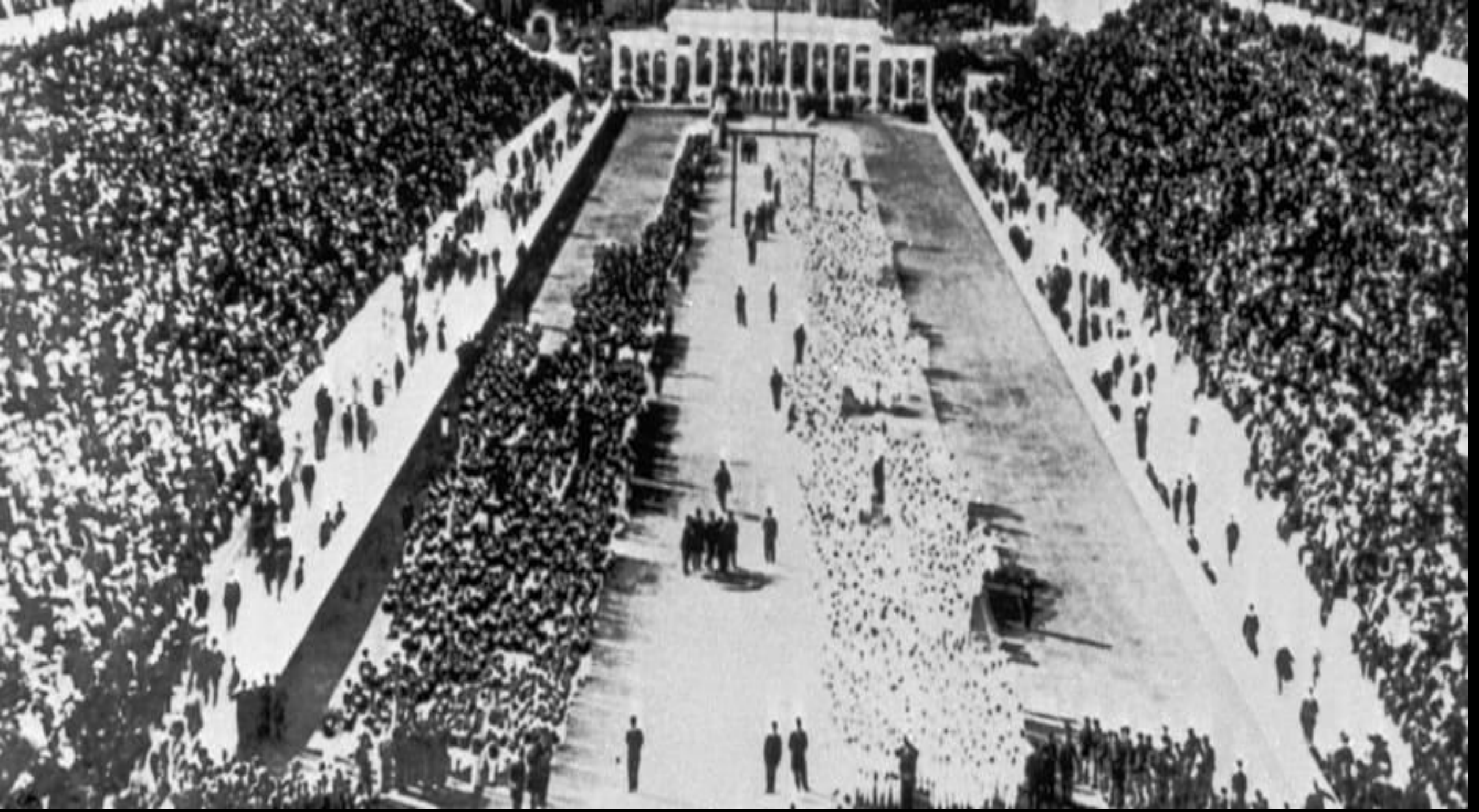

FORTINET
LINUXTIPS

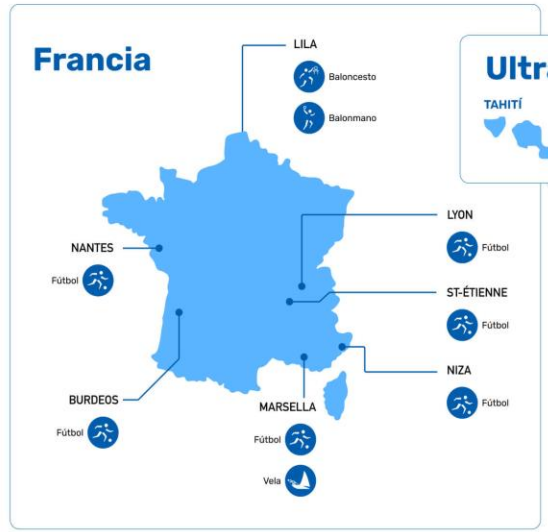
Sobrevoando Nuvens & Protegendo Aplicações

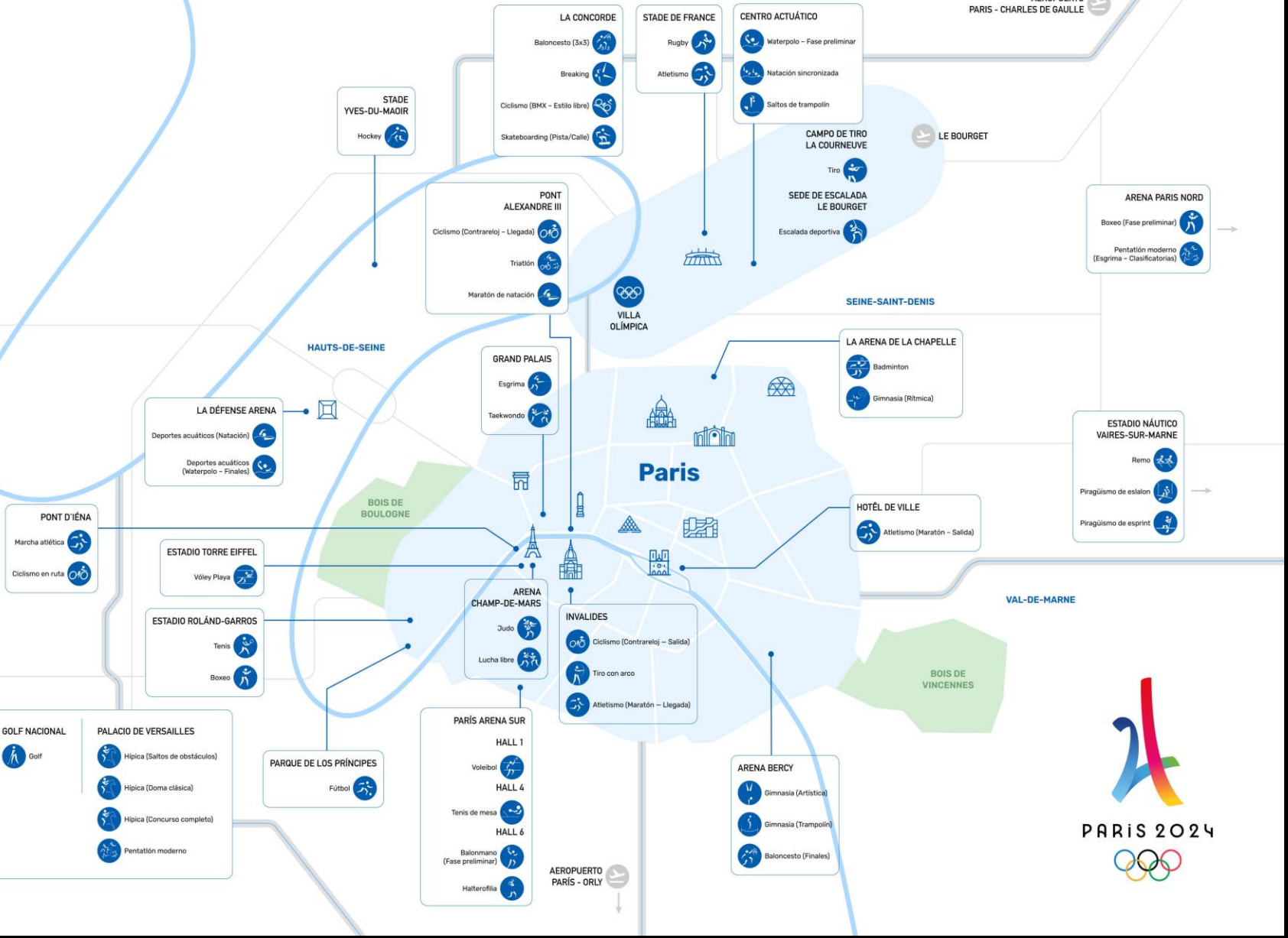

PARIS 2024

Instagram:
@marciodobeco



SEDES OLÍMPICAS MAPA



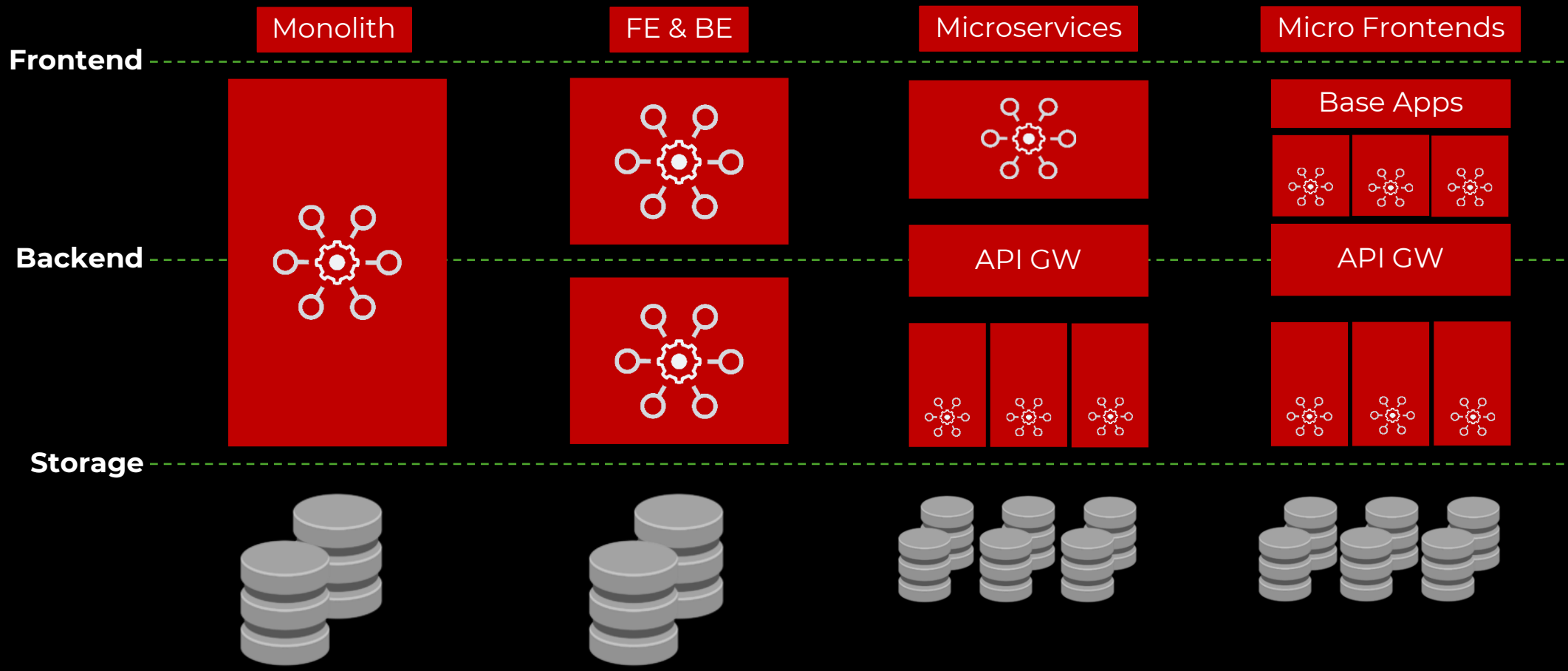


PARIS 2024


Rotary
Club de Guarulhos
GUARULHOS

Data Center

Evolução das Aplicações




CBG
Rio
loterias CAIXA
CBG

Linha do Tempo

1999 — Nasceu em 8 de maio

2003 — Aos 4 anos, começou na ginástica

2010 — Mudança para Curitiba aos 10 anos para treinar com a Seleção Brasileira

2011 — Mudança para o Rio de Janeiro para defender o Flamengo

2015 — Cirurgia no joelho direito após romper o ligamento cruzado anterior (LCA)

2016 — Estreia nos Jogos Olímpicos na edição do Rio de Janeiro

2019 — Cirurgia no joelho direito após romper o ligamento cruzado anterior (LCA)

2021 — Campeã mundial do Salto

Medalha de ouro no salto e prata no individual geral nos Jogos Olímpicos de Tóquio

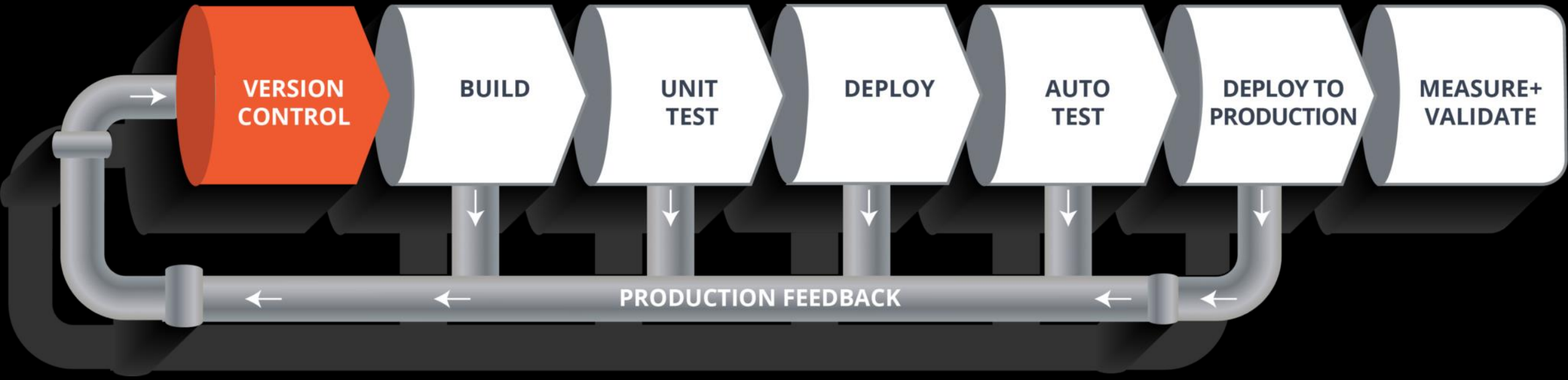
2022 — Campeã mundial do Individual Geral

