Curso DevOps

Aula 10 - DevSecOps

Prof. Esp. Guilherme Jorge Aragão da Cruz

guilherme.cruz@alumni.usp.br

linkedin.com/in/guijac

Roteiro

- Pilares da Segurança da Informação;
- DevSecOps:
  - Contexto Histórico;
  - Definição.
- Importância do Desenvolvimento Seguro;
- Atuais Desafios;
- Top 10 OWASP:
  - *Broken Access Control;*
  - *Cryptographic Failures;*
  - *Injection.*
- Caso Atento e Caso C6;
- Outros Casos Recentes;
- Mudanças Necessárias:
  - Pessoas;
  - Processos;
  - Tecnologias.
- Referências Bibliográficas.

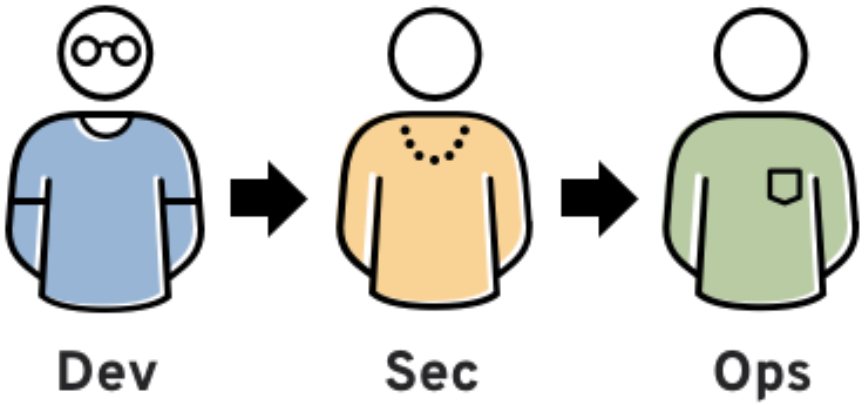
Pilares da Segurança da Informação

- **Confidencialidade**: informações sigilosas devem ser acessadas somente por pessoas autorizadas;
- **Integridade**: dados não devem ser alterados ou excluídos de forma não prevista ou autorizada;
- **Disponibilidade**: serviço ou o acesso às informações deve estar sempre disponível para quem possui autorização.

Fonte: Segurança da Informação | Matheus Almeida

DevSecOps: Contexto Histórico

- De forma similar a “Ops”, a equipe de segurança fazia parte de uma equipe mais isolada, que atuava no estágio final do desenvolvimento;
- Além da entrega de software e infraestrutura com agilidade, também é necessário que esta **entrega seja realizada com segurança**.

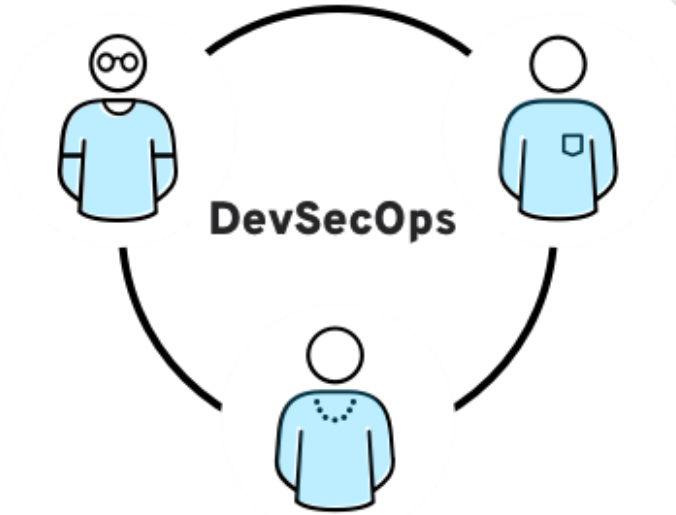


Fonte:DevSecOps: o que é e qual a diferença entre DevSecOps e DevOps (redhat.com)

DevSecOps: Definição

> *Pensar na segurança da **aplicação** e da **infraestrutura** desde o início;*
>
> ***Automatizar** barreiras de segurança, evitando que o fluxo de trabalho torne-se lento;*
>
> *Requer mais do que ferramentas novas: requer **mudanças culturais**.*

RED HAT (2023)



Fonte:DevSecOps: o que é e qual a diferença entre DevSecOps e DevOps (redhat.com)

