DEVSECOPS

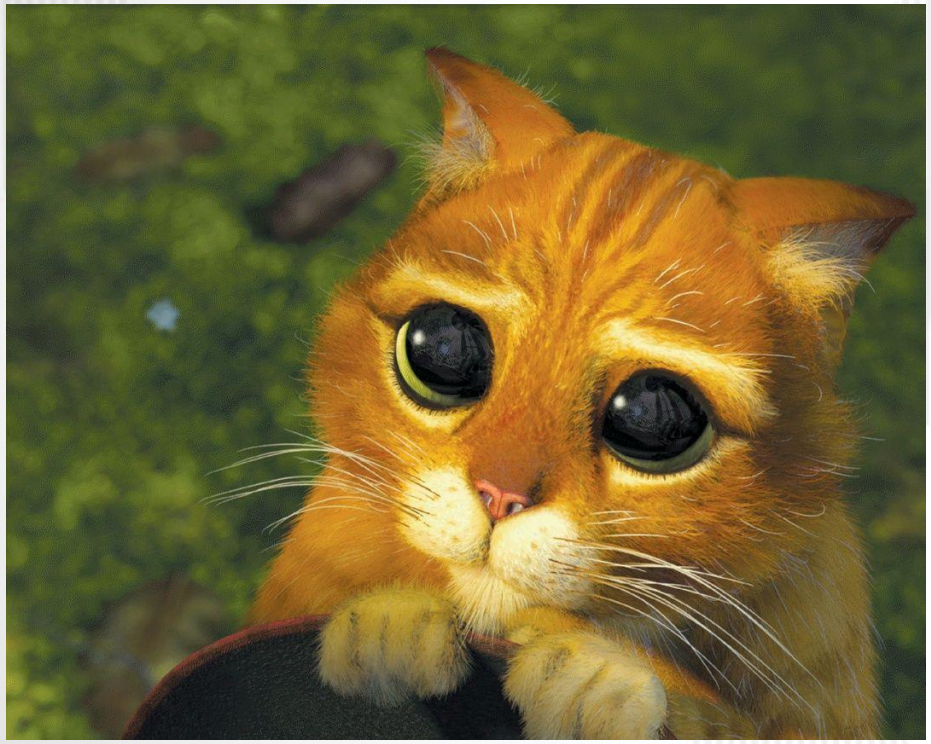
SHIFTLEFT

Henrique Moisés | hmoises@checkpoint.com | Check Point Security Engineer

José Irapuan | jfilho@checkpoint.com | Check Point Security Engineer

[Internal Use] for Check Point employees

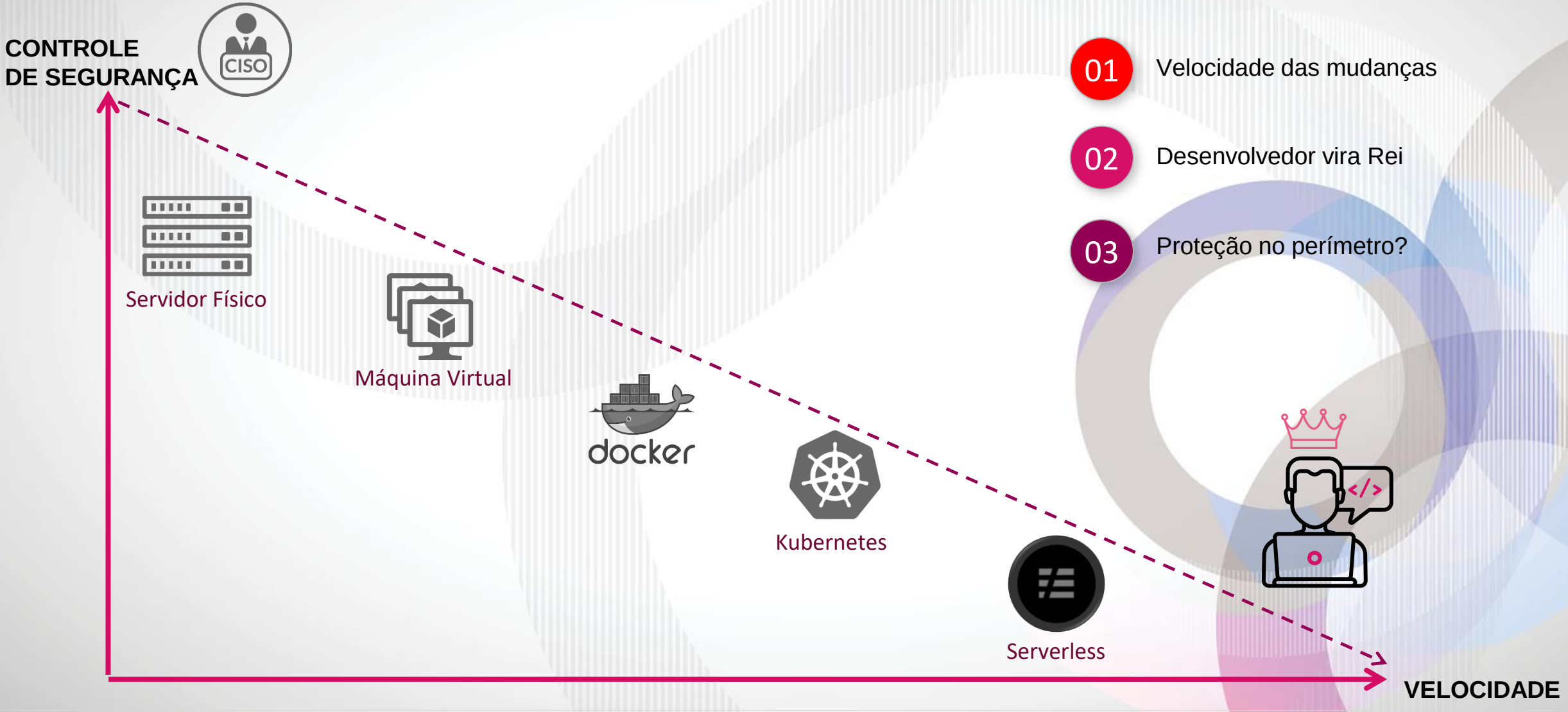
Mudança de Mindset para Segurança em Nuvem



X

[Internal Use] for Check Point employees ©[illegible] Software Technologies Ltd.

