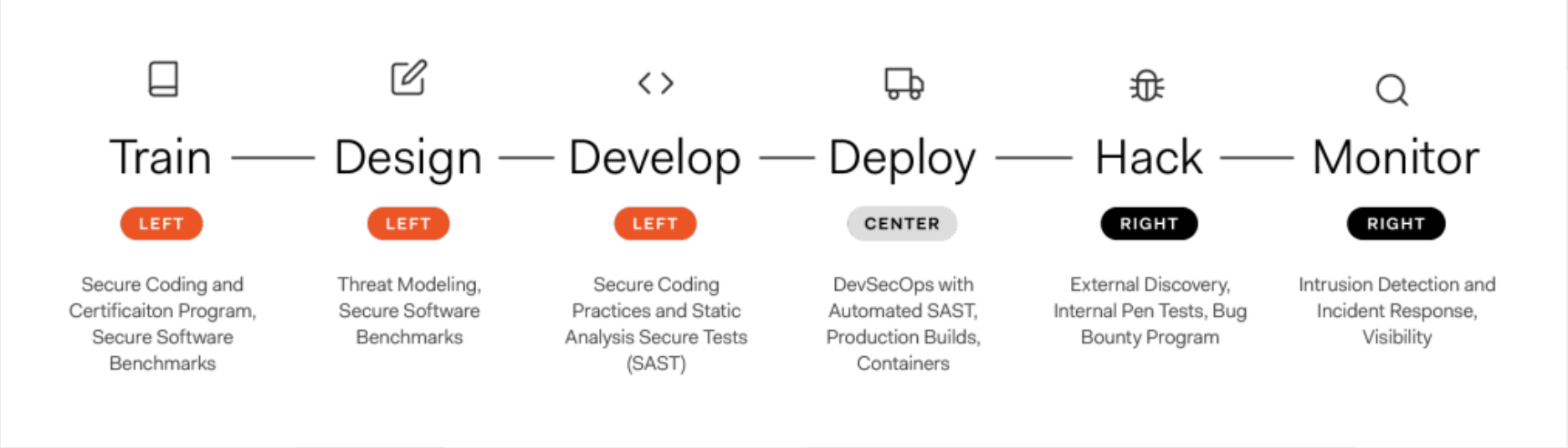


Introdução

- Benefícios:
  - Entrega de software rápida e com boa relação custo-benefício.
  - Segurança aprimorada e proativa.
  - Correção de vulnerabilidade de segurança acelerada.
  - Automação compatível com o desenvolvimento moderno.
  - Um processo repetível e adaptativo.

Práticas

- Shift Left:
  - Incentiva os engenheiros de software a mover a segurança da direita (final) para a esquerda (início) do processo de DevOps (entrega).
  - Arquitetos e engenheiros de segurança cibernética fazem parte da equipe de desenvolvimento.



Práticas

- Educação de Segurança:
  - Garantir que todos na organização entendam a postura de segurança da empresa e sigam os mesmos padrões.
  - Todos os envolvidos no processo de entrega devem estar familiarizados com os princípios básicos de segurança de aplicativos, os dez primeiros projetos de segurança de aplicativos da web (OWASP), testes de segurança de aplicativos e outras práticas de engenharia de segurança.

Práticas

- Cultura: Comunicação, pessoas, processos e tecnologia.
  - É importante e essencial comunicar as responsabilidades de segurança dos processos e propriedade do produto.
  - A equipe cria o ambiente de fluxo de trabalho que atenda às suas necessidades.
  - Os profissionais se tornam interessados no resultado do projeto.
- Rastreabilidade:
  - Permite rastrear itens de configuração em todo o ciclo de desenvolvimento até onde os requisitos são implementados no código.

Práticas

- Auditabilidade:
  - Os controles de segurança técnicos, procedimentais e administrativos precisam ser auditáveis, bem documentados e respeitados por todos os membros da equipe.
- Visibilidade:
  - a organização deve possuir um sistema de monitoramento sólido para:
    - Medir o ritmo da operação.
    - Enviar alertas.
    - Aumentar a conscientização sobre mudanças e ataques cibernéticos à medida que ocorrem.
    - Fornecer responsabilidade durante todo o ciclo de vida do projeto.

Questão de Concurso

- Prova: FGV - 2022 - TJ-DFT - Analista Judiciário - Análise de Sistemas
- A equipe de analista de sistemas Alfa aplica o DevSecOps ativamente em seu processo de desenvolvimento de software.
- Todos os membros da equipe Alfa são incentivados a se preocuparem com a segurança do software de forma proativa desde o início do processo de desenvolvimento, aplicando diretamente a prática DevSecOps:
- A shift left;
- B rastreabilidade;
- C auditabilidade;
- D visibilidade;
- E bug bounty.

Questão de Concurso

- Prova: FGV - 2022 - TJ-DFT - Analista Judiciário - Análise de Sistemas
- A equipe de analista de sistemas Alfa aplica o DevSecOps ativamente em seu processo de desenvolvimento de software.
- Todos os membros da equipe Alfa são incentivados a se preocuparem com a segurança do software de forma proativa desde o início do processo de desenvolvimento, aplicando diretamente a prática DevSecOps:
- A shift left;
- B rastreabilidade;
- C auditabilidade;
- D visibilidade;
- E bug bounty.