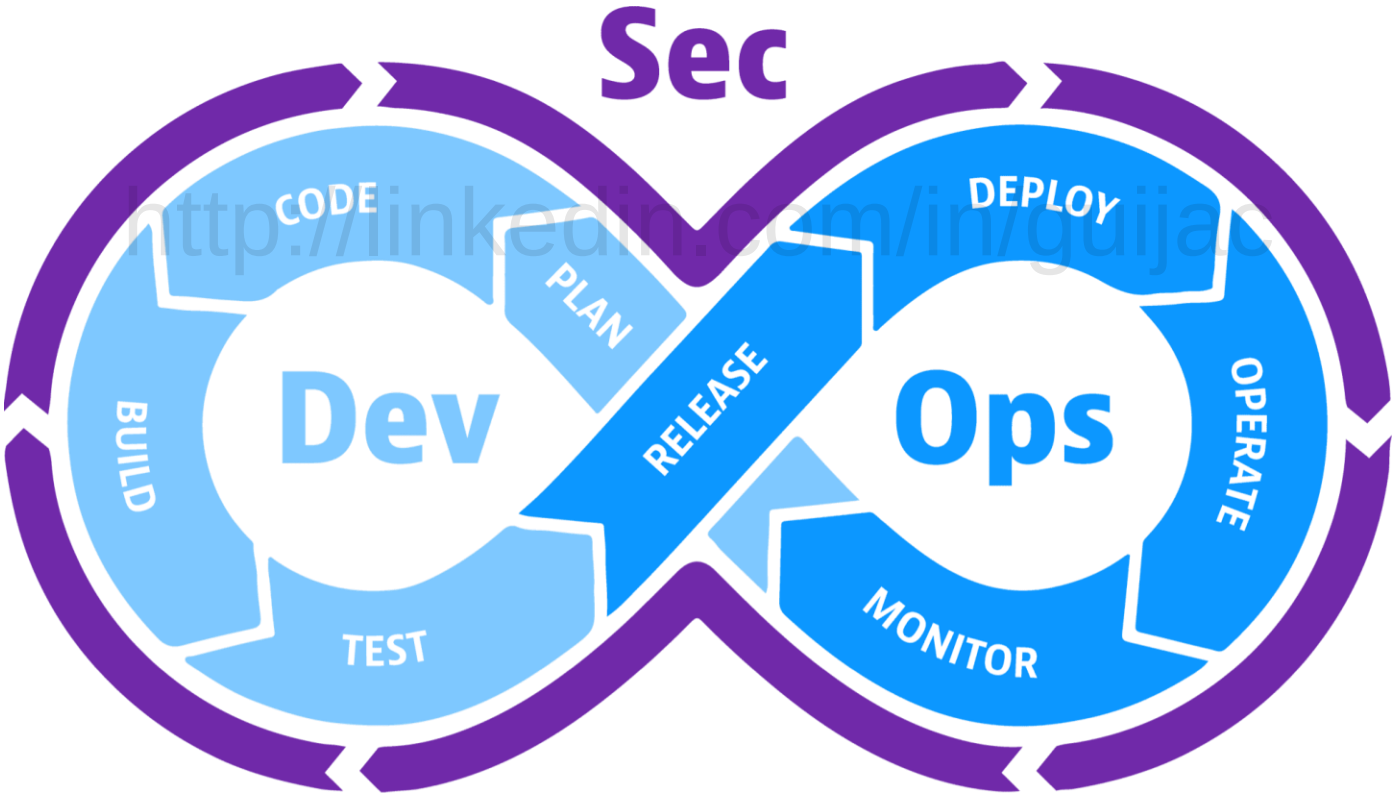
Importância do Desenvolvimento Seguro

- Cerca de 92% das aplicações possuem falhas ou vulnerabilidades exploráveis[1];
- Mais de 40 mil tentativas de ataque foram realizadas explorando a vulnerabilidade do Log4j[2];
- 80% dos clientes fecham com a concorrência após uma experiência ruim[3];
- O custo de um bug cresce exponencialmente conforme a sua fase de identificação[4].

[1] <https://www.securityweek.com/92-external-web-apps-have-exploitable-security-flaws-or-weaknesses-report>
[2] <https://tiinside.com.br/14/12/2021/check-point-research-alerta-sobre-vulnerabilidade-apache-log4j/>
[3] <https://www.adin.com.br/qual-importancia-da-experiencia-do-usuario/>
[4] <https://dzone.com/articles/the-exponential-cost-of-fixing-bugs>

Atuais Desafios

- Incluir a Segurança da Informação no ciclo de desenvolvimento de software.



Fonte: What is DevSecOps? And what you need to do it well (dynatrace.com)