Troca de “poder” conforme a tecnologia evolui...



01 Velocidade das mudanças

02 Desenvolvedor vira Rei

03 Proteção no perímetro?

“Desenvolvimento Primeiro, Segurança Depois...”

Hackers agora exploram infraestrutura do GitHub para minerar criptomoeda

Cibercriminosos estão explorando o GitHub Actions, solução que facilita a automatização de todos os fluxos de desenvolvimento de software

Da Redação
06/04/2021

Fonte: CISO Advisor

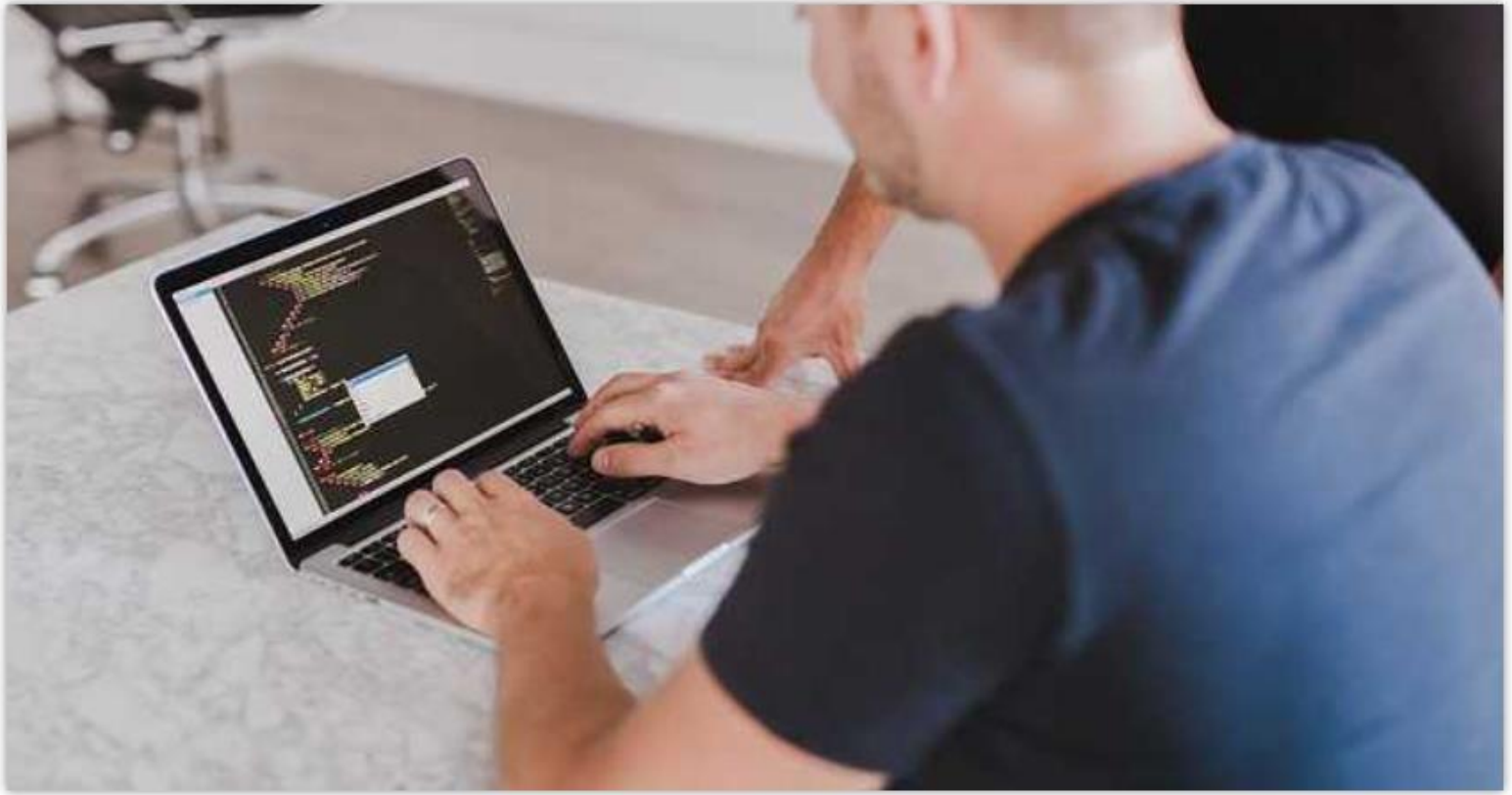
KUBERNETES / SECURITY

Kubernetes ‘Billion Laughs’ Vulnerability Is No Laughing Matter

9 Oct 2019 8:11am, by Jack Wallen

A new vulnerability has been discovered within the Kubernetes API. This flaw is centered around the parsing of YAML manifests by the Kubernetes API server.

Fonte: TheNewStack.io



Mercado DevSecOps está crescendo 33% ao ano

Estimado em US$ 2,9 bilhões no ano passado, o mercado deverá atingir um tamanho de US$ 17 bilhões em 2026, crescendo a uma taxa anual de 33,1%

Fonte: CISO Advisor

DevSecOps – viabilizando a Transformação Digital

33% de crescimento no período:
2020 a 2027 (taxa anual)

Integração de Segurança em todos os estágios de desenvolvimento

Automação de ferramentas para segurança avançada

Adoção da Cloud
viabilizada pela segurança

Source: https://www.researchandmarkets.com/reports/5301438/devsecops-market-by-deployment-type-by-vertical