2023 — Bicampeã mundial do Salto

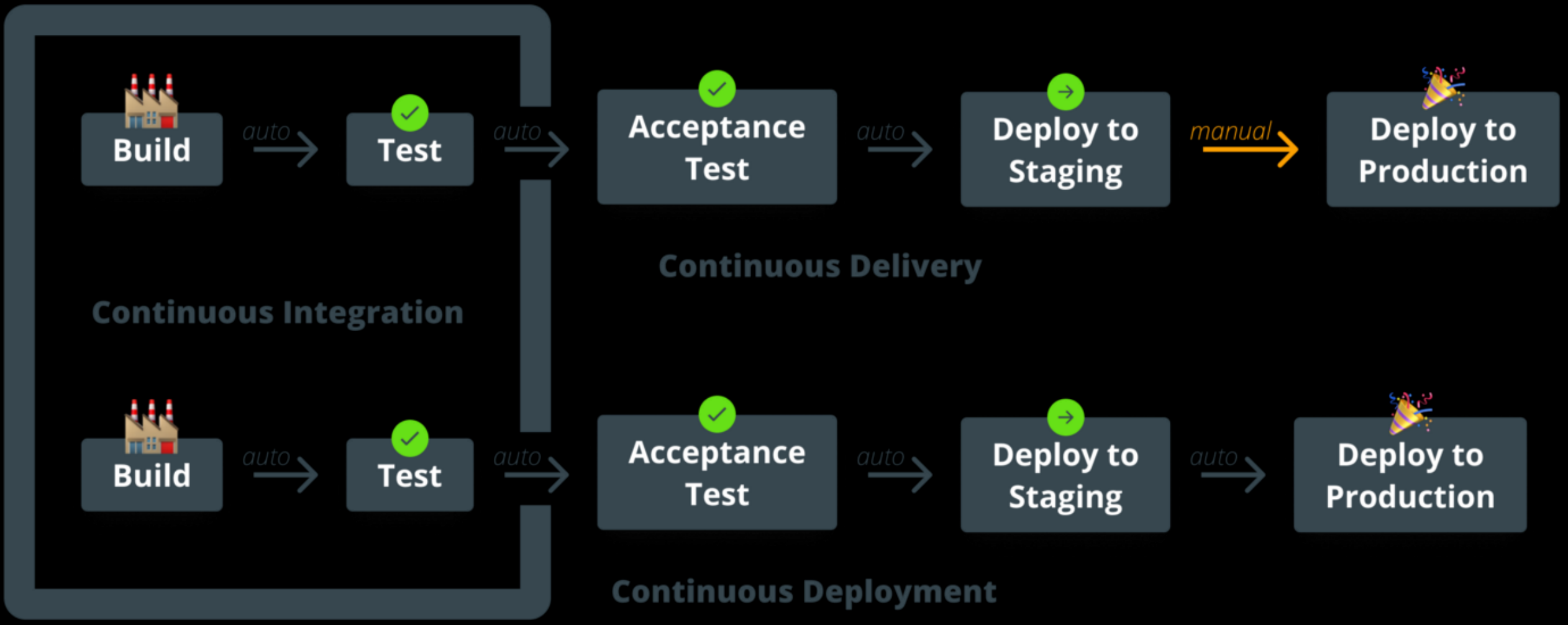
2024 — Carregando...

Rebeca Andrade

CI/CD Teoria


VERSION CONTROL
BUILD
UNIT TEST
DEPLOY
AUTO TEST
DEPLOY TO PRODUCTION
MEASURE+ VALIDATE
PRODUCTION FEEDBACK

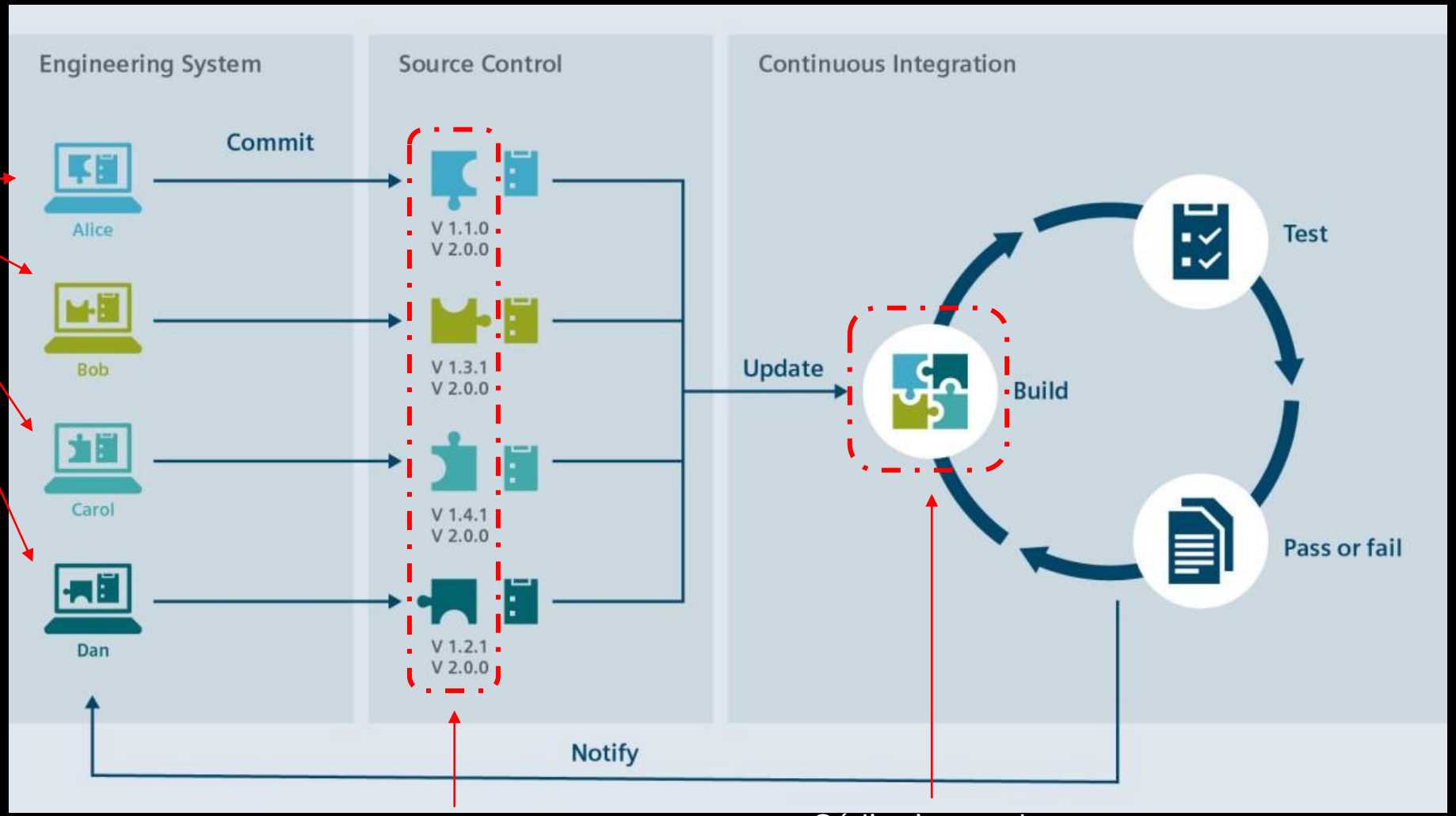
CI/CD Teoria


Build
auto
Test
auto
Acceptance Test
auto
Deploy to Staging
manual
Deploy to Production
Continuous Delivery
Continuous Integration
Build
auto
Test
auto
Acceptance Test
auto
Deploy to Staging
auto
Deploy to Production
Continuous Deployment


2
8
9
JAM
JAM
CAN
CAN

CI/CD Teoria – Integração Contínua

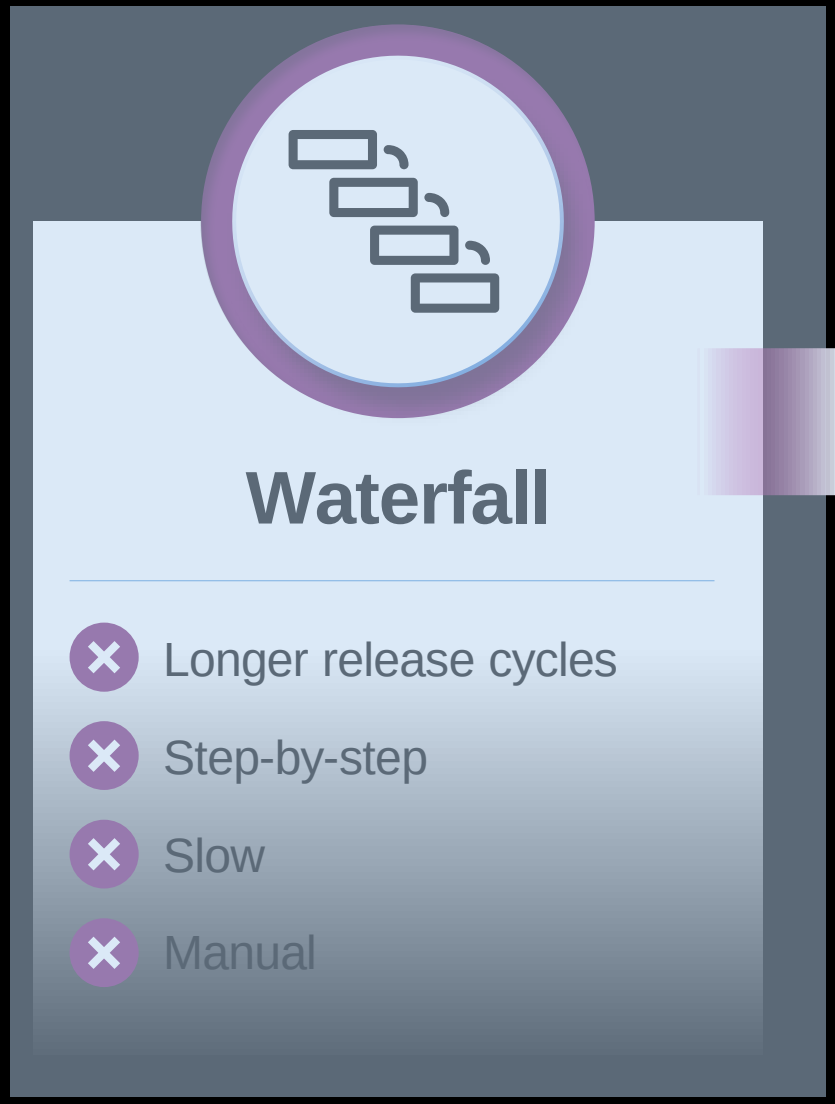
Vários desenvolvedores trabalhando simultaneamente