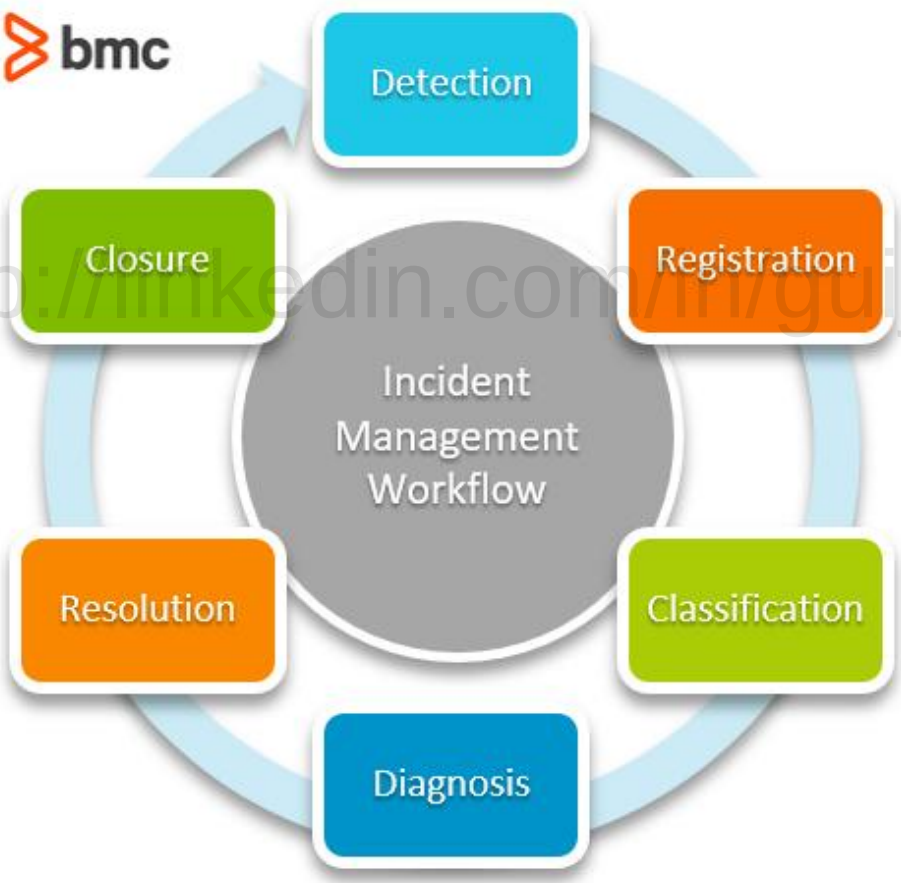
Atuais Desafios

- Conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD).

Fonte: [Infográfico: Conheça os 12 principais pontos sobre a LGPD | Opice Blum]

Atuais Desafios

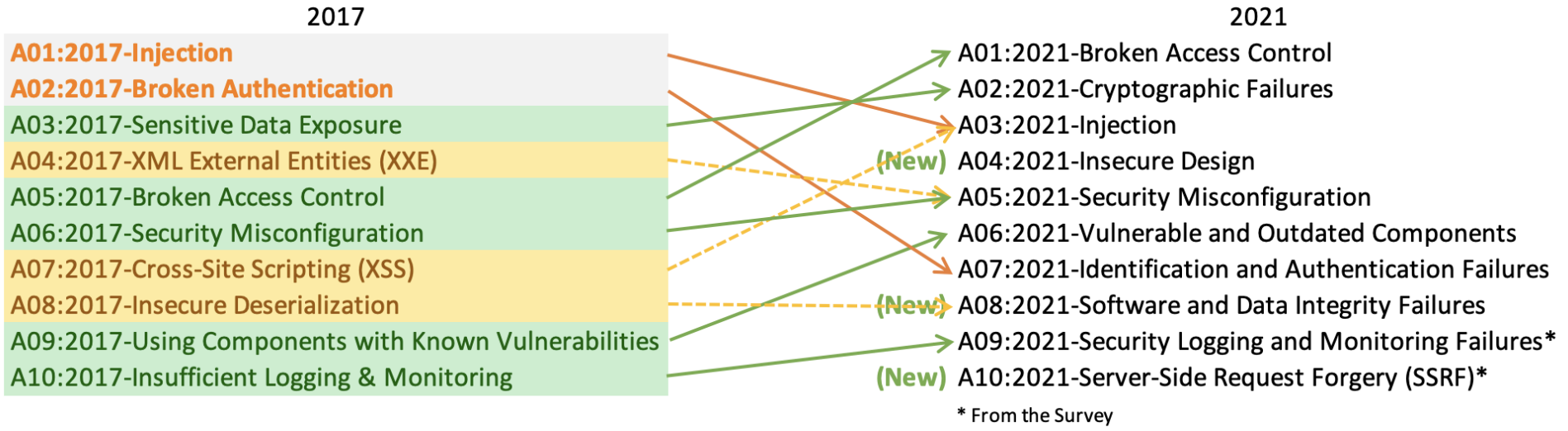
- Gerenciar e remediar incidentes rapidamente;
- Transformação digital segura e ágil.



Fonte: Incident Management: The Complete Guide – BMC Software

Top 10 OWASP

- Ranking feito com a análise de aproximadamente 500 mil aplicações;
- Foram elencadas oito categorias através dos dados recebidos e duas através de uma pesquisa sobre o tema.