[Internal Use] for Check Point employees
©2020 Check Point Software Technologies

DevSecOps – Benefícios

Organizations that do DevSecOps right:

deploy code 46x more frequently

are 2x more likely to exceed profitability

Organizations that utilize DevOps and the cloud:

deploy code 46% faster

reduce costs 56% more effectively

Last year, the average cost of a breach was over $3.6 Million

Mature DevOps organizations are 338% more likely to integrate automated security

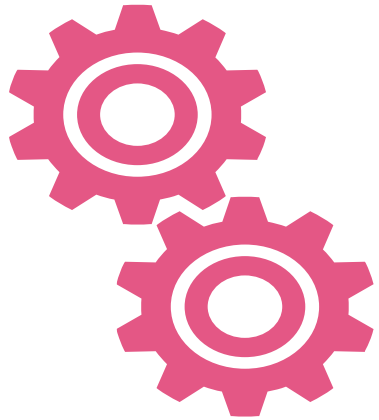
Organizations with high DevSecOps maturity are 144% more likely to resolve flaws quickly

The average annual cost of compliance for organizations is $5.47 Million

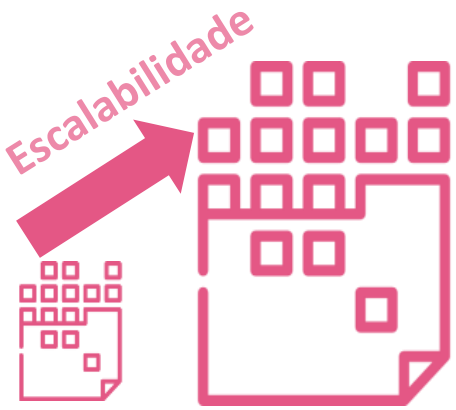
The cost of non-compliance has increased by 45% since 2011

Automated compliance technologies saved the average organization $1.43 Million

Agilidade



Automação



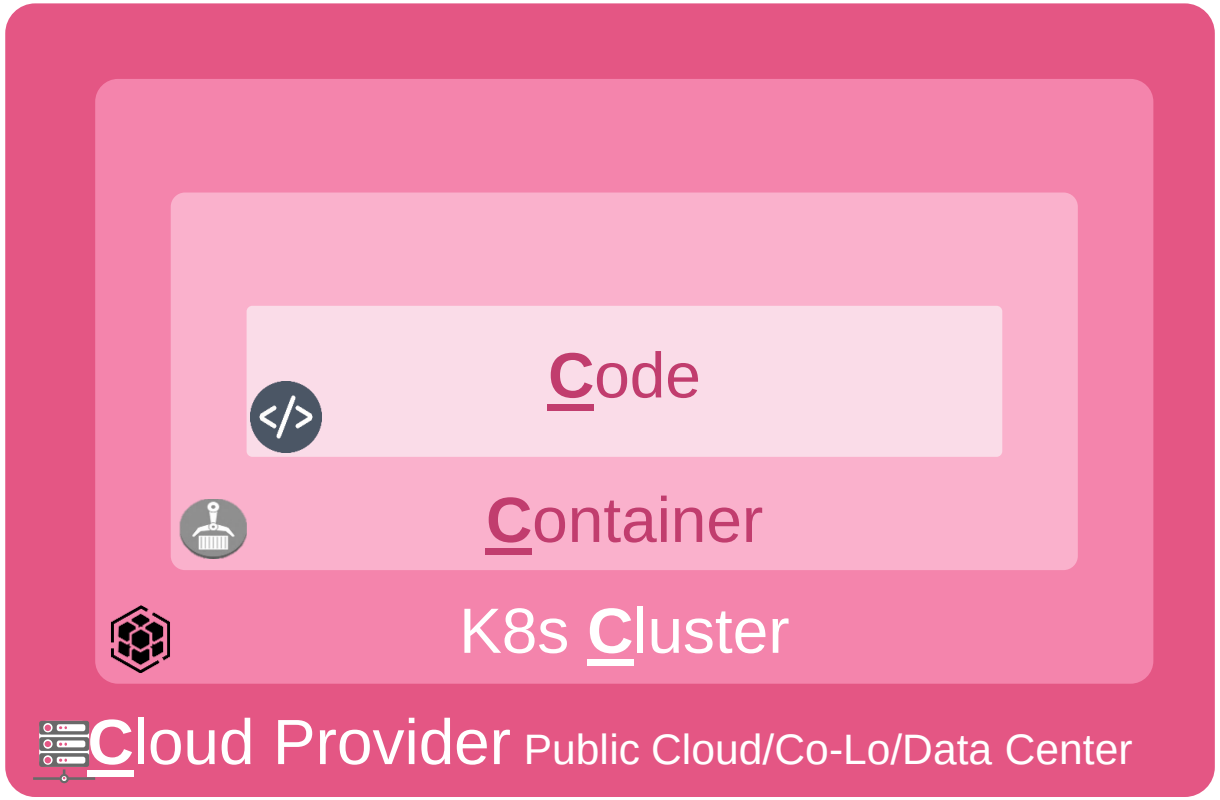
5 Ways DevSecOps Can Maximize ROI in the Cloud

[Internal Use] for Check Point employ

Abordagem em Camadas (4C model)

Princípio de Design :