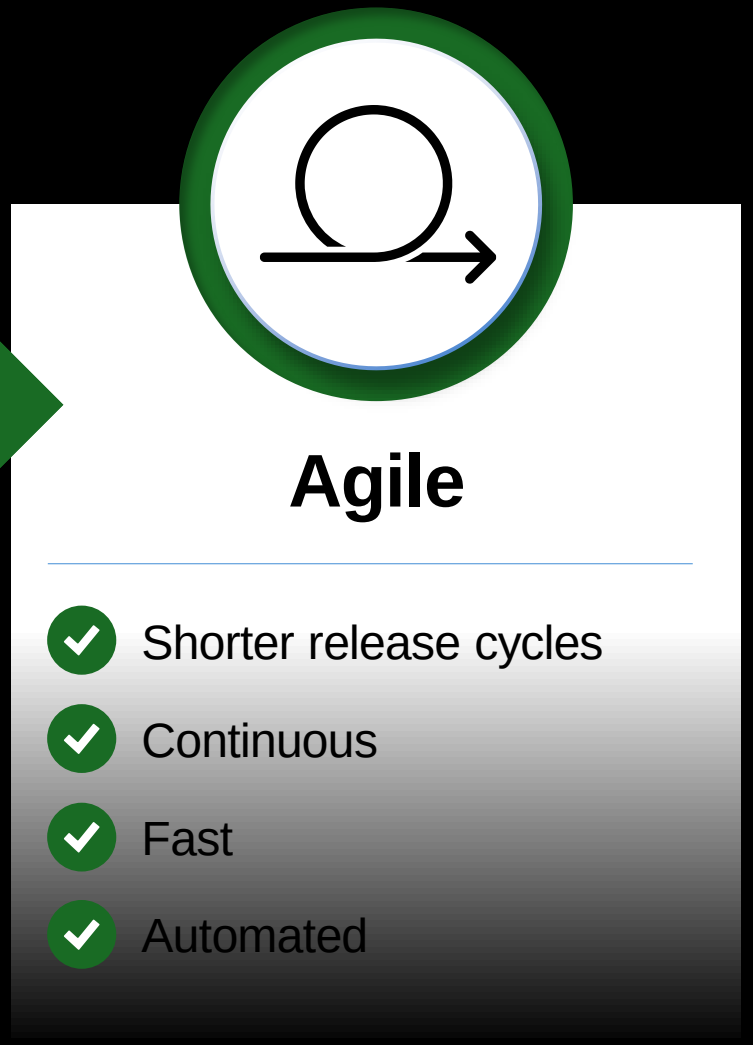


Pequenas partes de cód desenvolvidas por cada dev

Código integrado, criando a aplicação

Tendências no desenvolvimento de app modernos

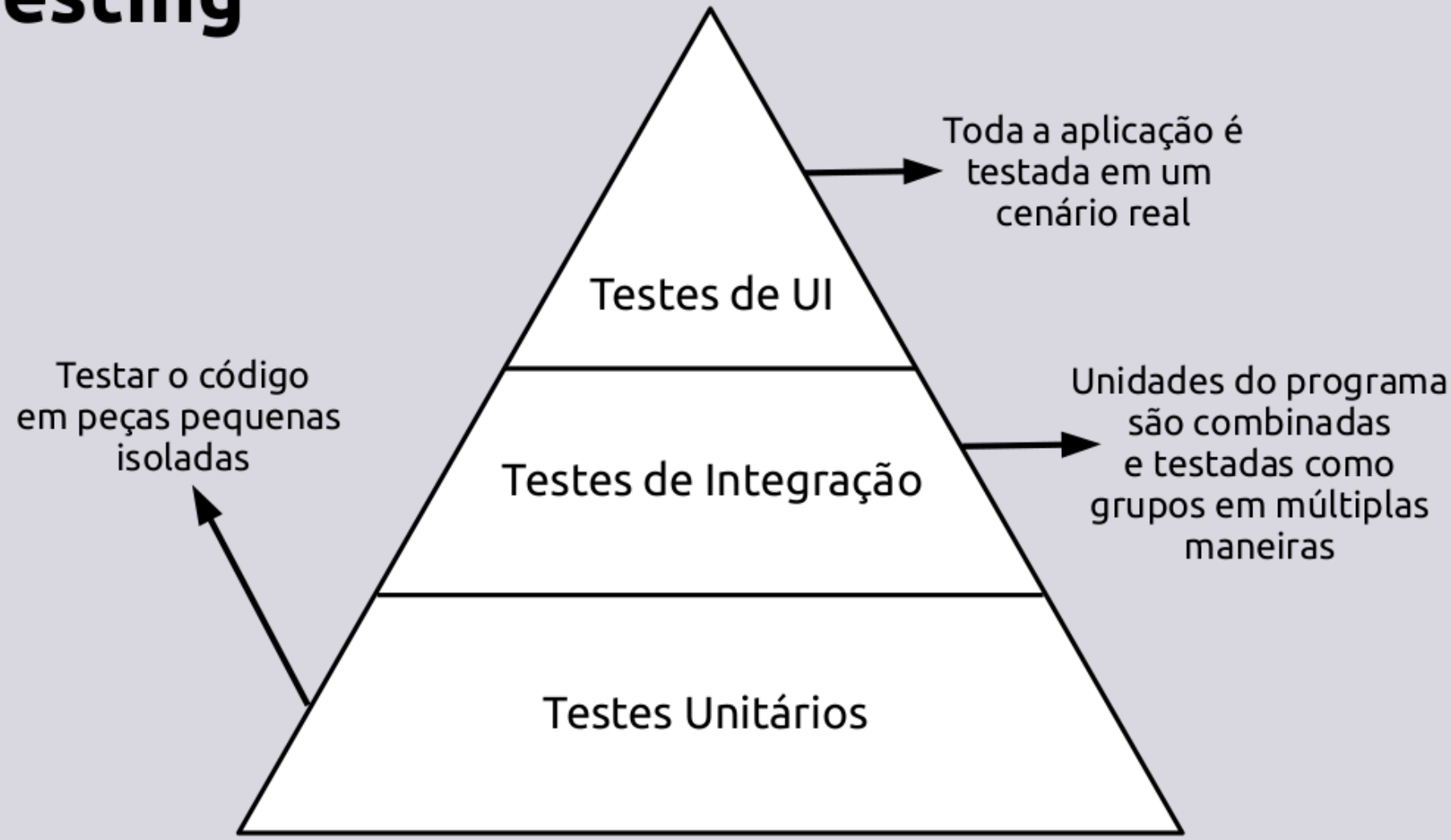


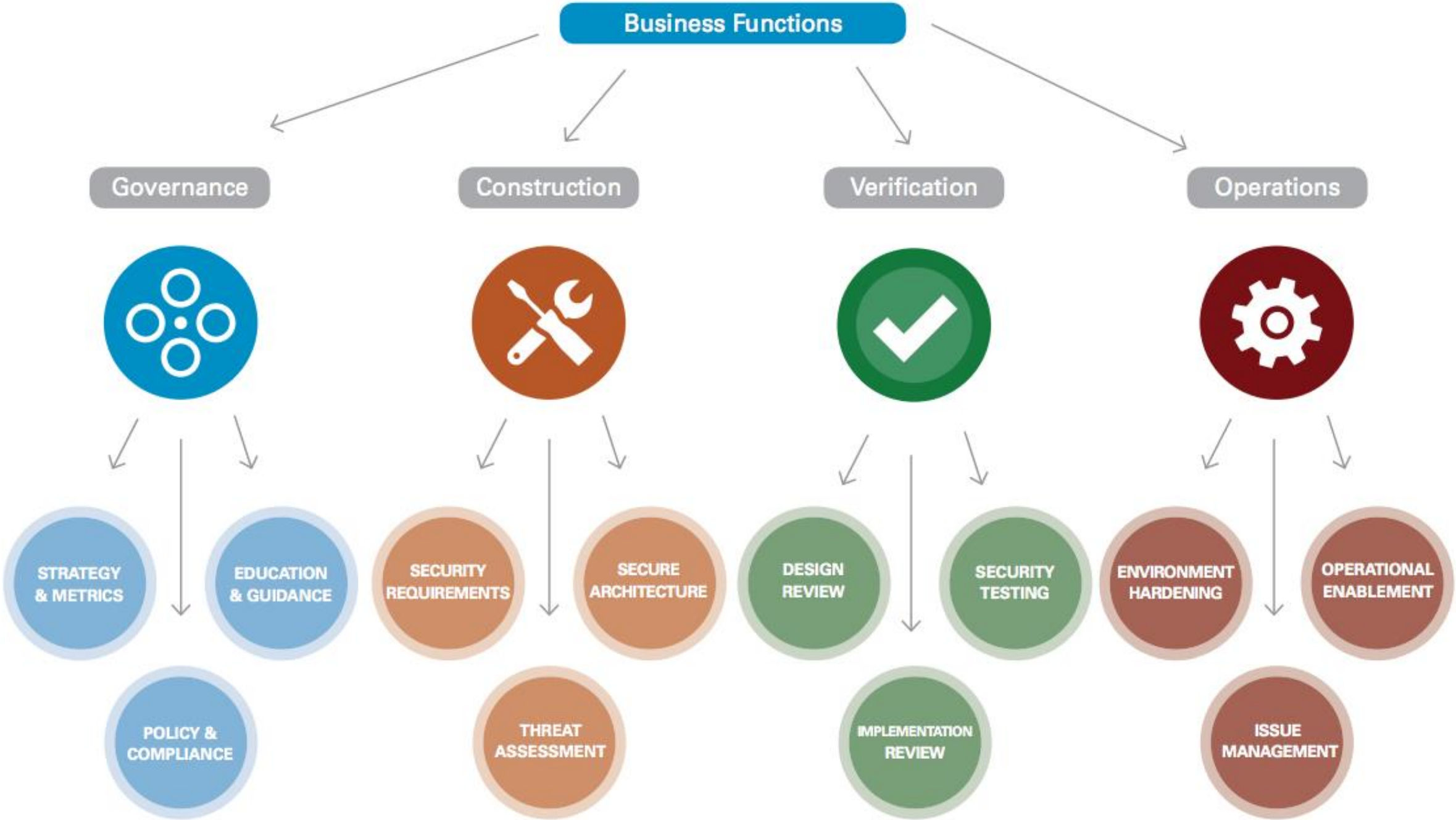


Agilidade não é fazer de qualquer jeito.

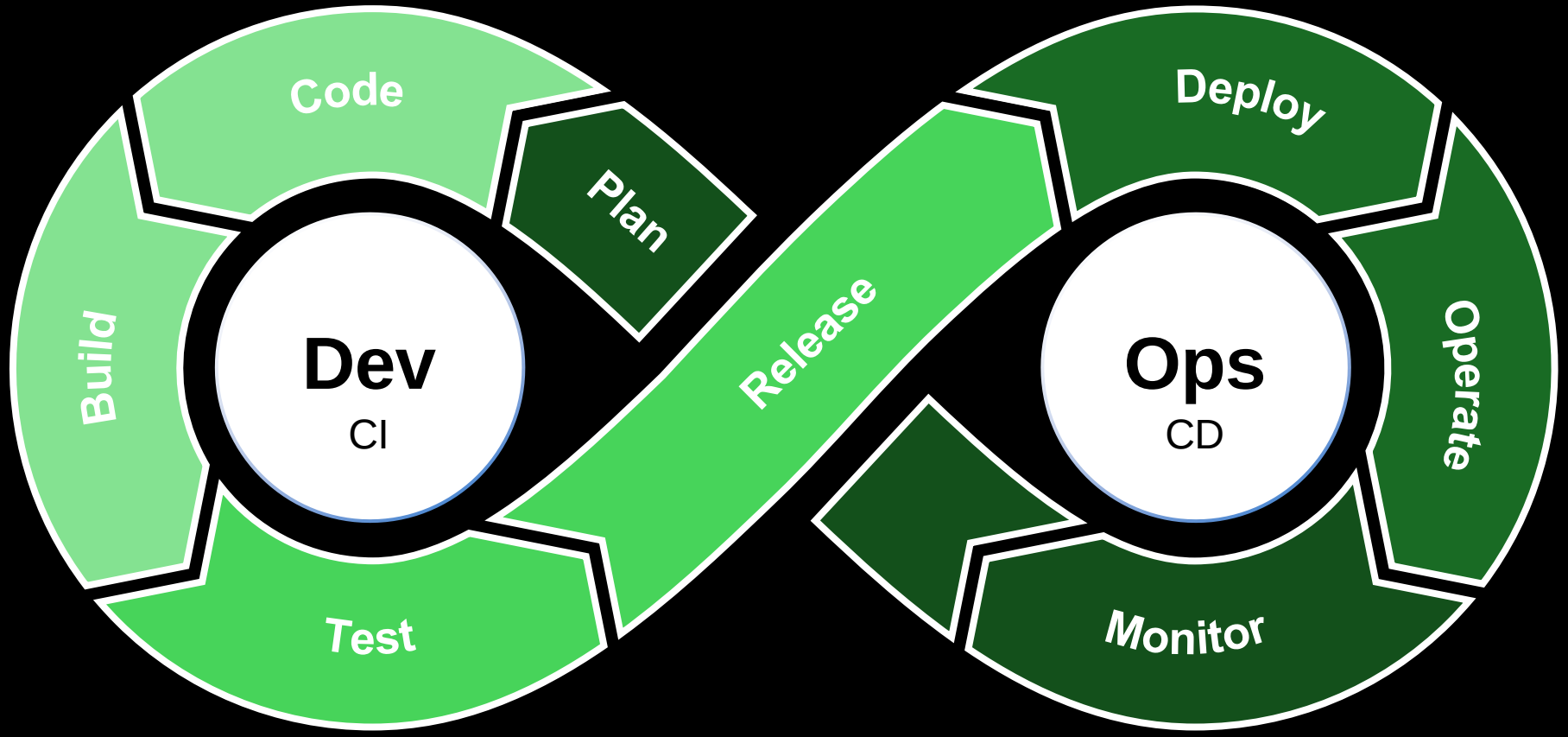

Developer
Tester

Testing

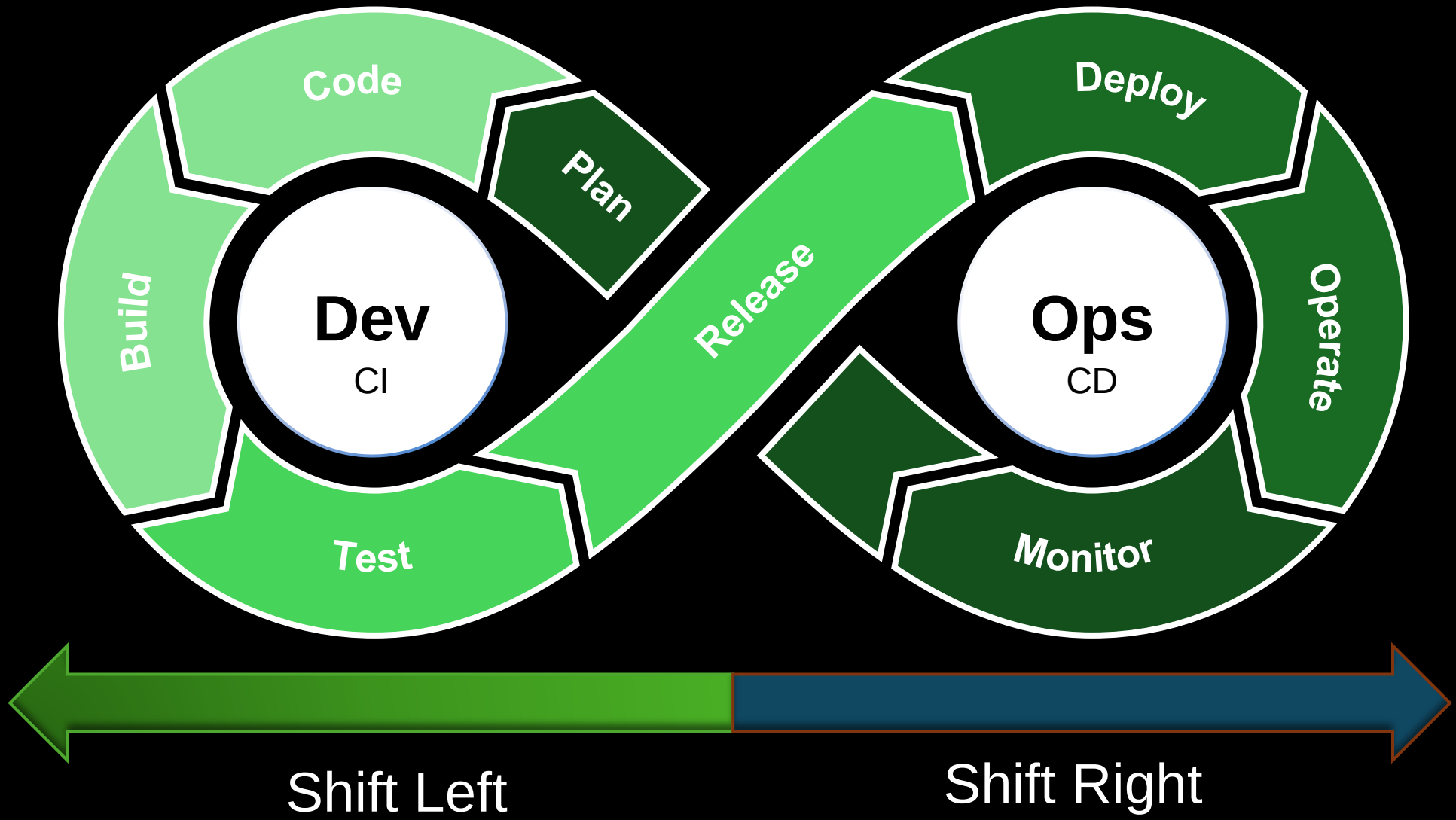

Toda a aplicação é testada em um cenário real
Testes de UI
Testar o código em peças pequenas isoladas
Testes de Integração
Unidades do programa são combinadas e testadas como grupos em múltiplas maneiras
Testes Unitários