Fonte: Open Web Application Security Project

Top 10 OWASP: *Broken Access Control*

- Uma violação nos controles de acesso de uma aplicação. Por exemplo, um determinado usuário conseguir acessar o conteúdo pertencente a outro.

tecnoblog

Notícias > Telecomunicações

Exclusivo: falha no Meu Vivo permite acessar CPF e telefone de outros clientes

Meu Vivo permite acessar fatura de outros clientes com CPF, nome e endereço; operadora já teve falha de segurança semelhante

Por Felipe Ventura
19/02/2021 às 17:53

Fonte: Exclusivo: falha no Meu Vivo permite acessar CPF e telefone de outros clientes – Tecnoblog

Top 10 OWASP: *Broken Access Control*

- Casos comuns: falta de **autorização** nas aplicações (existindo apenas a **autenticação**).

- Algumas abordagens para contorno:

  - Conceito de privilégio mínimo;
  - Governança de identidades (remoção de contas inativas, auditoria na criação de contas, etc.);
  - Correta implementação dos fluxos de autenticação e autorização.

Top 10 OWASP: *Cryptographic Failures*

- Exposição de dados sensíveis (como credenciais de acesso) através de um mal uso – ou mesmo não uso – de práticas de criptografia.

Fonte: Nova exposição de dados no Ministério da Saúde | Notícias | Baguete

Top 10 OWASP: *Cryptographic Failures*

- Casos comuns: uso de técnicas de codificação de dados que **não são criptografia**, como o Base64.

- Algumas abordagens para contorno:

  - Uso de técnicas de criptografia mais atualizadas;
  - Trabalhar com criptografia em trânsito e em repouso;
  - Não exibir senhas ou outros dados sensíveis em arquivos de fácil acesso, como logs de aplicação.

Top 10 OWASP: *Injection*

- Códigos maliciosos que podem ser inseridos das mais diversas formas em aplicações, como através de uma URL ou instrução SQL.

Fonte: [Cassinos rivais da Blaze invadem sites do governo para manipular o Google (uol.com.br)]

Top 10 OWASP: *Injection*

- Casos comuns: erros clássicos de injeções, como “SQL Injection” (veremos na prática).

- Algumas abordagens para contorno:

  - Separar adequadamente comandos e dados dinâmicos, evitando uma concatenação direta de caracteres;
  - Uso de frameworks de apoio para construção e execução de instruções SQL;
  - Adoção de tecnologias que possibilitem identificar um comportamento anômalo em um ambiente.

Top 10 OWASP: *Injection*

- Qual é o trecho de código vulnerável?
- Há mais de um? 🤔

```
1 from sqlalchemy.sql import text
2 from sqlalchemy import create_engine
3
4 db_connect = create_engine('mysql://root:my-password@db/my_database’)
5 conn = db_connect.connect()
6
7    sql_Query = text("select * from user where id=:user_id")
8    result = conn.execute(sql_Query, parameters=dict(user_id = id))
9
10   sql_Query = text("select * from user where id={}".format(id))
11   result = conn.execute(sql_Query)
```

Top 10 OWASP: *Injection*

- Qual é o trecho de código vulnerável?
- Há mais de um? 🤔

```
1 from sqlalchemy.sql import text
2 from sqlalchemy import create_engine
3
4 db_connect = create_engine('mysql://root:my-password@db/my_database’)
5 conn = db_connect.connect()
6
7     sql_Query = text("select * from user where id=:user_id")
8     result = conn.execute(sql_Query, parameters=dict(user_id = id))
9
10    sql_Query = text("select * from user where id={}".format(id))
11    result = conn.execute(sql_Query)
```

Caso Atento

Canaltech

O ataque de ransomware sofrido em outubro do ano passado pela Atento, uma das maiores empresas brasileiras do setor de atendimento, gerou um impacto de mais de R$ 197 milhões para a companhia. O valor envolve as perdas de faturamento pela interrupção nas atividades, que estaria na casa dos R$ 164 milhões, bem como cerca de R$ 32 milhões em esforços de controle e contenção de danos.

Fonte: Atento teve perdas de R$ 197 milhões após sofrer golpe de ransomware - Canaltech

Caso C6 Bank

C6 Bank: usuários desviam R$ 23 milhões via brecha no app; entenda o caso

Fraude foi aplicada por correntistas, que descobriram falha em um produto de investimento da fintech. Banco digital ainda não se pronunciou sobre o caso; confira

Por Marcela Franco, para o TechTudo

03/05/2022 15h13 · Atualizado há 3 semanas

O **C6 Bank** teve um desvio fraudulento de R$ 23 milhões feito por usuários. O caso aconteceu após cerca de cinco mil correntistas da fintech encontrarem uma brecha no sistema do banco digital, no produto de investimento CDB Crédito. As informações foram divulgadas com exclusividade pela revista Veja na última sexta-feira (29), e a fraude é investigada pela Polícia Civil de São Paulo em duas vertentes.