- Abordagem em Camadas
- Aumenta e oferece opções para os times de Segurança

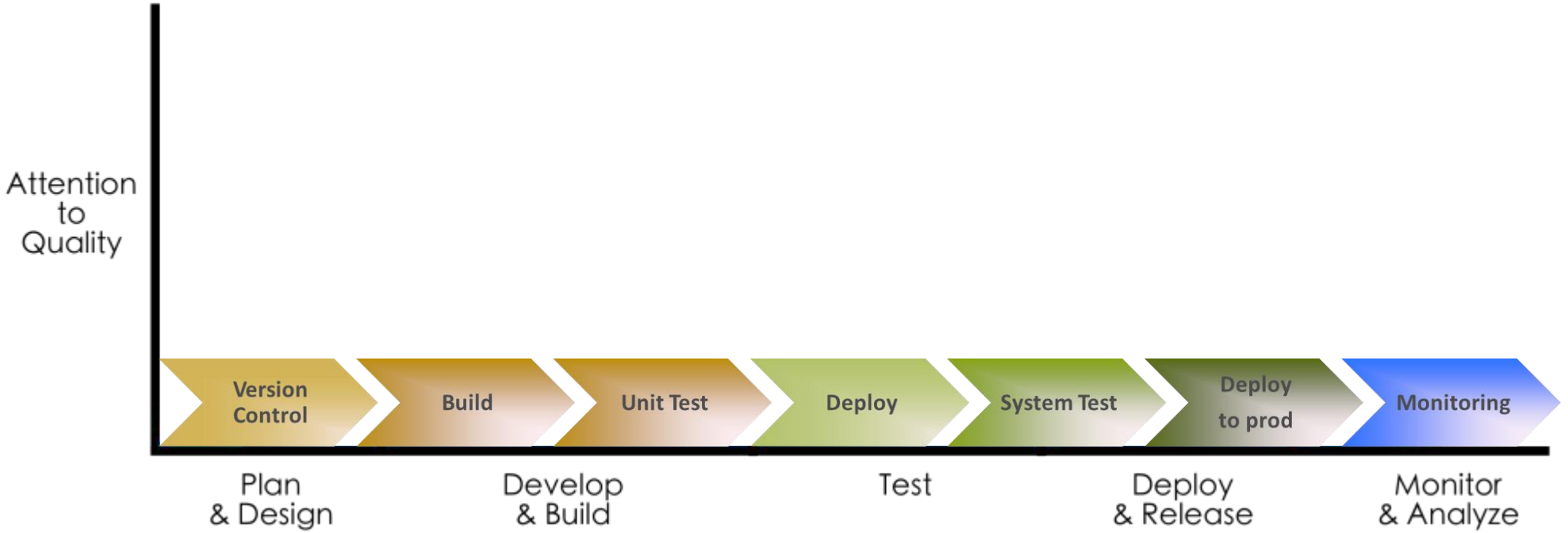


Source: https://kubernetes.io/docs/concepts/security/overview/

[Internal Use] for Check Point employees

©2021 Check Point Software Technologies Ltd.

DevSecOps - ShiftLeft



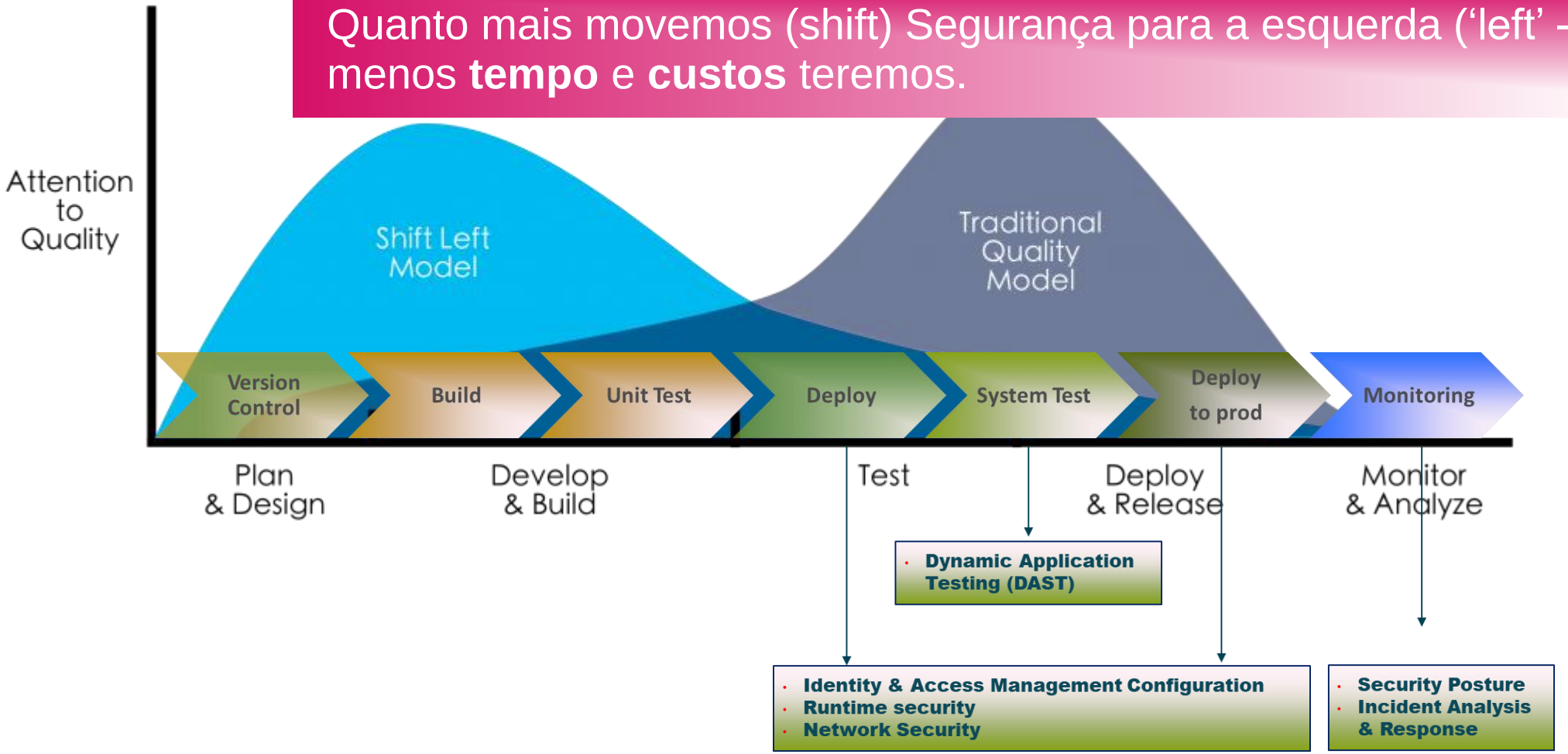
https://www.zdnet.com/article/cybercriminals-spotted-hiding-cryptocurrency-mining-malware-in-forked-projects-on-github/

[Internal Use] for CheckPoint employees

©2021 Check Point Software Technologies Ltd.

