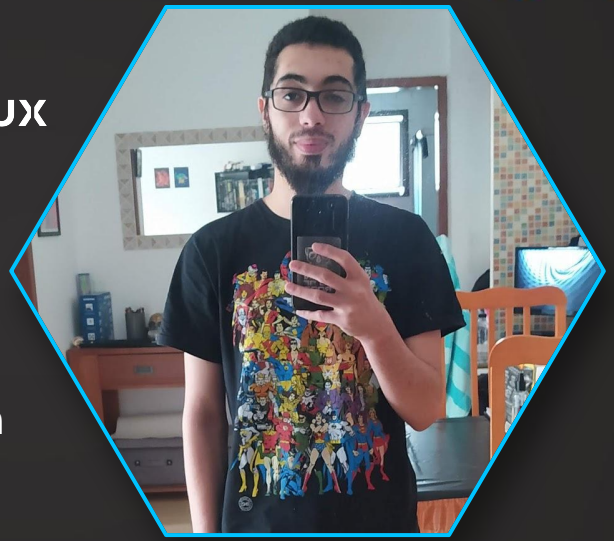
Hardening Automatizado

Aumentando a Segurança de Servidores Linux com Ansible

Whoami

Yago Ésquines

- Coordenador de TI na 4·Linux
- Bacharel em Ciência da Computação
- Tecnólogo em Segurança da Informação
- + 7 anos de experiência em projetos FOSS (Free and Open Source Software



Linux Professional Institute LPIC-1 LINUX ADMINISTRATOR

Linux Professional Institute LPIC-2 LINUX ENGINEER

CERTIFIED kubernetes ADMINISTRATOR

DevOps ESSENTIALS CERTIFIED ITCERTS

Agenda

01

Segurança vs Automação

Introdução a Segurança Ágil.

02

DevSecOps

Identificar onde a Segurança Ágil se encaixa nisso tudo.

03

Hardening e Ansible

Conhecer o que é Hardening e entender o funcionamento do Ansible.

04

Demo

Demonstração práticas de automações voltadas para segurança.

01

Segurança vs Automação

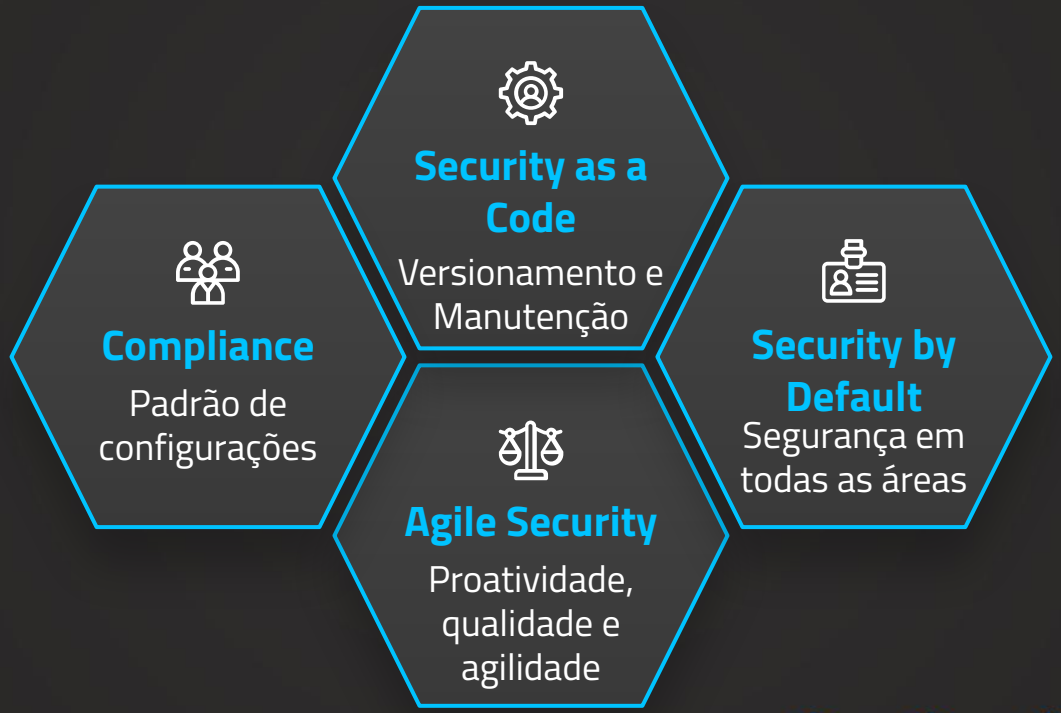
Use 1234 as you password again! I dare you, I DOUBLE DARE YOU!