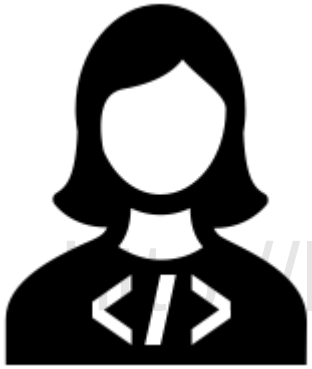
Fonte: C6 Bank: usuários desviam R$ 23 milhões via brecha no app; entenda o caso | Bancos digitais | TechTudo

Outros Casos Recentes

Fonte: [Incidentes Relevantes | IBRASPD]

Mudanças Necessárias: Pessoas

Time de Desenvolvimento



- Meu código não tem erros;
- Essa solução é a melhor;
- Isto não é responsabilidade da aplicação.

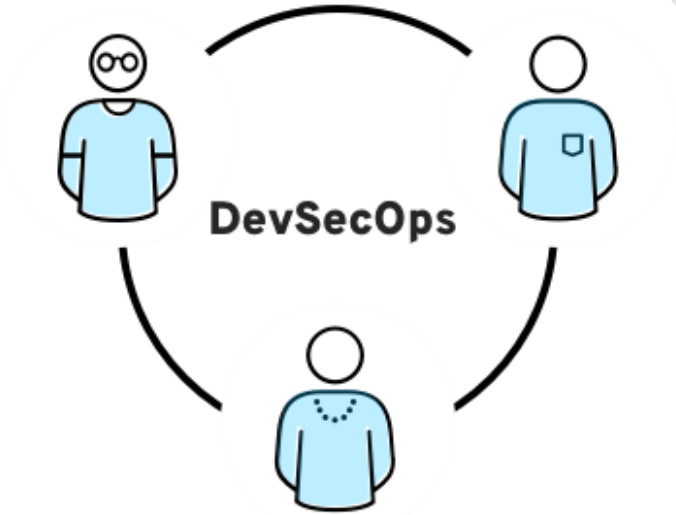
Time de SI

- Não pode;
- Achei essa vulnerabilidade em produção;
- Isto não está compliance.

Mudanças Necessárias: Processos

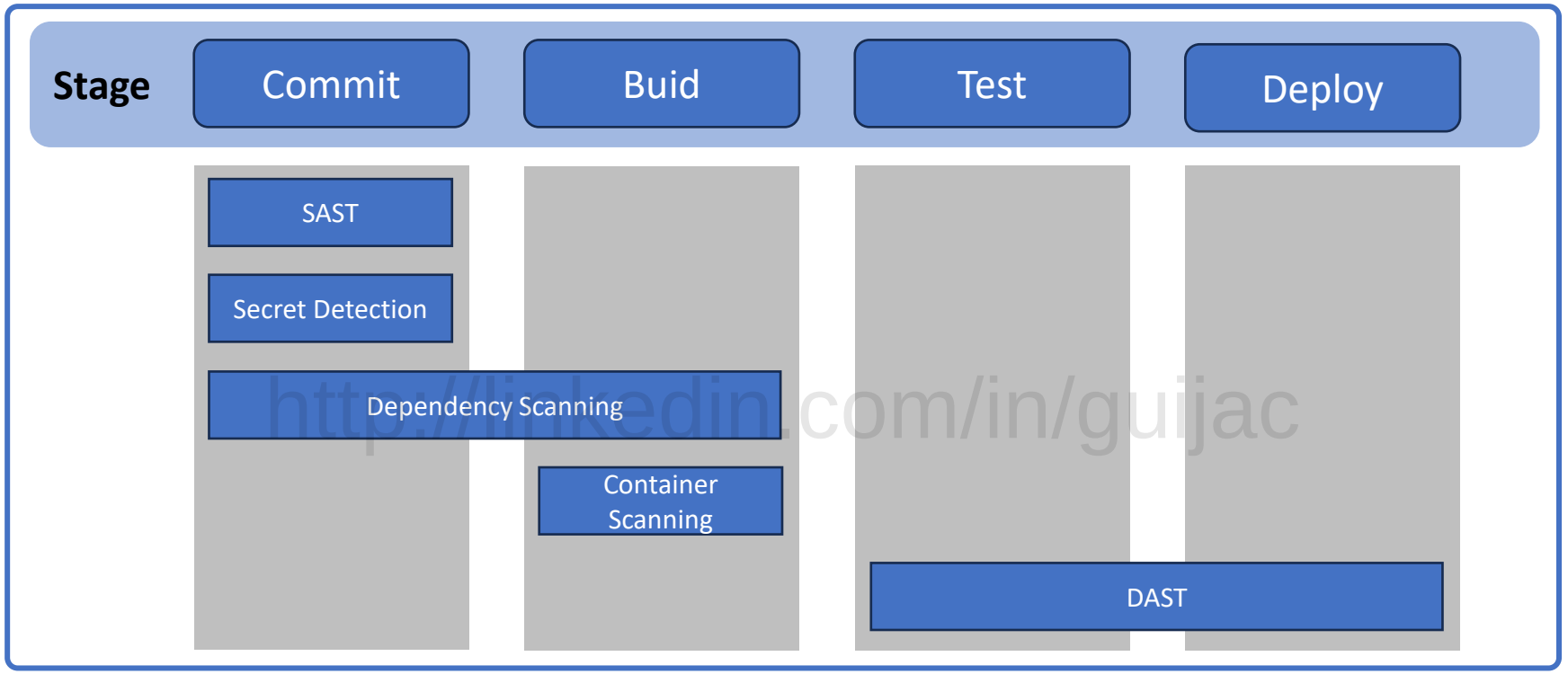
> *Pensar na segurança da **aplicação** e da **infraestrutura** desde o início;*
>
> ***Automatizar** barreiras de segurança, evitando que o fluxo de trabalho torne-se lento;*
>
> *Requer mais do que ferramentas novas: requer **mudanças culturais**.*