DevSecOps - ShiftLeft

Quanto mais movemos (shift) Segurança para a esquerda (‘left’ - dev side), menos **tempo** e **custos** teremos.

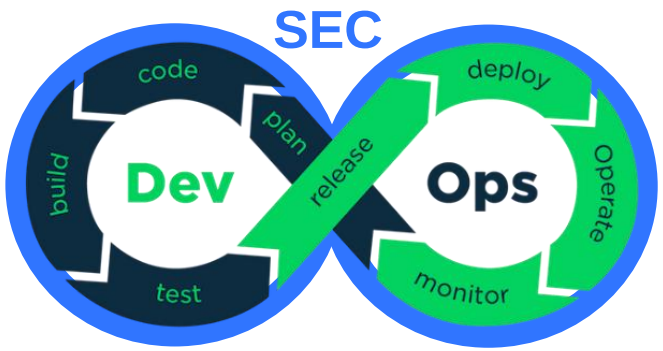


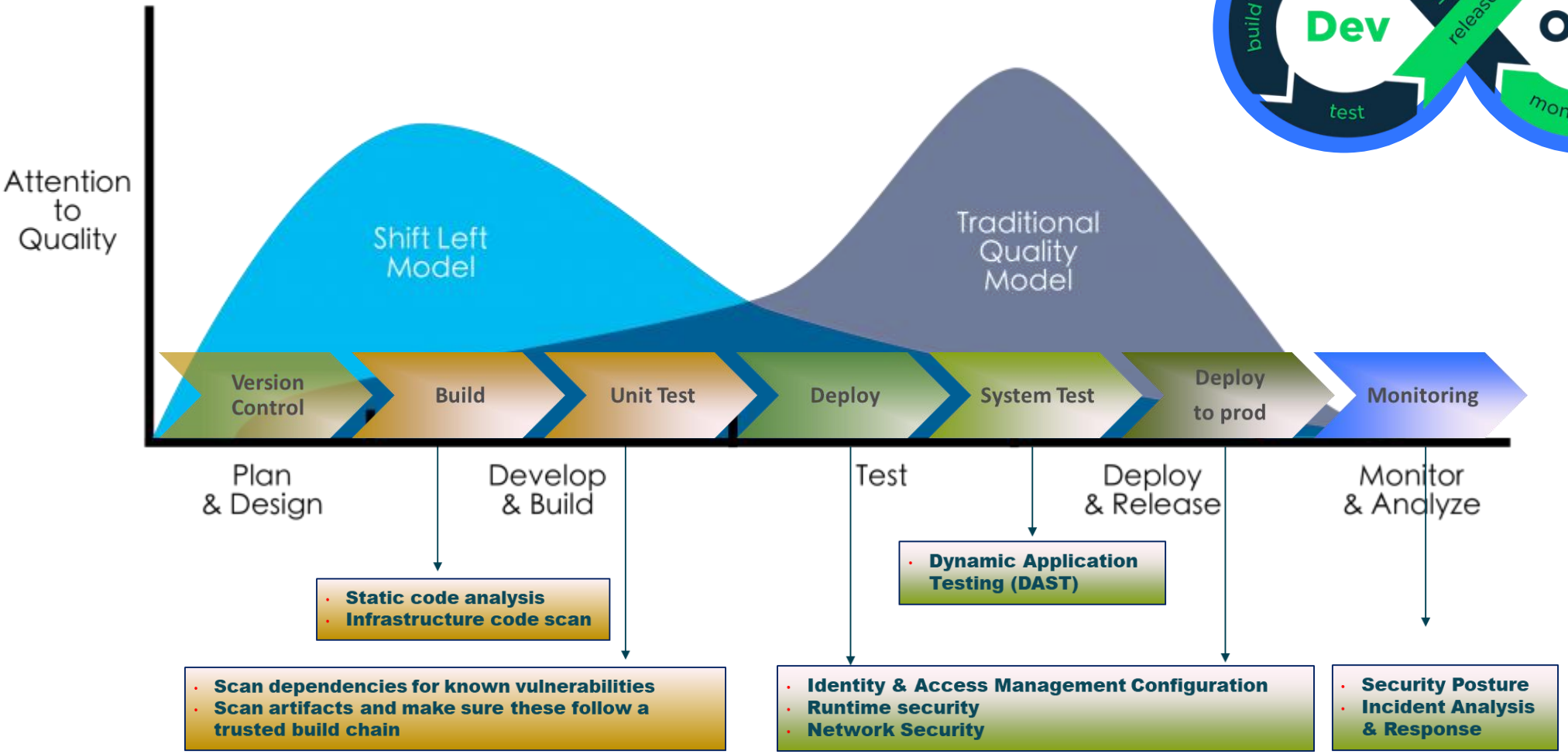
https://www.zdnet.com/article/cybercriminals-spotted-hiding-cryptocurrency-mining-malware-in-forked-projects-on-github/

[Internal Use] for CheckPoint employees

©2021 Check Point Software Technologies Ltd.

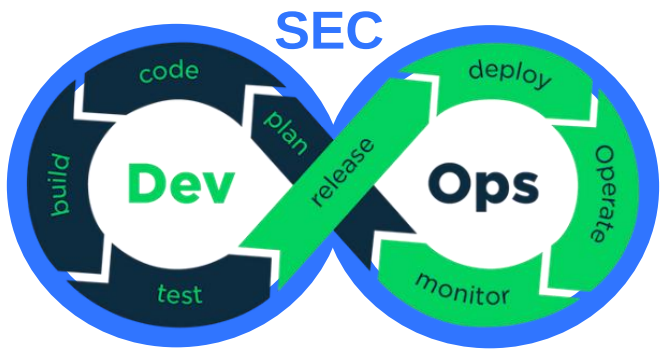
DevSecOps – “Shifting Left”





[Internal Use] for Check Point employees
©2021 Check Point Software Technologies Ltd.

“Novos” conceitos – SAST, DAST, RASP, IAST...