Segurança da Informação

Controles básicos de Segurança da Informação:

- Garantir a configuração de boas práticas
- Garantir a integridade e privacidade dos dados
- Realizar Controlar pleno de acesso
- Mitigar ataques ou incidentes de segurança
- Identificar potenciais vulnerabilidades
- Manter a conformidade com frameworks e regulamentações.

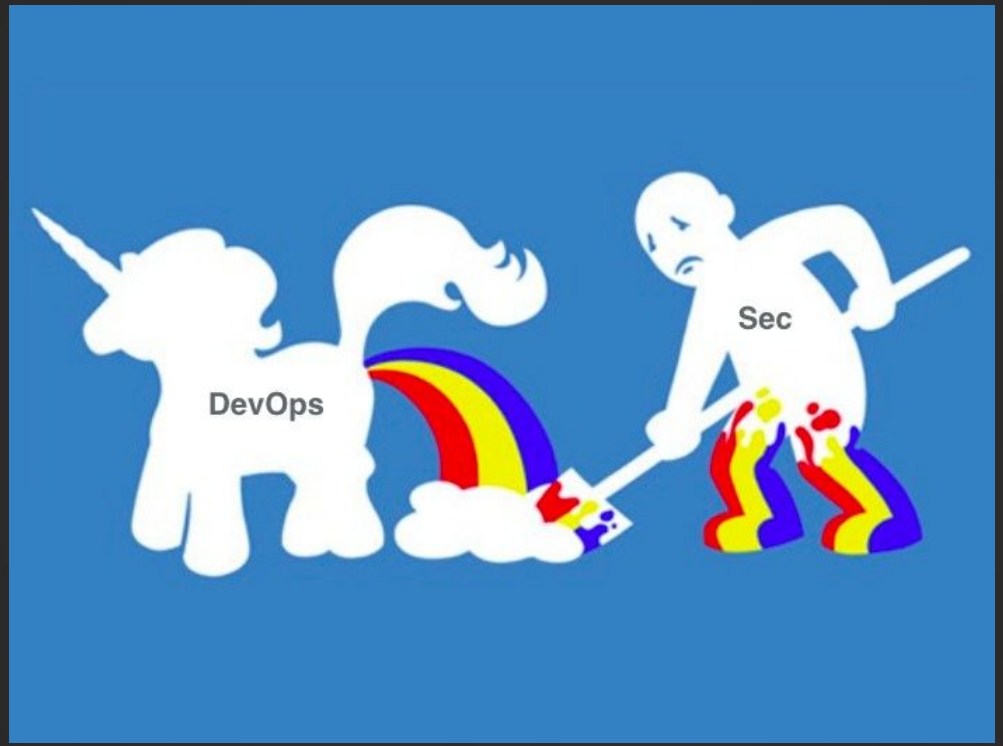
Por que automatizar a Segurança?



02

DevSecOps

Hum... Então você quer uma aplicação segura, mas não quer testar seu código...

