prezensa

COMO A Z ESTRUTUROU O CICLO DE SEGURAÇA CONTÍNUA

sem comprometer a velocidade da entrega

CENÁRIO

Uma operação DevOps madura, pronta para dar o próximo passo

Foi identificada a necessidade de verificar vulnerabilidades em aplicações novas e em produção. Já contava com uma esteira CI/CD estruturada, garantindo automação e entrega contínua.
Com o crescimento da base de aplicações e aumento da criticidade dos sistemas, tornou-se necessário elevar o nível de proteção, não apenas reagindo a vulnerabilidades, mas antecipando-as.

O desafio era evoluir para DevSecOps de forma estruturada.

DESAFIO

4 FRICÇÕES ESTRUTURAIS NO PIPELINE.

01 Segurança Tardia

Vulnerabilidades identificadas apenas após consolidação do código ou próximas ao deploy, aumentando custo de correção e impacto no fluxo de entrega.

02 Validações Manuais

Ausência de bloqueios automáticos exigia revisões pontuais, criando gargalos e inconsistência na aplicação de políticas.

03 Risco de Rollback

Falhas detectadas em homologação ou pré-produção geravam ciclos adicionais de correção, comprometendo previsibilidade e tempo de entrega.

04 Falta de Governança

Sem gates técnicos estruturados, decisões críticas ficavam dispersas, reduzindo controle sobre padrões mínimos de segurança.

A segurança ainda não estava integrada ao fluxo.

O QUE FIZEMOS

ARQUITETURA DE CONTINUOUS SECURITY INTEGRADO AO CI/CD

1 SEGURANÇA ANTES DO AVANÇO

A partir da esteira DevOps já existente, estruturamos o modelo CI/CD-CS (Continuous Security), incorporando validações automatizadas desde o commit.

2 A ESTEIRA VALIDATE

A cada commit ou merge na branch de desenvolvimento, o pipeline executa automaticamente validações de workflow, qualidade de código e vulnerabilidades (dependências e código).

A política aplicada foi que nenhuma vulnerabilidade seria aceita.
A aplicação só avança com aprovação total.

3 SEGURANÇA PÓS-DEPLOY

Implementamos escaneamento dinâmico em homologação, com OWASP ZAP e Snyk DAST, ampliando a validação para aplicações já implantadas.
Se vulnerabilidades são identificadas, o fluxo retorna para correção antes de qualquer promoção para produção.

MÉTODO

CONTINUOUS SECURITY COMO ARQUITETURA ESTRUTURANTE

Como parte do modelo People Tech, estruturamos a evolução a partir de um blueprint de segurança integrada ao fluxo de engenharia.

Organizamos o modelo com:

- Segurança incorporada desde o commit
- Bloqueios automáticos orientados por política
- Responsabilidade distribuída entre os squads
- Governança técnica integrada ao pipeline
- Monitoramento contínuo além do deploy

Mais do que adicionar ferramentas, estruturamos um sistema onde segurança se tornou parte do modo de operar da engenharia.

RESULTADOS

Segurança que virou capacidade de entrega

GATE AUTOMÁTICO
como padrão mínimo de segurança

100%
de validações automatizadas antes da promoção

ZERO
Vulnerabilidades críticas em produção

CULTURA DISTRIBUIDA
Segurança incorporada aos squads

Continuous Security deixou de ser prática isolada e tornou-se capacidade organizacional.