ShiftLeft

PIPELINE

AUTOMATION

SAST

RASP

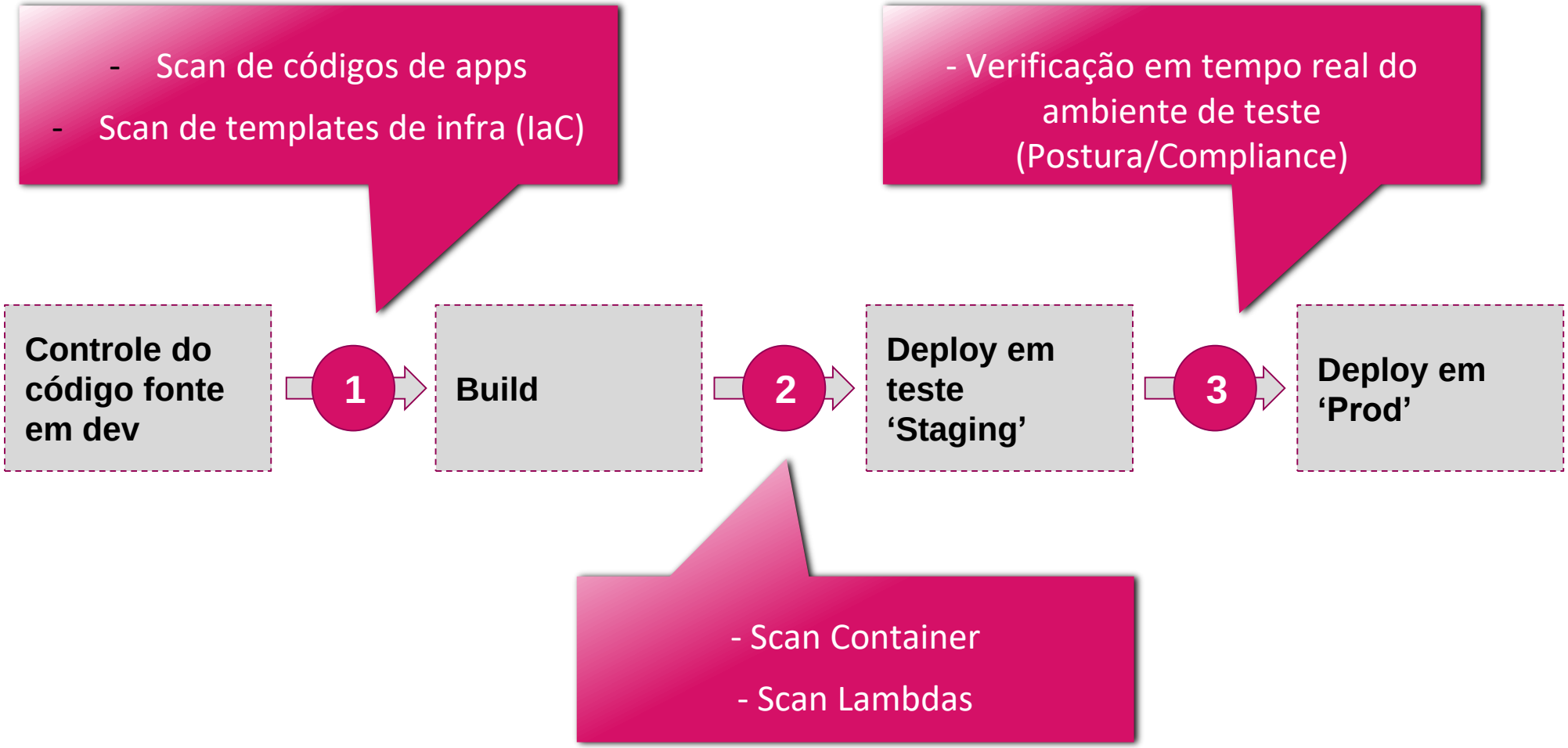
IAST

[Internal Use] for Check Point employees

©2021 Check Point Software Technologies Ltd.

SAST

Static Application Security Testing



[Internal Use] for Check Point employees

©2020 Check Point Software Technologies Ltd.

DAST

Dynamic Application Security Testing ou Runtime Security

Check Point
SOFTWARE TECHNOLOGIES LTD

O que é?

- Criação de um baseline baseado no comportamento da aplicação [white list]
- Prevenção de técnicas de ataque comuns [blacklist]

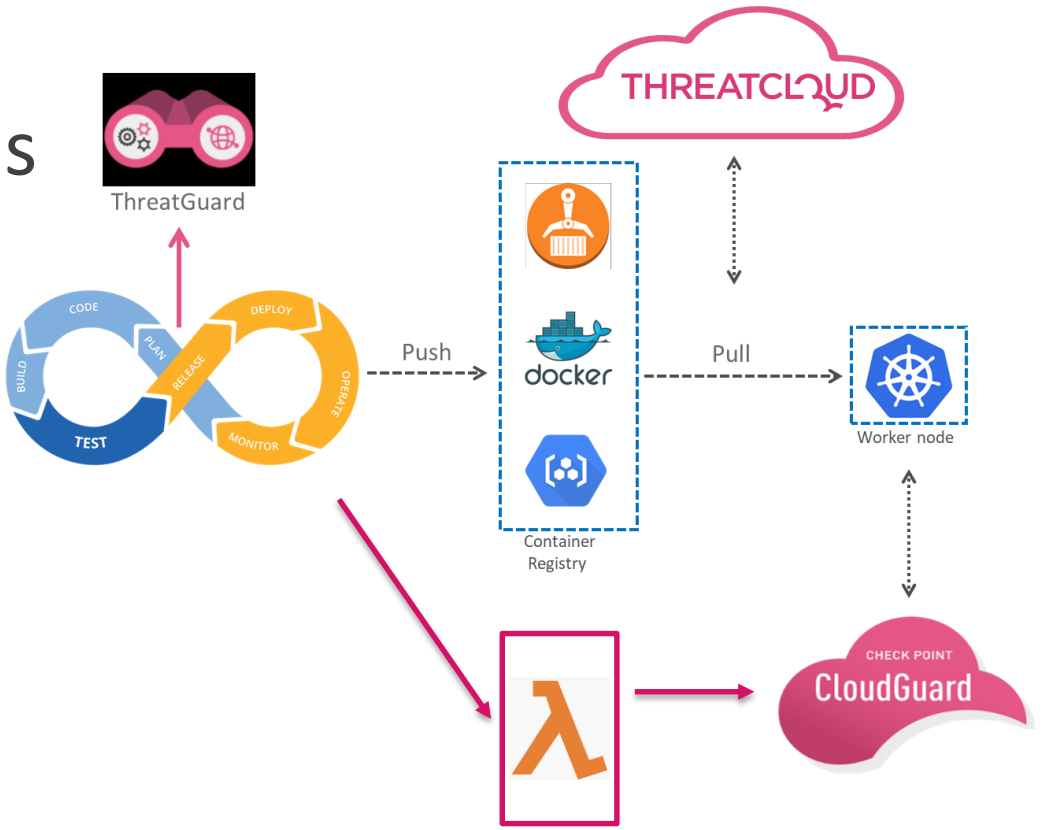
Como funciona?