RED HAT (2023)



Fonte:DevSecOps: o que é e qual a diferença entre DevSecOps e DevOps (redhat.com)

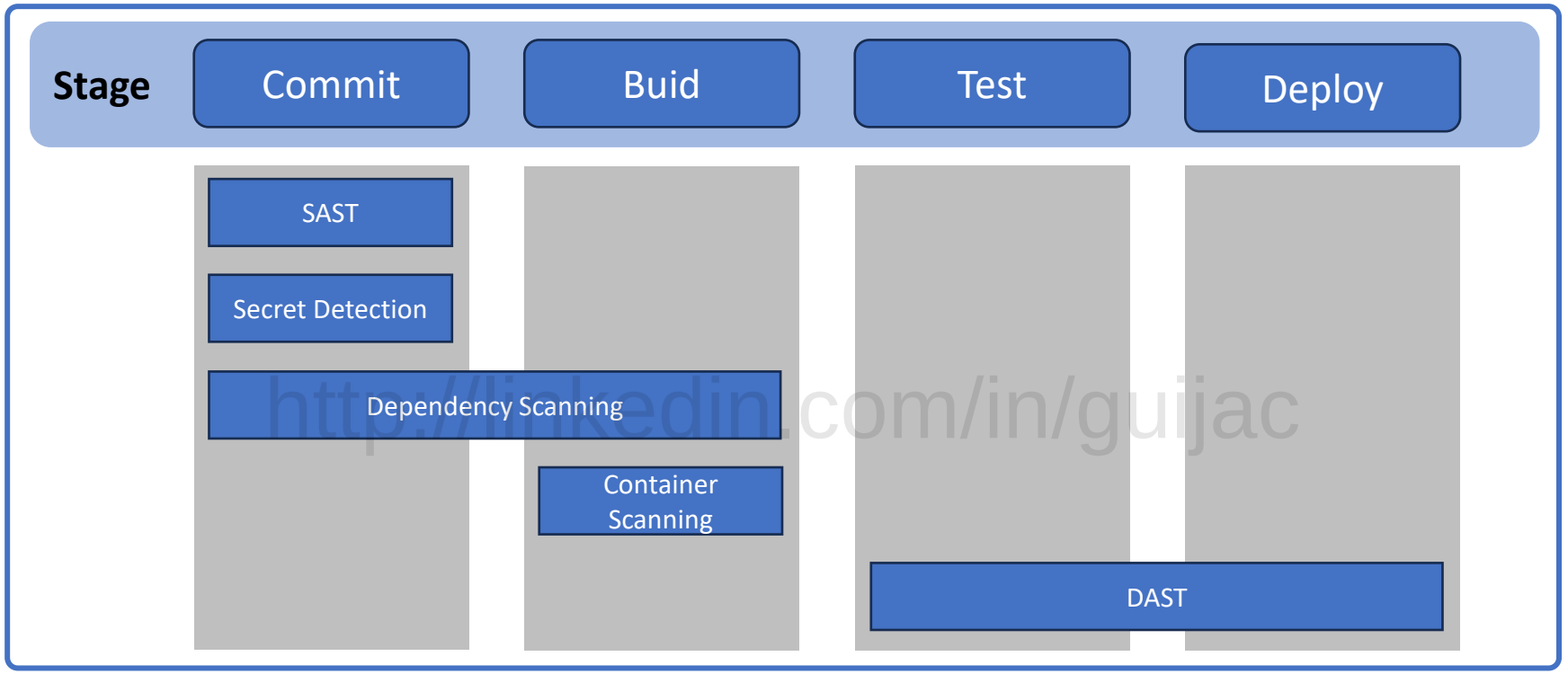
Mudanças Necessárias: Tecnologias



Fonte: Adaptado de Application security | GitLab

- **SAST: S**tatic **A**pplication **S**ecurity **T**esting, analisa o **código-fonte** para localizar vulnerabilidades (teste caixa-branca);
- **Secret Detection:** realiza a análise do **repositório** para localizar valores confidenciais como senhas, chaves ou tokens.