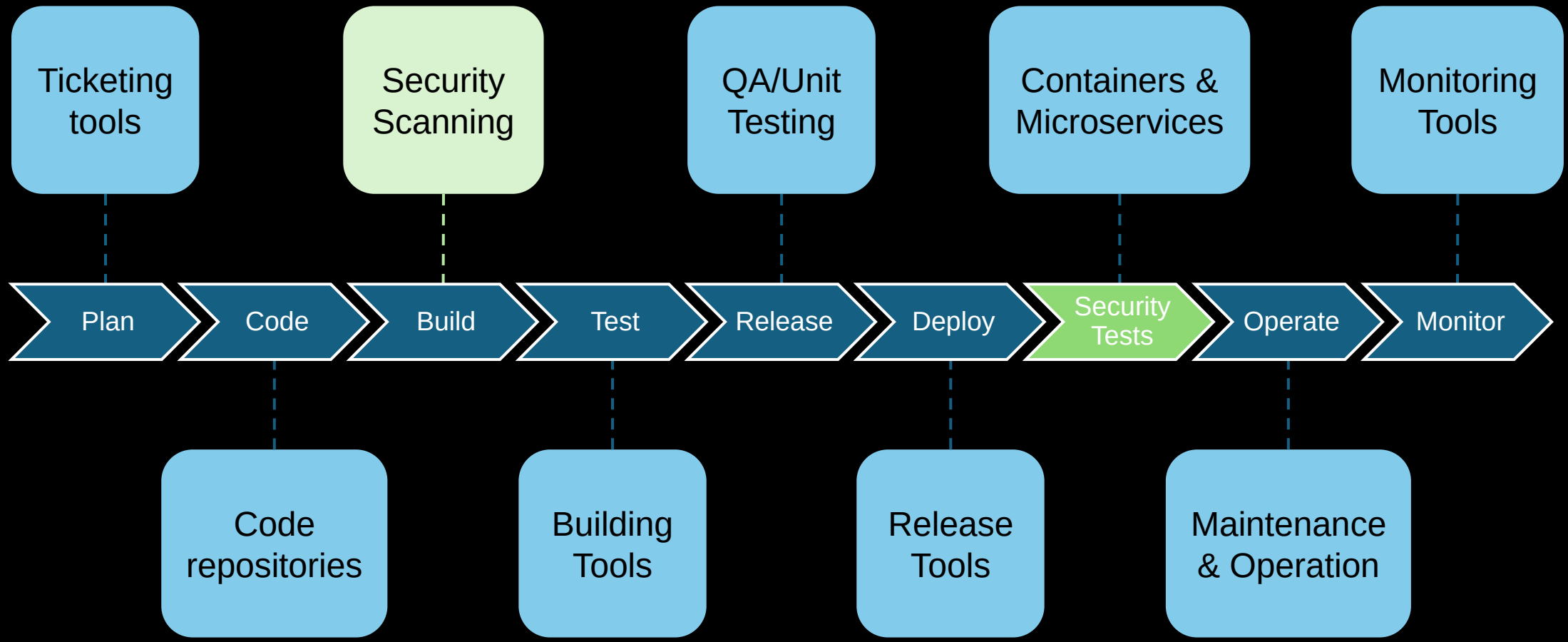

Business Functions
Governance
Construction
Verification
Operations
STRATEGY & METRICS
EDUCATION & GUIDANCE
POLICY & COMPLIANCE
SECURITY REQUIREMENTS
SECURE ARCHITECTURE
THREAT ASSESSMENT
DESIGN REVIEW
SECURITY TESTING
IMPLEMENTATION REVIEW
ENVIRONMENT HARDENING
OPERATIONAL ENABLEMENT
ISSUE MANAGEMENT

A Cultura Devops



DevSecOps: Shift Left & Shift Right




Ticketing tools
Security Scanning
QA/Unit Testing
Containers & Microservices
Monitoring Tools
Plan
Code
Build
Test
Release
Deploy
Security Tests
Operate
Monitor
Code repositories
Building Tools
Release Tools
Maintenance & Operation


Staff
PARIS 2024
CLEMENT BOSSE
ATHLÉTISME FRANCE
A3


Staff
PARIS 2024
PIERRE ALLEMAND
ATHLÉTISME FRANCE
A4


Staff
PARIS 2024
JEAN GAGNE
ATHLÉTISME FRANCE


Guardrails

Três personagens e seus problemas

DevOps

- Múltiplas integrações e configurações complexas

Security

- Muitos tipos de scans
- High Touch
- Não é escalável.

Dev

- Muitos problemas e entregas
- Falsos positivos

Falta experiência em segurança de aplicativos

DevSecOps é realmente importante

Toyota customer data exposed as dev published key on GitHub

Updated on: 11 October 2022

Vilius Petkauskas, Senior Journalist

Image by Shutterstock.

Toyota confirmed that data of almost 300,000 of its customers leaked online after the company's developer published the source code of the user site on GitHub five years ago.

The world's largest car manufacturer, Toyota, apologized for leaking the details of 296,019 of its customers since 2017. The leaked data included email addresses and customer management numbers Toyota assigns to each client.

CPO MAGAZINE

HOME NEWS INSIGHTS RESOURCES

CYBER SECURITY NEWS · 4 MIN READ

Lapsus$ Hackers Published 70GB of Source Code Stolen in the Globant Data Breach

ALICIA HOPE · APRIL 7, 2022

Globant confirmed a data breach after Lapsus$ hackers claimed to have stolen 70GB of source code from the company. In the United States Securities and Exchange Commission (SEC) filing, the company said it detected authorized access to a "limited section" of its code repository for a "very limited number of clients."

- Advertisement -

Screenshots shared by the Lapsus$ hacking group suggested that the leaked customer source code belonged to companies like Apple and Facebook, DHL, Fortune, CSpan, and

Visibilidade

Veja os problemas agregados em vários tipos de verificação.

SAST

Static / source code scanning

Verifica problemas de segurança no codigo fonte de maneira estática.

SCA/OSS

SCA/OSS scanning

Verifica problemas em bibliotecas de terceiros e de código aberto, por exemplo. log4j

Secrets

Static / source code scanning

Verifica problemas de credenciais contidas no cod fonte

DAST

Dynamic scanning

Simula explorações usando o URL de front-end do aplicativo, usando FortiDAST

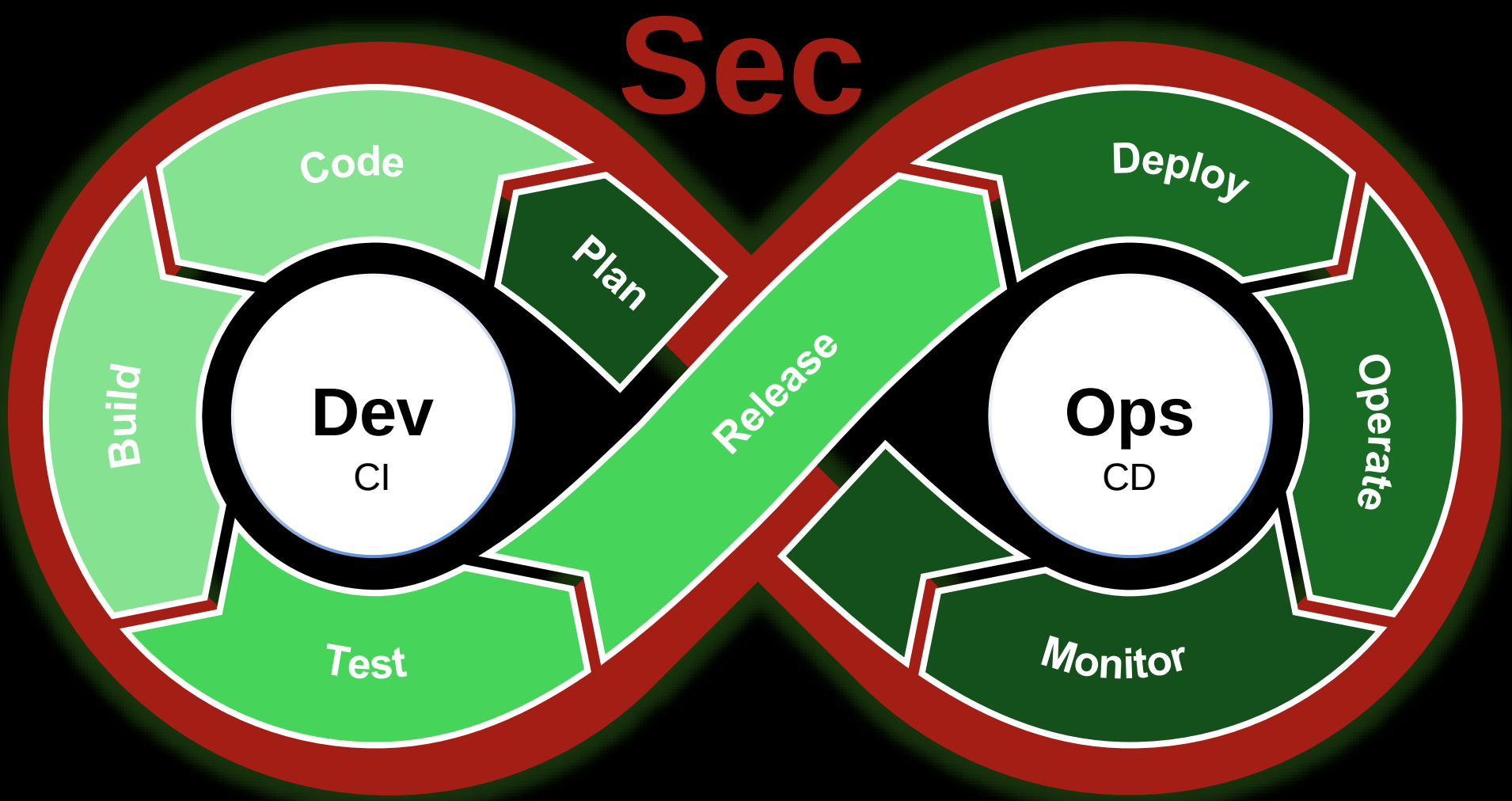
IaC (Infrastructure-as-Script scanning)

Scanning IaC scripts, terraform, etc.

Containers

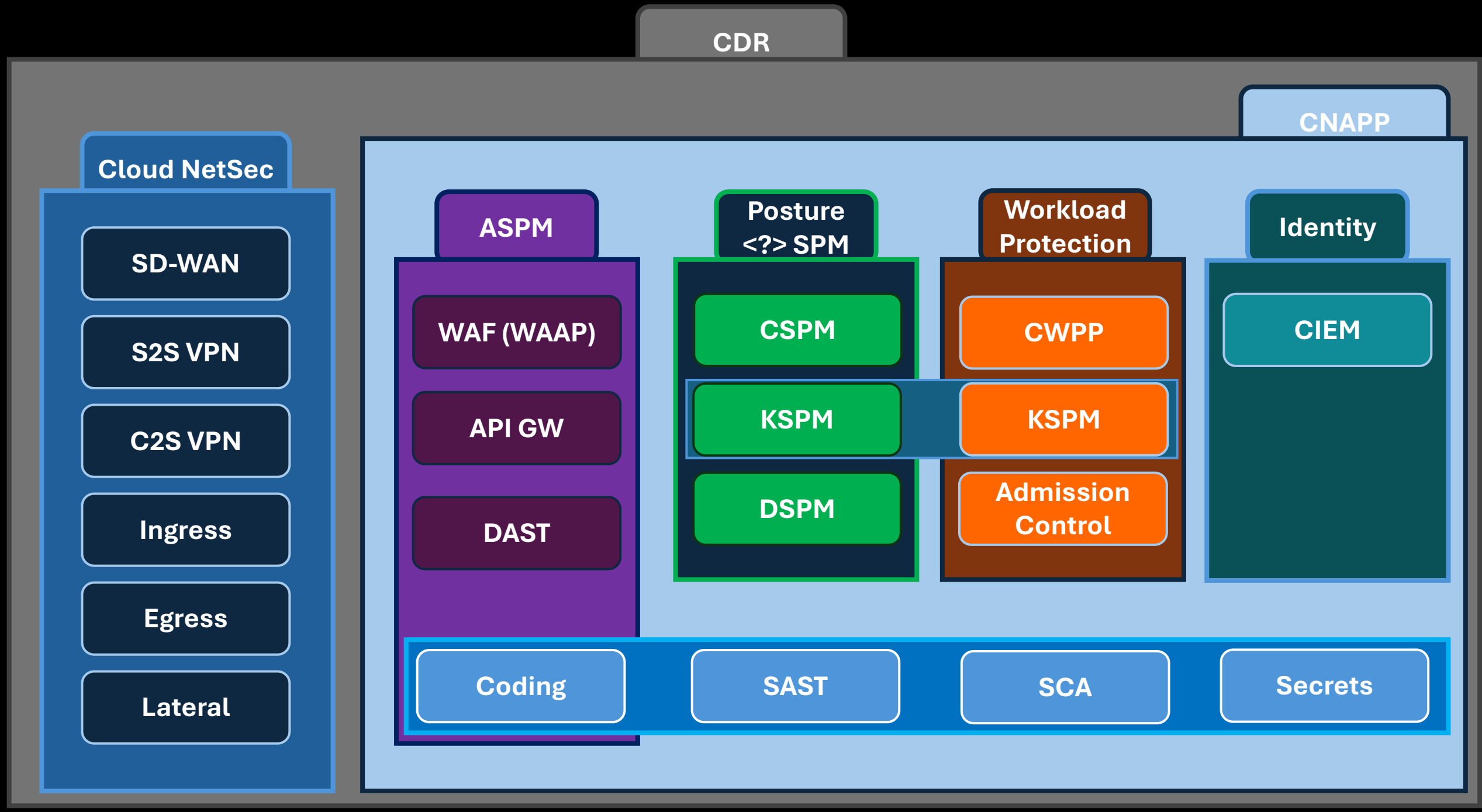
Scanning **Containers** criados no pipeline.