- Por meio de análise de conexões de rede, chamadas API, Processos Locais, …

©2019 Check Point Software Technologies Ltd.
[Internal Use] for Check Point employees

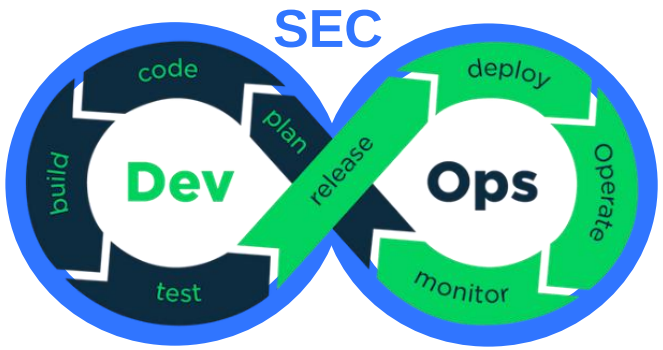
Scan de Workload

- Fazendo parte do pipeline CI/CD
- De maneira contínua nos workloads



[Internal Use] for Check Point employees
[Highly Restricted] ONLY for designated individuals
©2020 Check Point Software Technologies Ltd.

Atribuindo Segurança ao Pipeline



Version Control

Build

- Análise do Código
- Scan de IaC

SHIFTLEFT

Unit Test

- Scan de dependencias por vulnerabilidades
- Scan de métodos, garantindo que eles sigam uma cadeia confiável

SHIFTLEFT

Deploy

System Test

- Dynamic Application Testing (DAST)

SERVERLESS

WORKLOAD PROTECTION

Deploy to prod

- Configuração de Identity & Access Management
- Segurança em tempo de Execução
- Segurança de Rede

WORKLOAD PROTECTION

SERVERLESS

IAM PROTECTION

Monitoring

LOG.IC

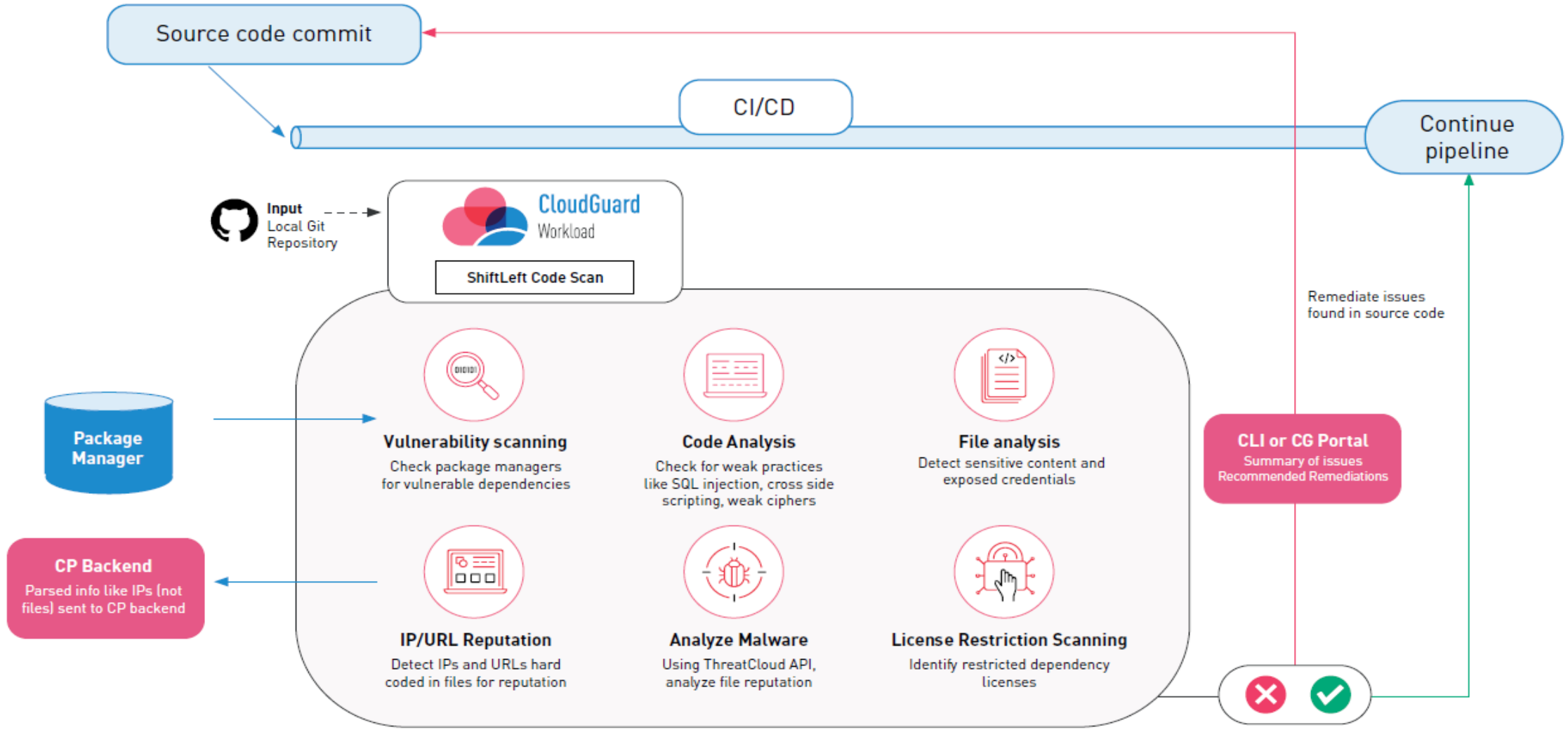
POSTURE MANAGEMENT

- Postura de Segurança
- Análise & Resposta à Incidentes

[Internal Use] for Check Point employees

©2021 Check Point Software Technologies Ltd.