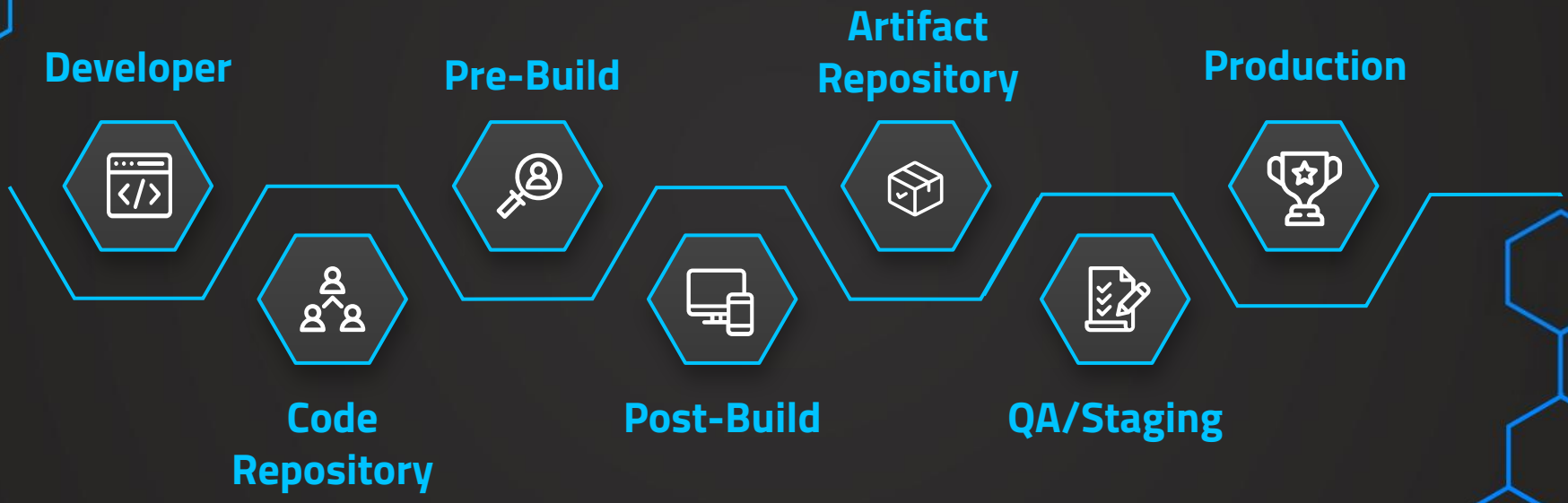

DevOps
Sec

Definição de DevSecOps

DevSecOps é uma abordagem de segurança da informação sobre os princípios do DevOps.

Seu principal objetivo é fortalecer os controles de segurança sem diminuir agilidade e qualidade na entrega de um produto

Fluxo DevSecOps



03

Hardening e Ansible

Ahh... Mas vou gastar 10h para automatizar uma tarefa de 10 minutos? Por quê? #chatiado

Hardening

Boas Práticas de Configuração

Hardening é o *endurecimento* das configurações para que seja possível deixar o sistema mais seguro e, dessa forma, mitigar a exploração de vulnerabilidades.

Todo Hardening tem que ser devidamente avaliado antes de ser implementado. Já que cada ambiente tem suas própria características.

- CIS - Center for Internet Security: https://www.cisecurity.org/
- DevSec Hardening Framework: https://dev-sec.io/
- NIST Cybersecurity: https://www.nist.gov/cyberframework

Ansible

Ferramenta focada em Automação

Arquitetura Push

Entendimento e Manutenção Simples

Não precisa de Agentes

Arquitetura em Python

Formato descritivo usando YAML

Demo!

Que Murphy não esteja vendo essa palestra.

Obrigado!

Perguntas?

yago.almeida@4linux.com.br
linkedin.com/in/yago-esquines/
github.com/yesquines
4linux.com.br

CREDITS: This presentation template was created by **Slidesgo**, including icon by **Flaticon**, and infographics & images from **Freepik**

- Manifesto DevSecOps: https://www.devsecops.org/
- Palestra DevSecOps - What and How de Anant Shrivastava (Black Hat USA 2019)
- RedHat Ansible: https://ansible.com