Protegendo o DevOps




4GIFs.com


DOPING
TEST


CDR
CNAPP
Cloud NetSec
SD-WAN
S2S VPN
C2S VPN
Ingress
Egress
Lateral
ASPM
WAF (WAAP)
API GW
DAST
Posture
<?> SPM
CSPM
KSPM
DSPM
Workload
Protection
CWPP
KSPM
Admission
Control
Identity
CIEM
Coding
SAST
SCA
Secrets

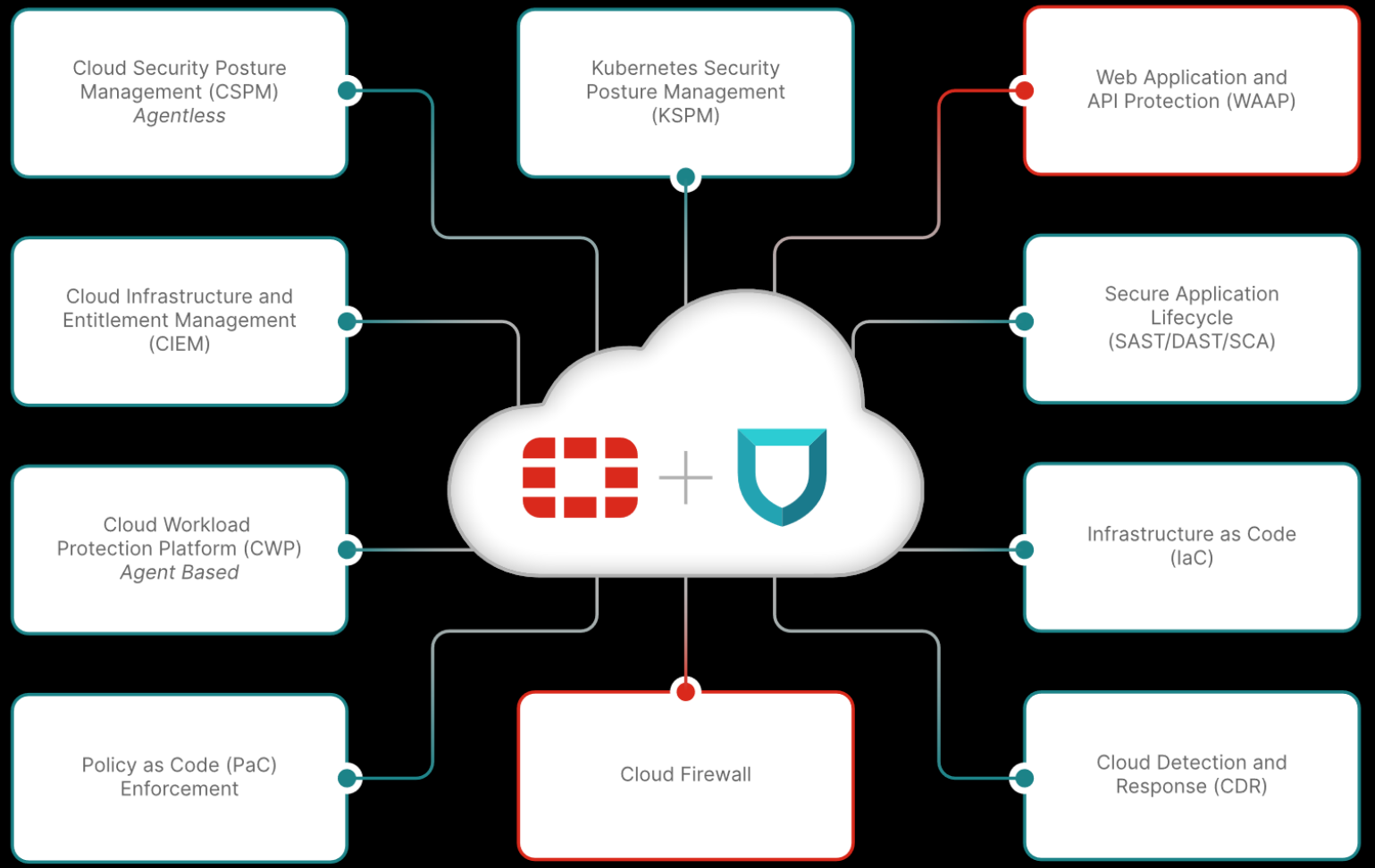
Fortinet + Lacework FortiCNAPP

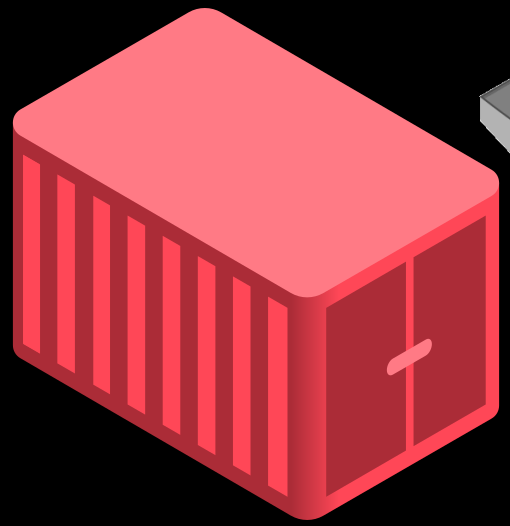
The Most Complete AI-driven Cloud-Native Application Protection Platform

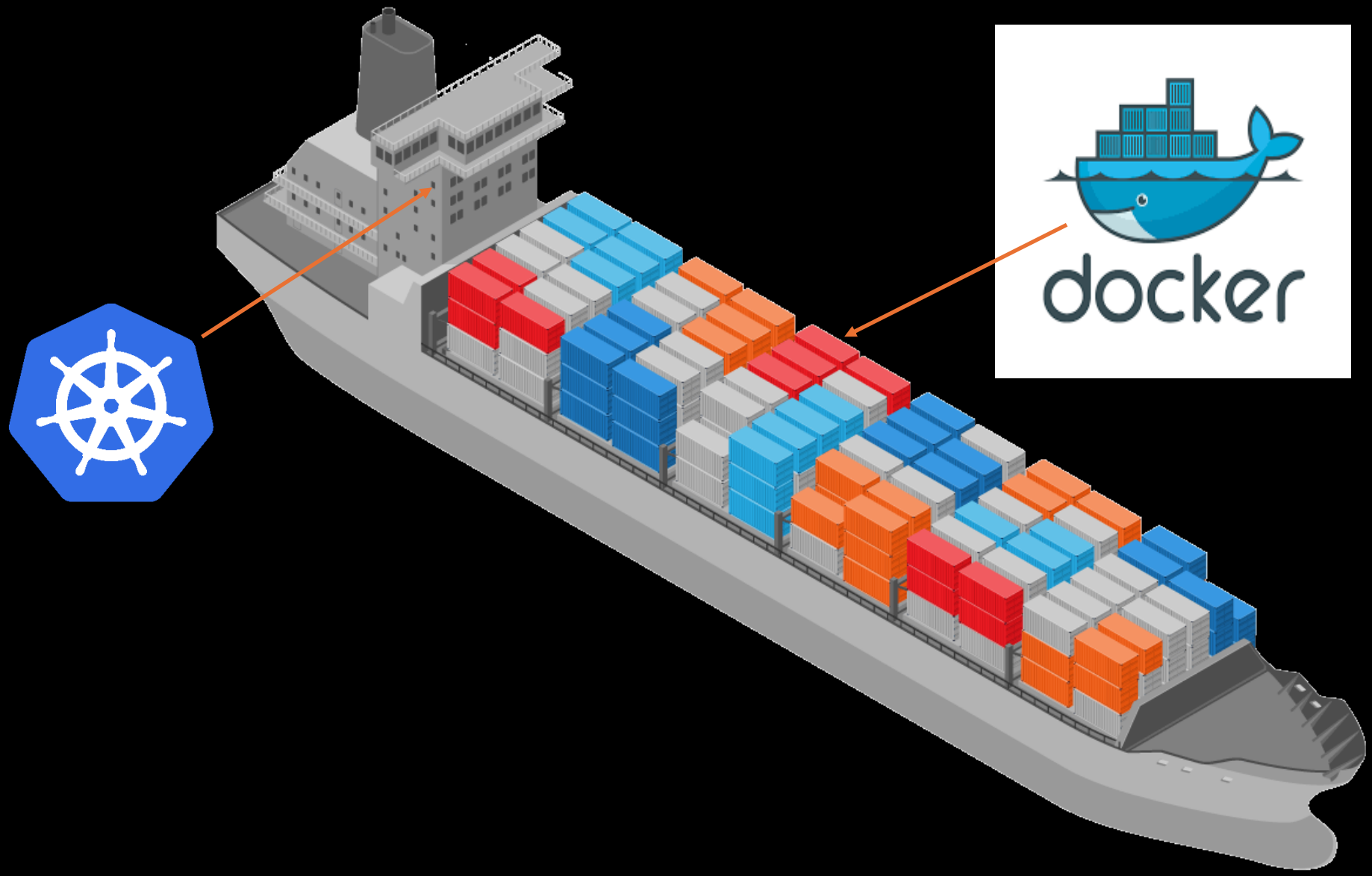
Single vendor for all cloud security and secure CI/CD application development needs

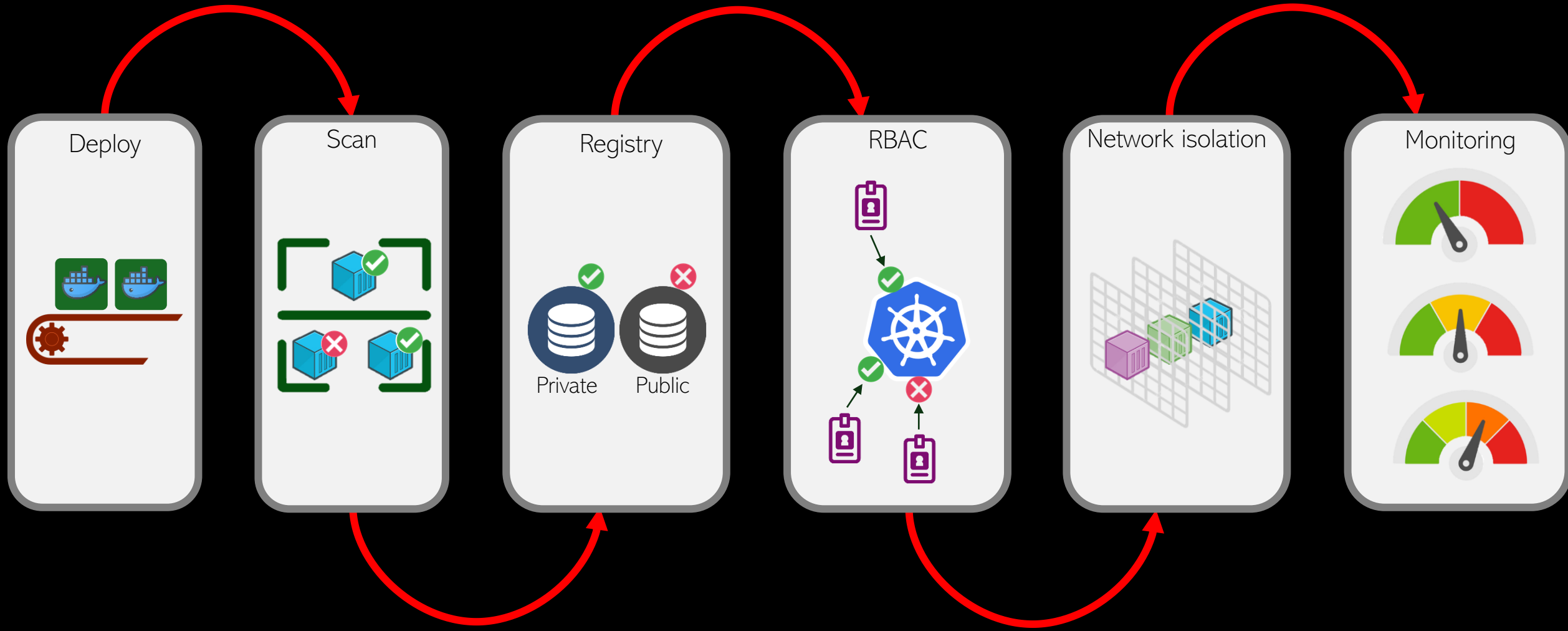
See <u>AND</u> protect everything from coding, deploying, and running applications across hybrid and multi-clouds

Simplify security with AI-driven platforms from both Lacework FortiCNAPP and Fortinet






docker


Deploy
Scan
Registry
Private
Public
RBAC
Network isolation
Monitoring

BLOG

Hardening Docker containers, images, and host - security toolkit

August 10, 2017 | by Yathi Naik

Introductio

Container technol
and deployed. Not
new features or co
great for DevOps,
and developers mu
experts has built s
several years. This
containers and hos
environment. You
should be following.

Securing Docker

An objective, consensus-driven security guideline for the Docker Server Software.