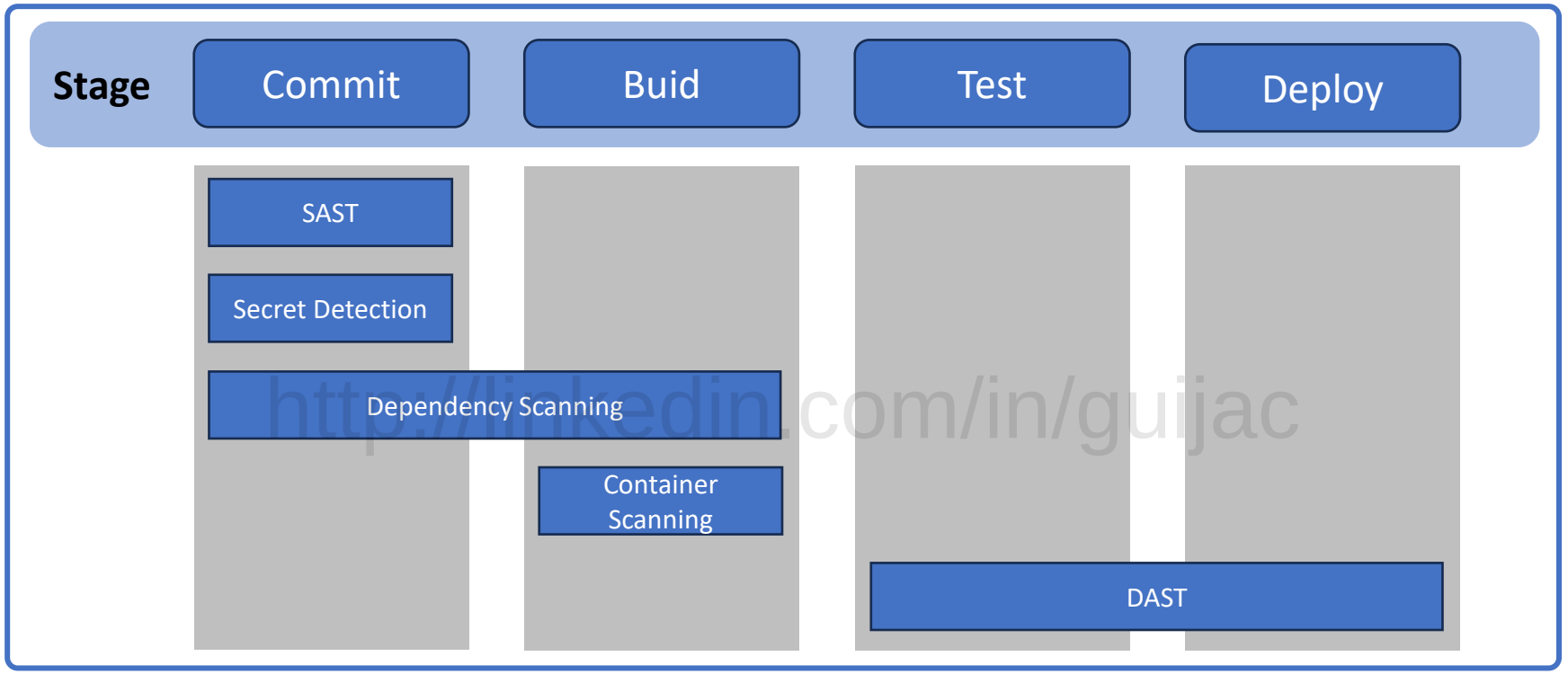
Mudanças Necessárias: Tecnologias



Fonte: Adaptado de Application security | GitLab

- **Dependency Scanning** e **Container Scanning:** parte da ***S**oftware **C**omposition **A**nalysis* (SCA), inspeciona itens que a sua aplicação faz uso, geralmente importados de fontes externas ao invés de escritos pela equipe de desenvolvimento.

Mudanças Necessárias: Tecnologias



Fonte: Adaptado de [Application security | GitLab]

- **DAST:** **D**ynamic **A**pplication **S**ecurity **T**esting, analisa uma aplicação em **tempo de execução** para localizar vulnerabilidades (teste caixa-preta).