A step-by-step checklist to secure Docker:

DOWNLOAD LATEST CIS BENCHMARK →
FREE TO EVERYONE

For Docker (CIS Docker Benchmark version 1.3.1)

CIS has worked with the community since 2015 to publish a benchmark for Docker.


4GIFs.com

Containers: um constante alvo de ataques

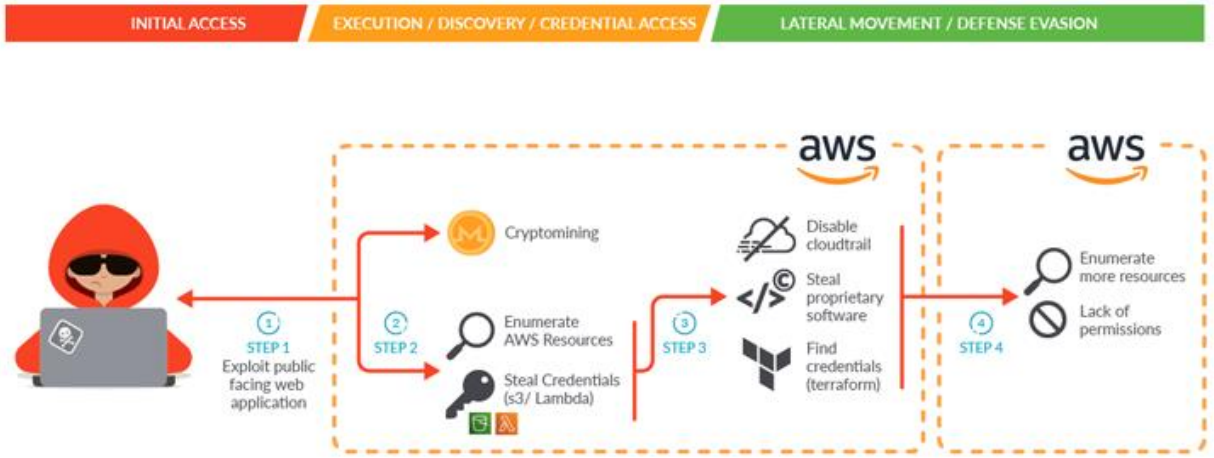
Remote Workforce | 5 MIN READ | ARTICLE

Cloud security, Architecture

Hackers Exploit Containerized Environments to Steal Proprietary Data and Software

Mar 02, 2023 Ravie Lakshmanan

Container Security / Cyber Threat



A sophisticated attack campaign dubbed **SCARLETEEL** is targeting containerized environments to perpetrate theft of proprietary data and software.

Source: Orange Deer studio via Shutterstock

Todos os verões, turistas de todo o mundo enchem as ruas de Paris para descobrir a arte de viver francesa, a Torre Eiffel e o Museu do Louvre. Mas, em **2024**, juntar-se-ão a eles os viajantes que vieram especialmente para os Jogos Olímpicos de Paris, que decorrem de 26 de julho a 11 de agosto, e os **Jogos Paralímpicos**, de 28 de agosto a 8 de setembro.

Uma vaga suplementar de turistas que se junta aos habitantes da Ilha de França que ficarão no local, por motivo de férias ou de teletrabalho, e aos franceses que querem viver a competição do século na capital! São esperados nada menos que **15,3 milhões de visitantes** na capital por ocasião dos Jogos **Olímpicos** e **Paraolímpicos de Paris**!

Um número que pode ser assustador, tendo em conta que a população da região parisiense é já de 12,4 milhões de habitantes. Mas a cidade de Paris afirma estar *"tranquila*" e **capaz** de acolher todas essas pessoas, uma vez que a capital já é *"a cidade mais turística do mundo"*. Pierre Rabadan, vice-prefeito de Paris, disse à *France Bleu* que, de acordo com as estimativas, o afluxo será de apenas *"um ou dois milhões a mais do que o habitual*'.

Olimpíadas-França rejeitou muitos pedidos de credenciamento para os Jogos de Paris por medo de segurança, diz ministro

Por KAROLOS GROHMANN

OLIMPÍADAS™

França recusa credenciar voluntários russos para as Olimpíadas

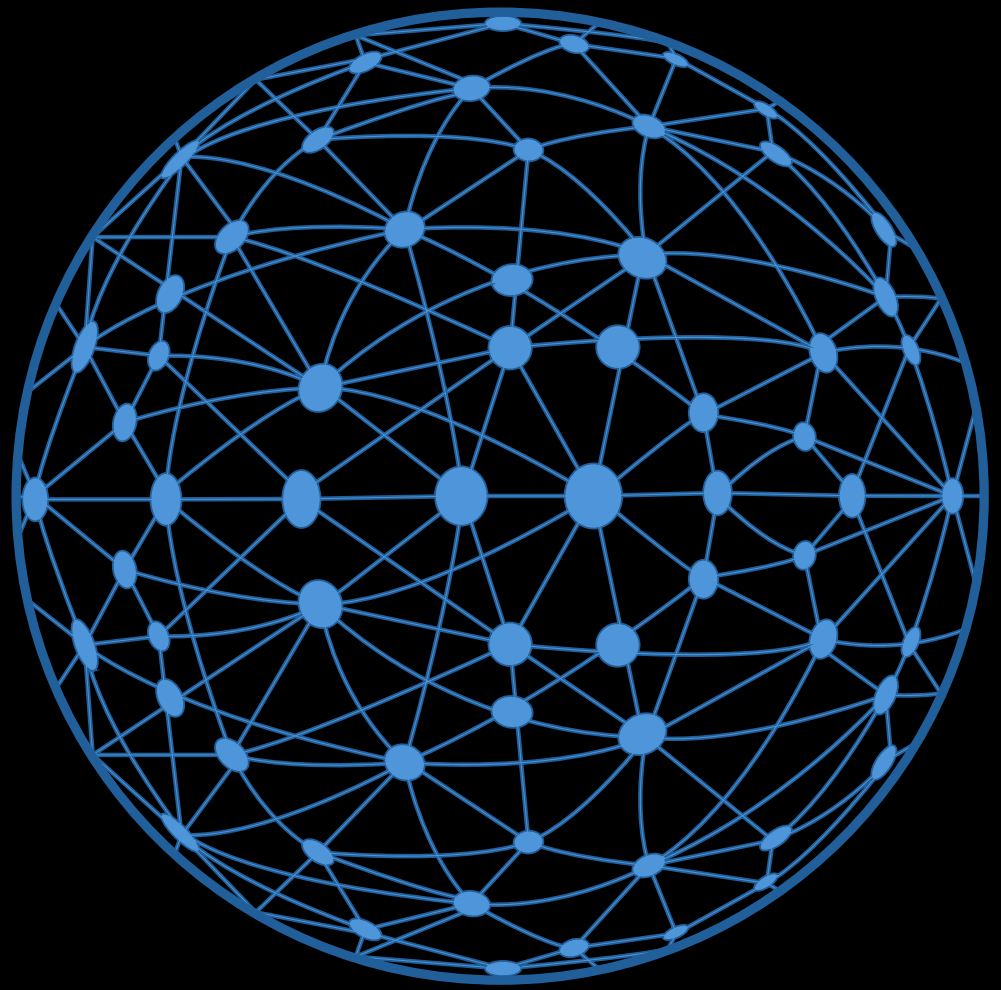
Mais de 20 cidad
francesas

PARIS (Reuters) - Os serviços
de credenciamento para as O
espionagem e ataques ciberne
domingo.

Paris contará com 45.000 agentes de segurança para garantir a segurança dos Jogos e sua cerimônia de abertura única ao longo do rio Sena, onde os atletas flutuarão em barcaças, passando por centenas de milhares de espectadores.

Os organizadores reduziram o número inicial de espectadores de 600.000 para cerca de 300.000.

Superfície de Ataque Expandida com WebApps



Explorações

incluindo OWASP Top 10

Ameaças Avançadas

incluindo ataques de dia zero

Ataques de bots

incluindo preenchimento de credenciais, extração de conteúdo

Ataques de API

incluindo ataques que extraem dados em massa

APIs e Aplicações Web expostas

The Ub
Vulner

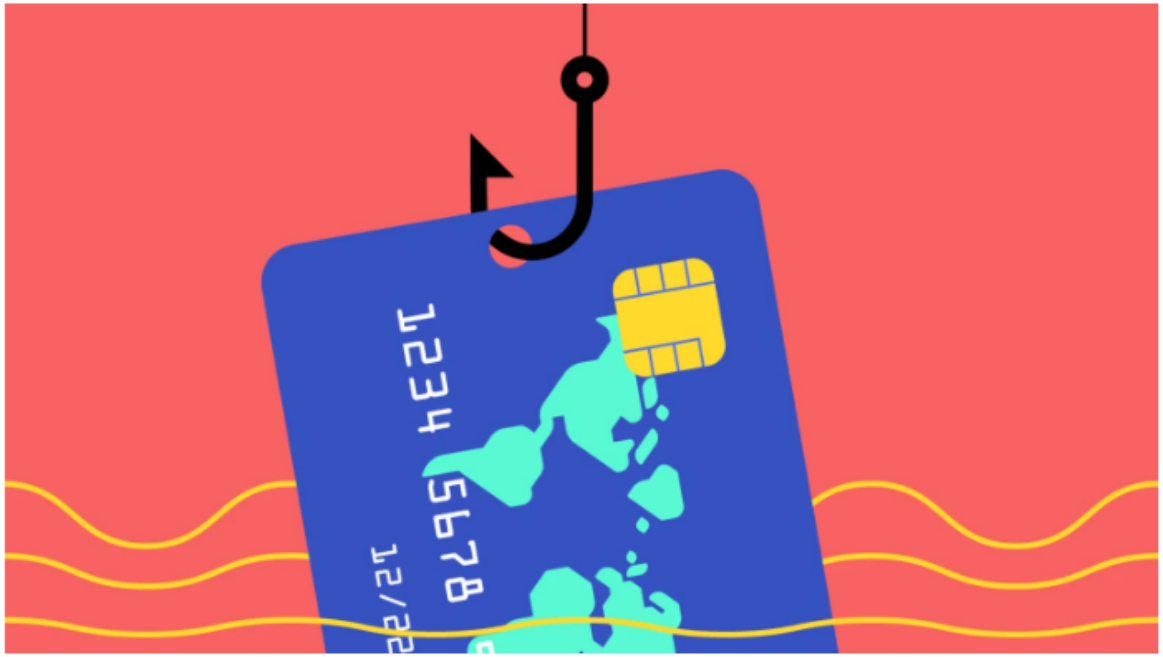
Inon Shkedy

What Ha

In September
allows mercha
services to cu
programming
valuable data,
records and a
authenticatio
takeover.

Hackers Inject Shell Scripts into eCommerce Sites to Steal Credit Card Data

By **Guru** - June 6, 2023 0



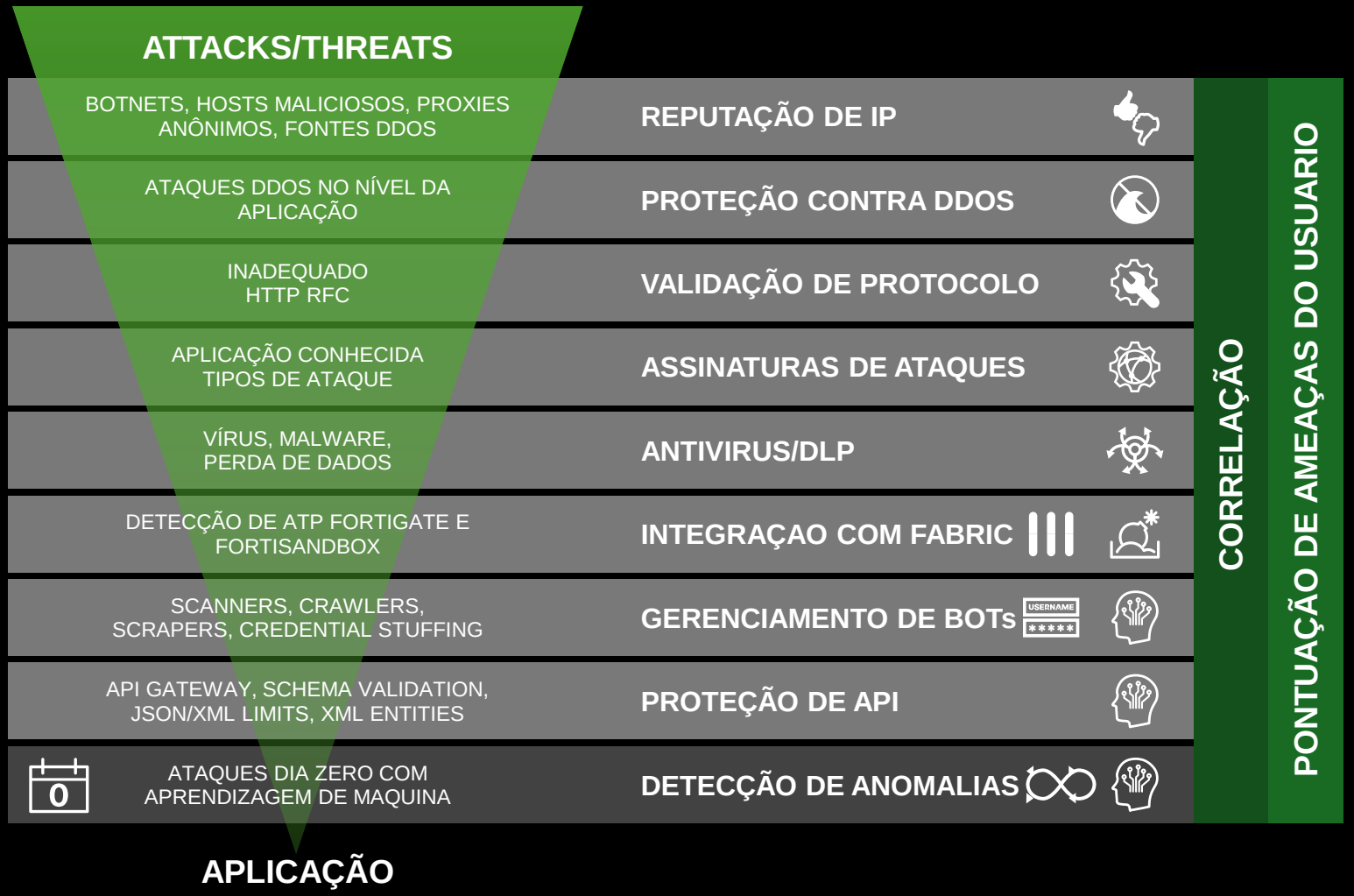
A recently discovered credit card theft operation, Magecart, has adopted an innovative approach by utilizing authentic websites as makeshift C2 servers.

This strategy enables them to illicitly implant and conceal skimming malware within specific eCommerce websites.

Tim Keary
@tim_keary

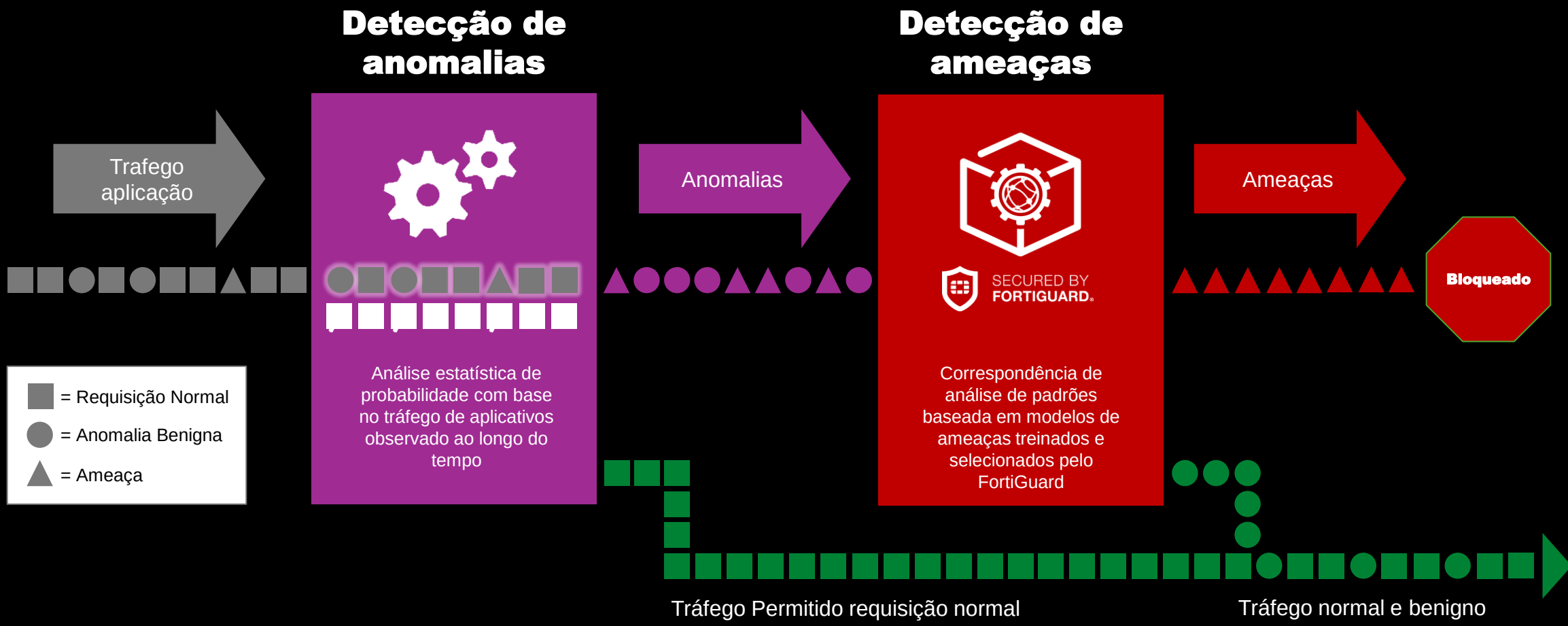
November 28, 2022 12:15 PM

Machine Learning para detecção de anomalias



A detecção de anomalias baseada em aprendizado de máquina aprende como seus usuários interagem com seu aplicativo, proporcionando detecção aprimorada de ameaças e reduzindo os falsos positivos que geram sobrecarga administrativa

FortiWeb funciona em uma inspeção de 2 camadas

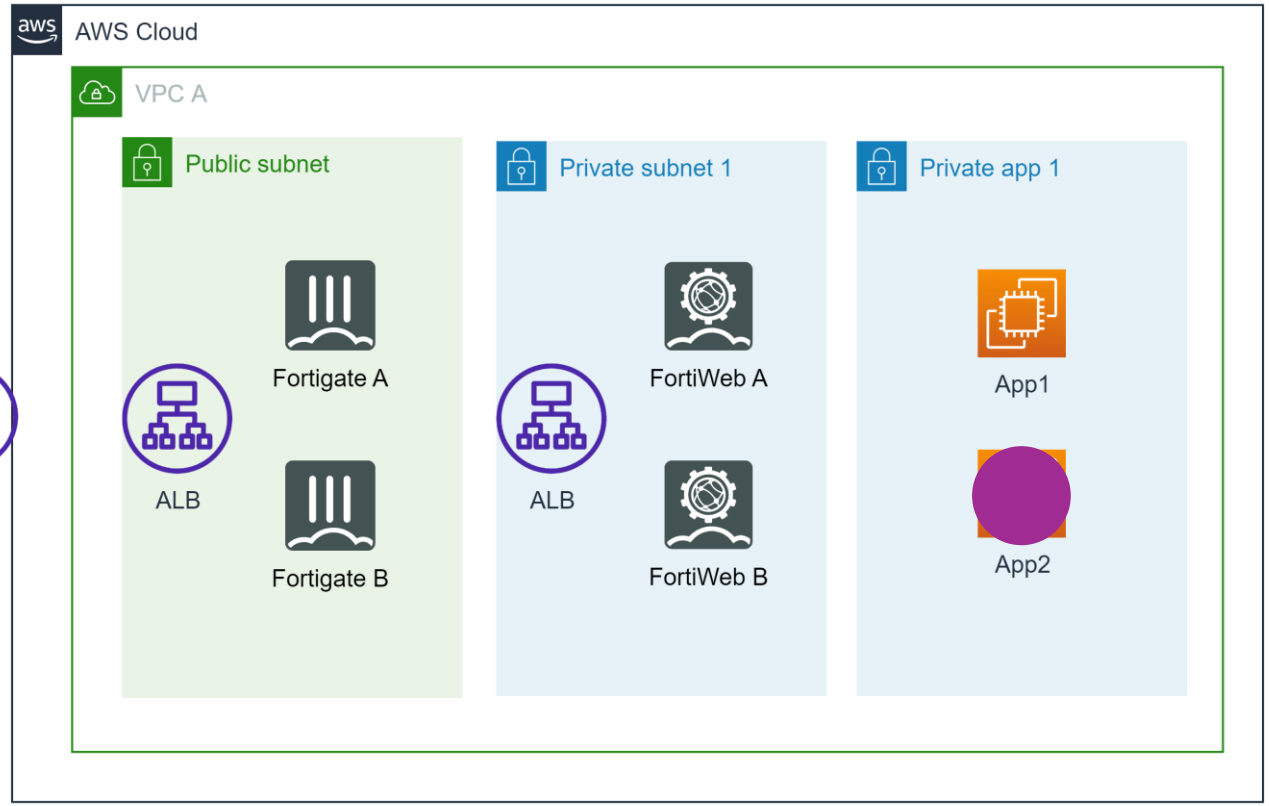


Reduza os problemas ao implantar aplicações web!

FortiWeb & FortiGate

Serie

1. Tráfego chega ao FortiGate antes de ir ao FortiWeb
2. Todo o tráfego de entrada destinados à aplicação são inspecionados em 2 etapas
3. NAT (duplo) antes de chegar à aplicação



Internet user accessing a web application/API

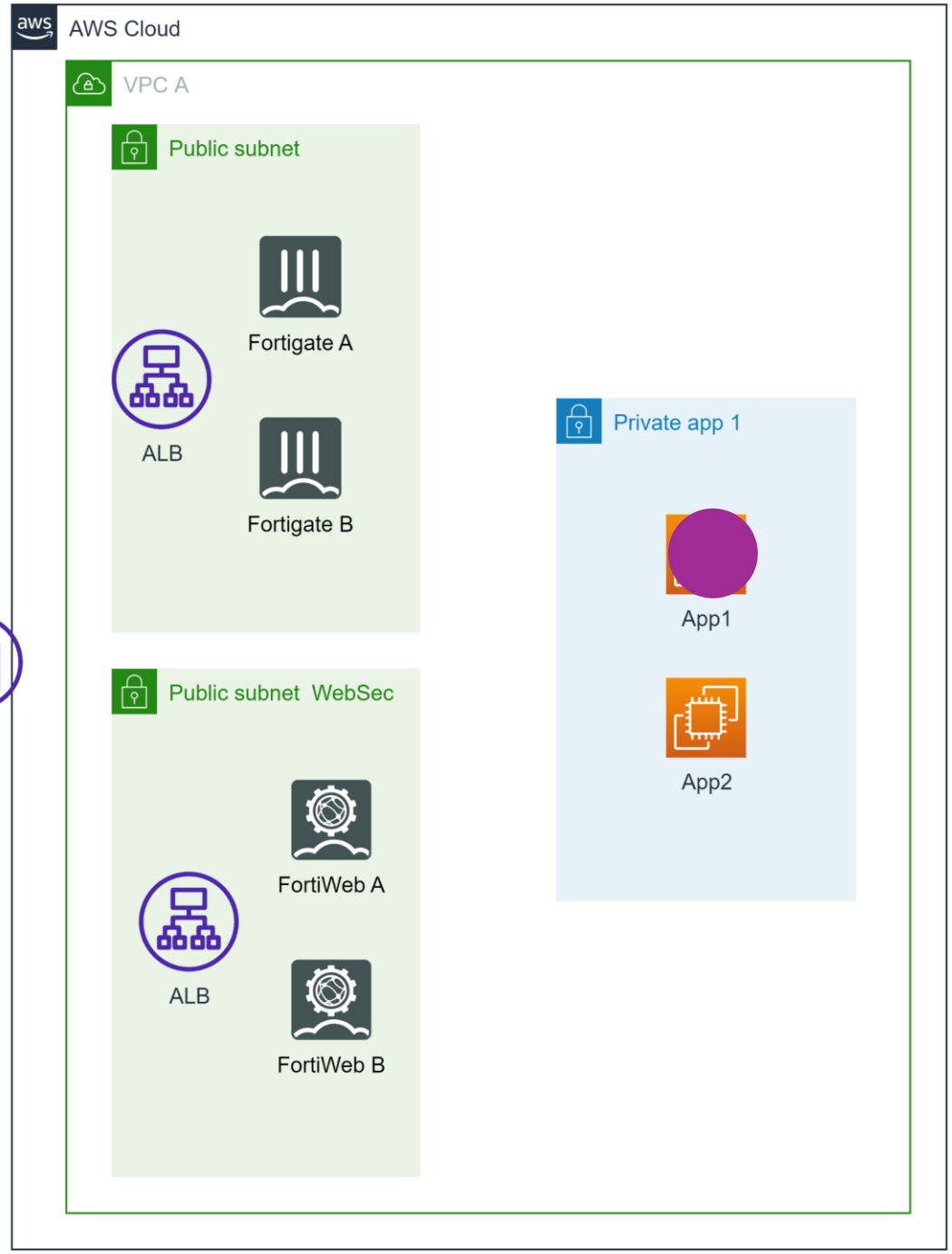
VM downloading OS updates, sending/uploading information to external APIs, etc

Paralelo

1. FortiGate é o responsável por todo tráfego de saída (egress)
2. Todo tráfego às aplicações (ingress) são direcionados ao FortiWeb
3. Gerenciamento simplificado
4. Tráfego otimizado

Internet user accessing a web application/API

VM downloading OS updates, sending/uploading information to external APIs, etc



Mónica Valladolid
Julho 24, 2024 @ 2: 50 pm

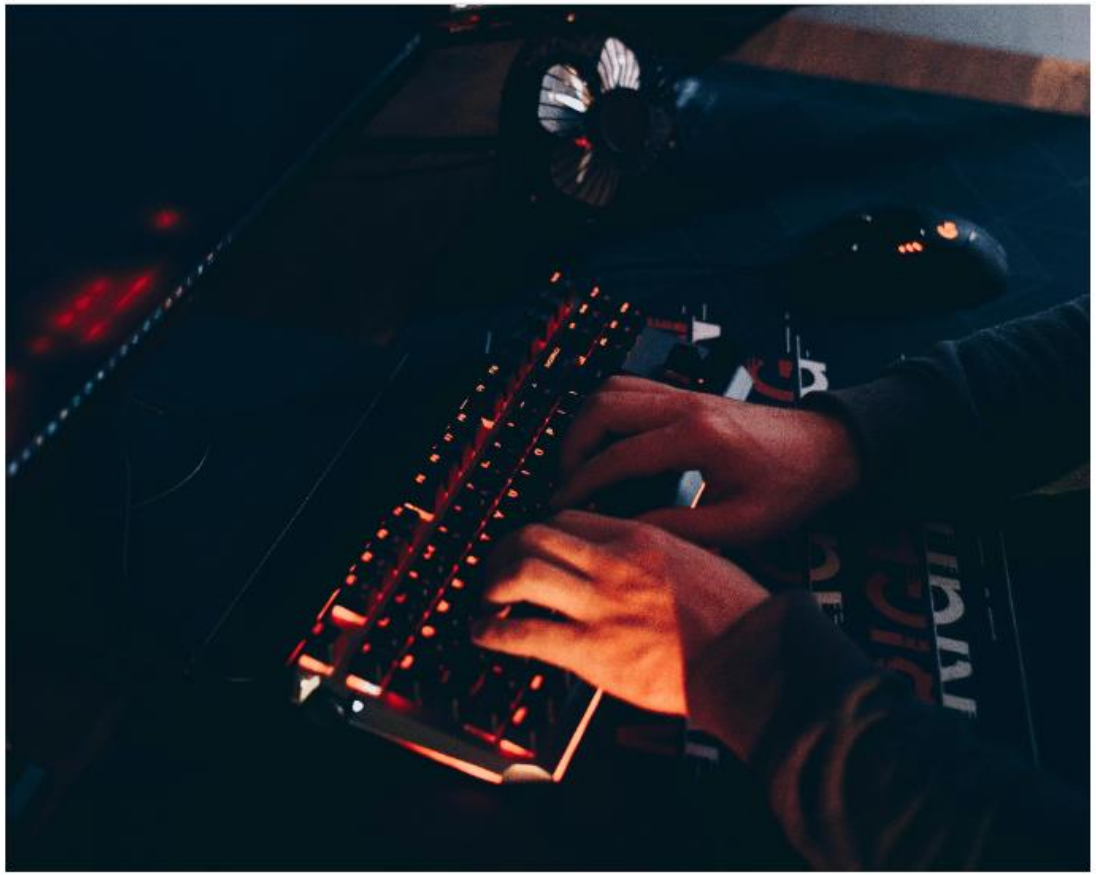
Animado para as Olimpíadas? Reduza o risco de hackers com essas dicas

Os fãs podem ser vítimas por quererem assistir a competições em plataformas de acesso gratuito, diz a empresa de segurança cibernética Fortinet.