Referências Bibliográficas

- CONVISO. **O que é Arquitetura de Segurança?** https://blog.convisoappsec.com/afinal-o-que-e-arquitetura-de-seguranca/. Acesso em 23 out 2023;

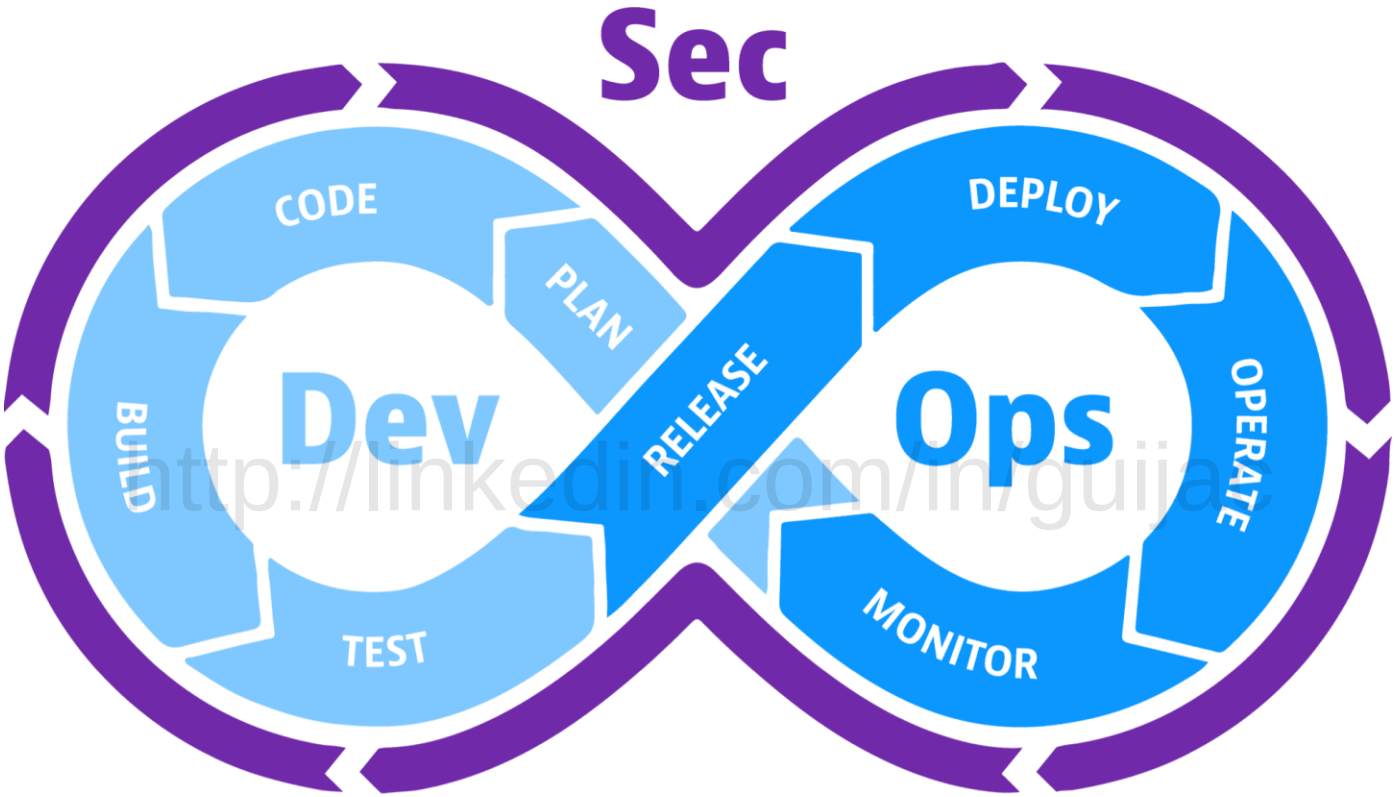
- CONEXIAM. **O que é Arquitetura de Segurança**. https://conexiam.com/pt/what-is-security-architecture/. Acesso em 23 out 2023;

- CTIR Gov - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo. **ALERTA 08/2023**. Disponível em https://www.gov.br/ctir/pt-br/assuntos/alertas-e-recomendacoes/alertas/2023/alerta-08-2023. Acesso em 03 Abr 2024;

- OWASP. **Open Web Application Security Project**. Disponível em https://owasp.org/Top10. Acesso em 03 mai 2022;

- PRIME CONTROL. **OWASP: Conheça as 10 maiores vulnerabilidades de software**. Disponível em https://www.primecontrol.com.br/owasp-conheca-as-10-maiores-vulnerabilidades-de-software/. Acesso em 29 mar 2023;

Por hoje (de teoria!) é só!



Fonte: What is DevSecOps? And what you need to do it well (dynatrace.com)

Prof. Esp. Guilherme Jorge Aragão da Cruz

guilherme.jacruz@sp.senac.br

linkedin.com/in/guijac

Licença

- Este conteúdo está licenciado sob a Licença Creative Commons Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional (CC BY-NC-SA 4.0).
- Todos os direitos autorais sobre este conteúdo pertencem ao autor, e este material não pode ser usado comercialmente sem autorização expressa.
- Para ver o texto completo da licença, acesse o https://creativecommons.org/licenses/by-nc-sa/4.0/legalcode.

Prof. Esp. Guilherme Jorge Aragão da Cruz

guilherme.cruz@alumni.usp.br

linkedin.com/in/guijac