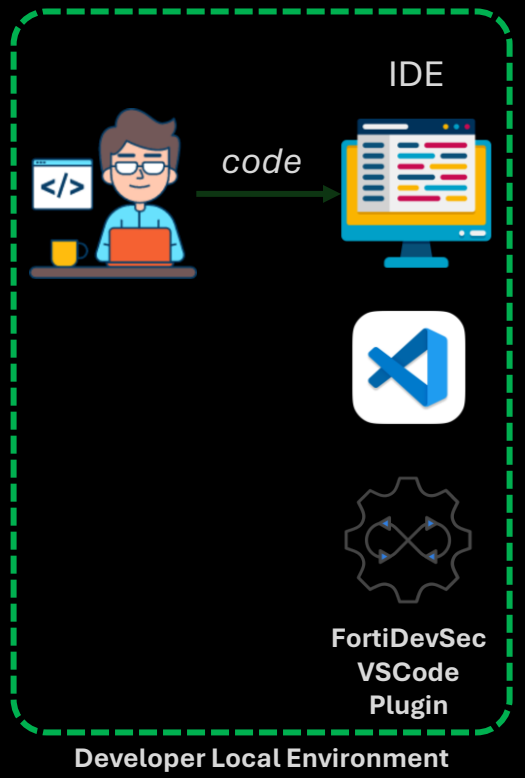
Hackers Eye Paris 2024: How Safe Are You From Olympic Cyber Attacks?

The Paris 2024 Olympics faces unprecedented cyber threats from phishing scams to ransomware. According to a Fortinet report, uncover the dark side of the Games and how to safeguard your data.

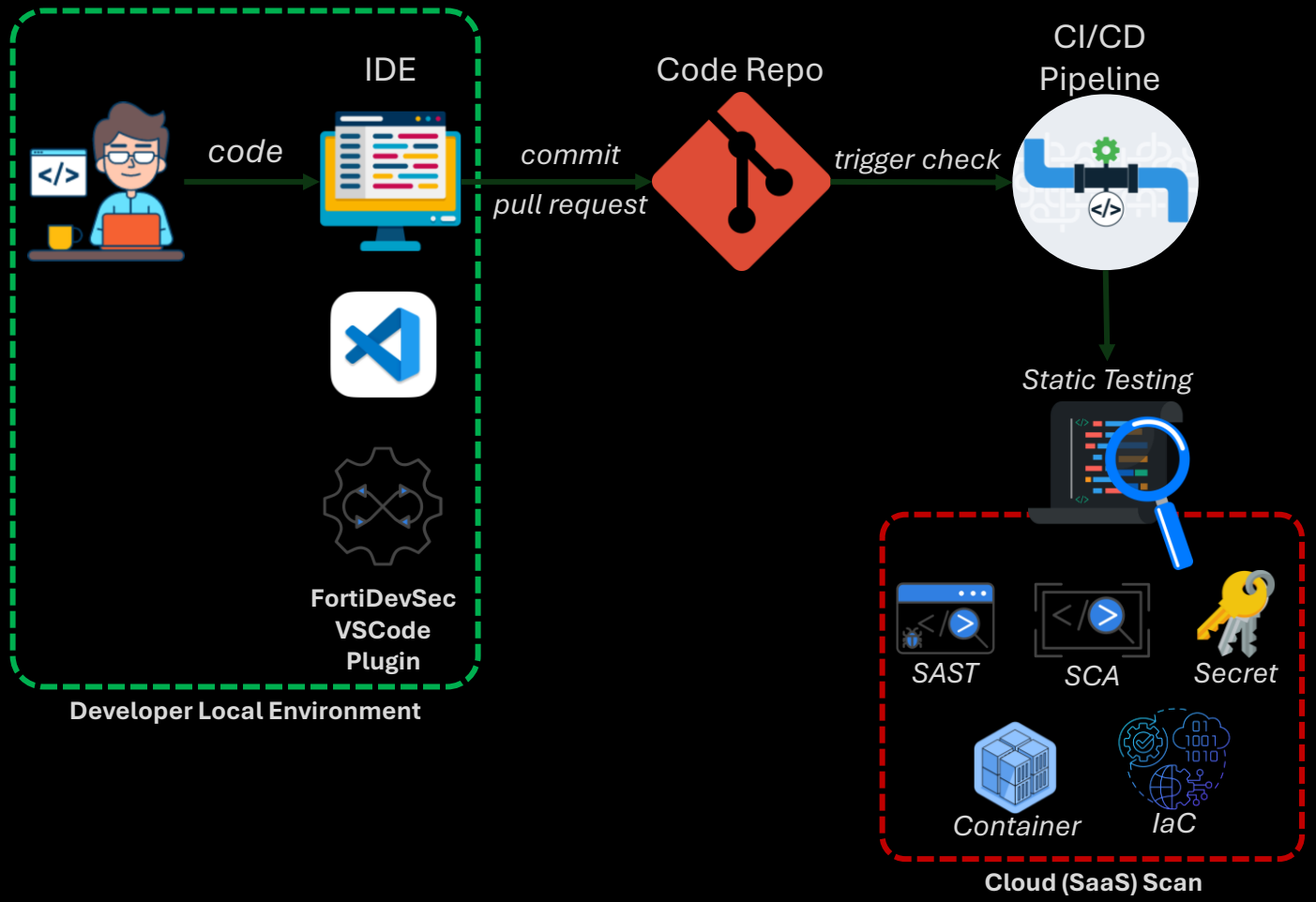
By Sindhu V Kashyap



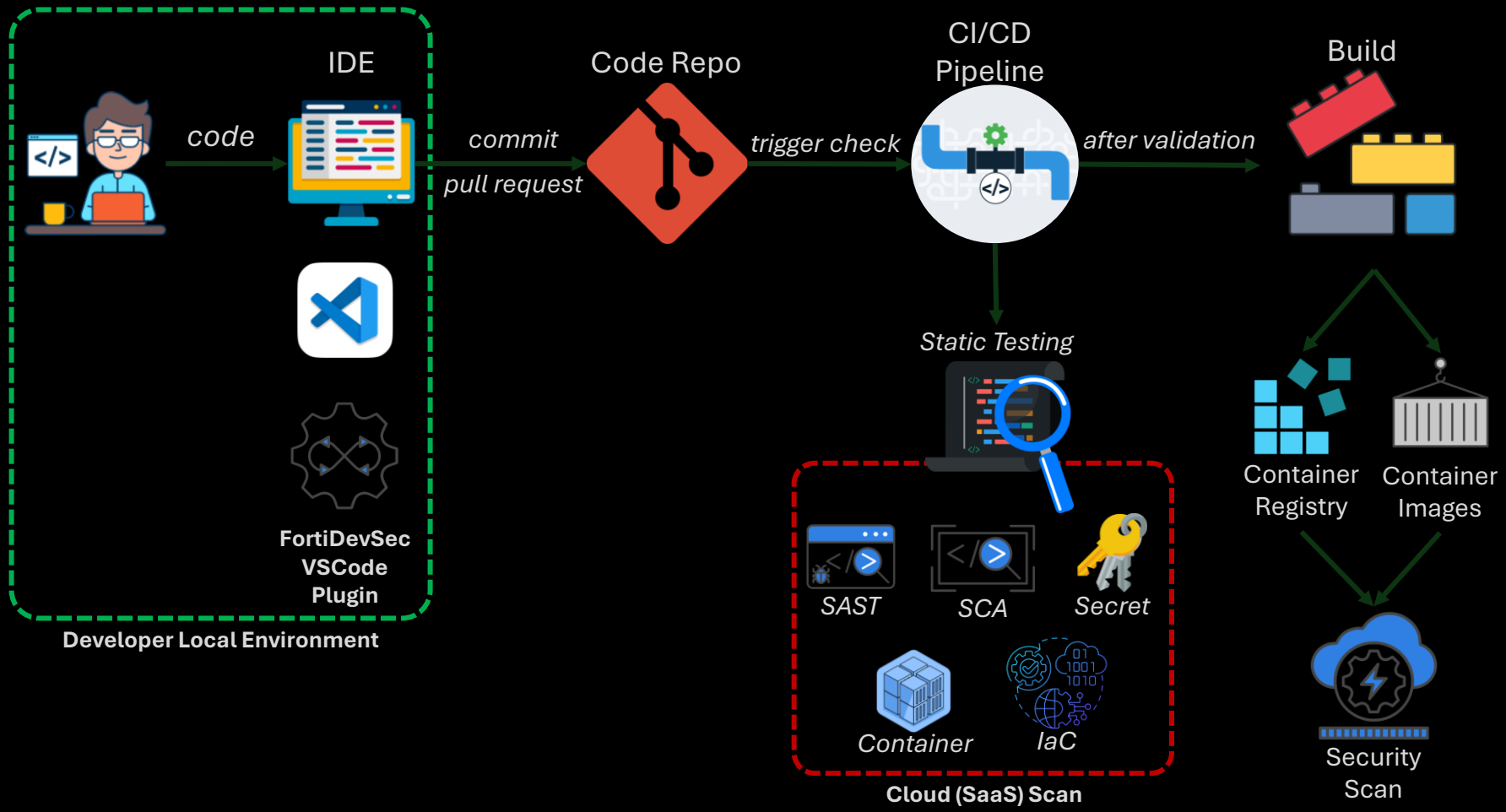
Segurança de Aplicações – Antes mesmo de um commit



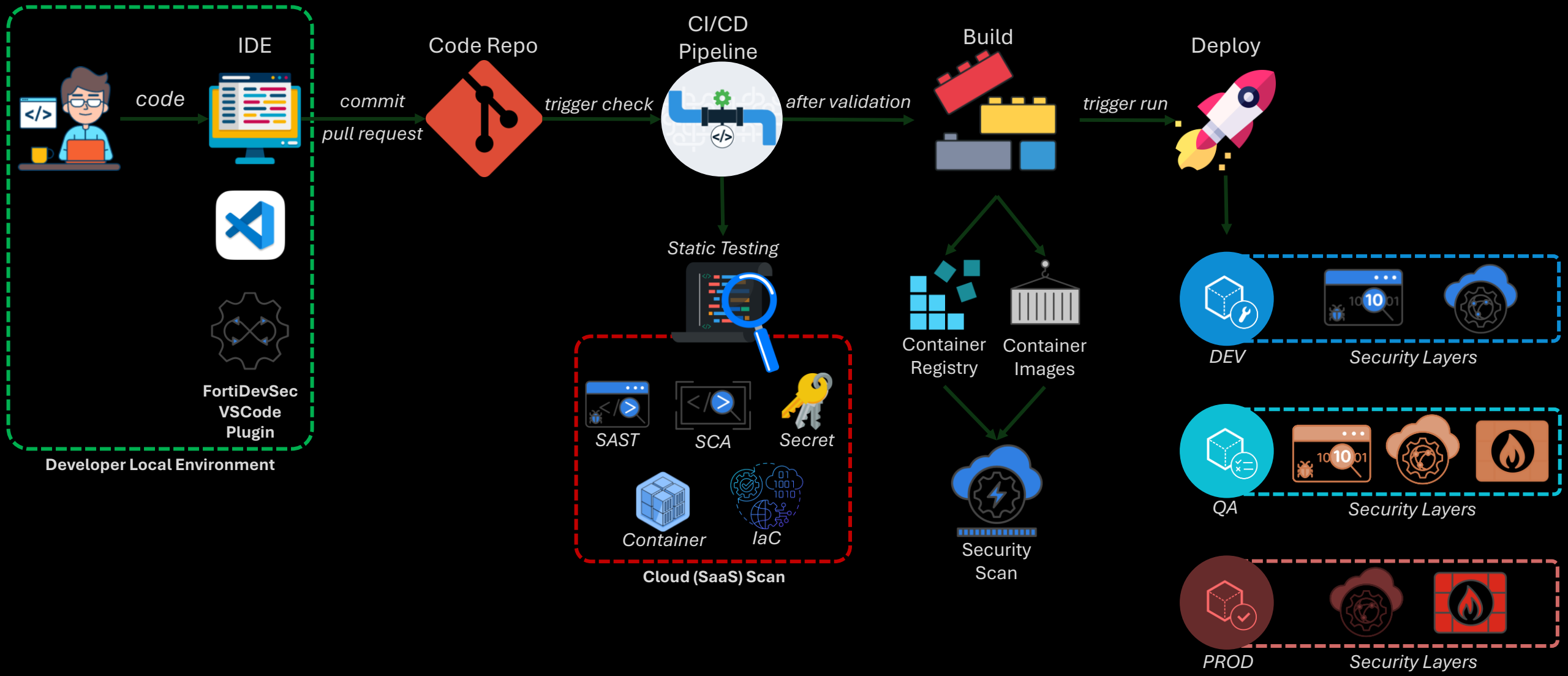
Segurança de Aplicações - Integrada à Pipeline



Segurança de Aplicações - Validações antes do Build



Segurança de Aplicações - Do Código ao Deploy




FORTINET