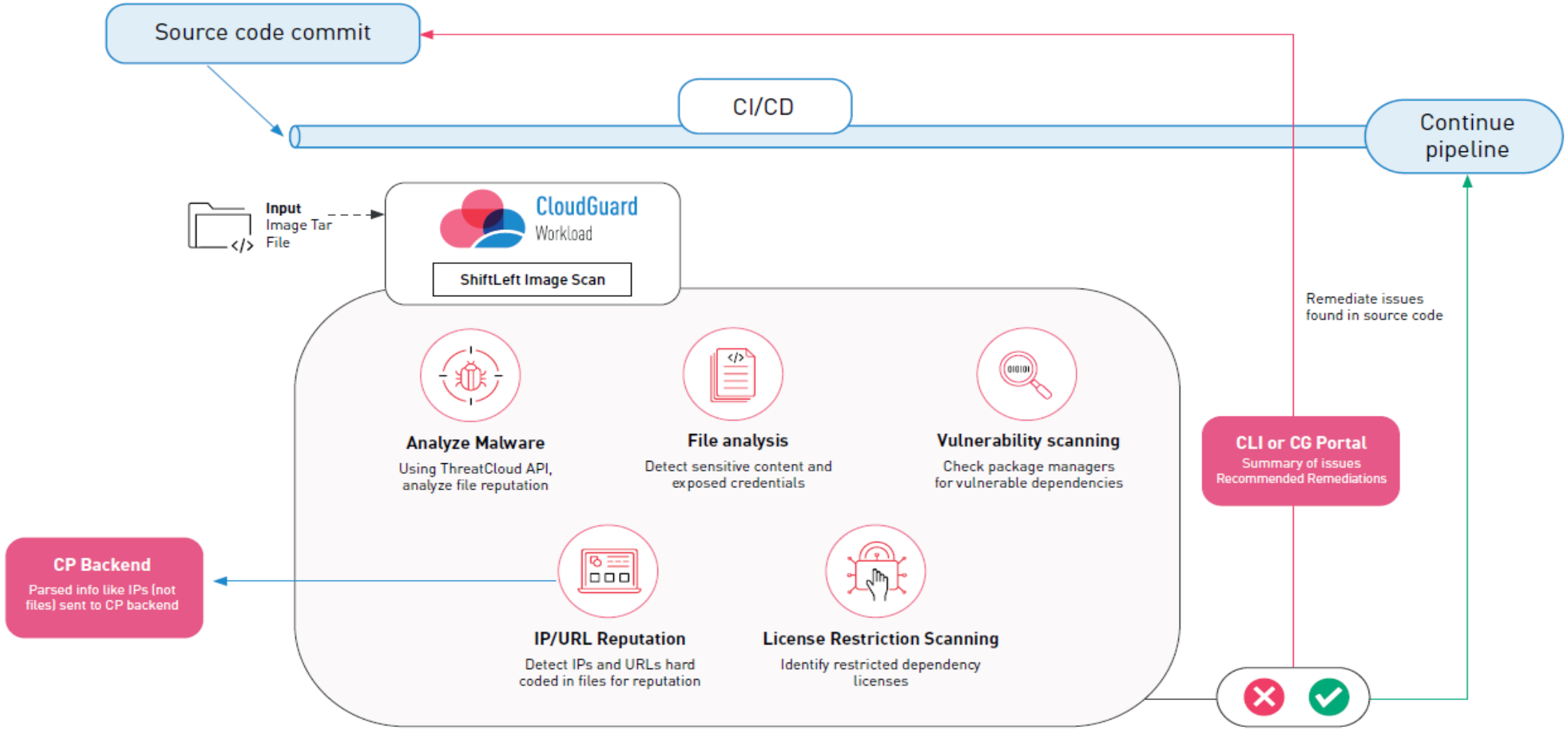
Segurança Integrada ao Pipeline – Code Scan



[Internal Use] for Check Point employees

©2021 Check Point Software Technologies Ltd.

Segurança Integrada ao Pipeline – Image Scan

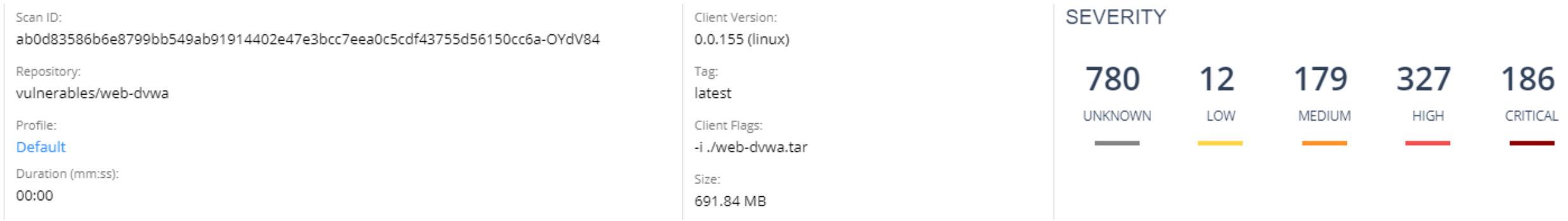


[Internal Use] for Check Point employees

©2021 Check Point Software Technologies Ltd.

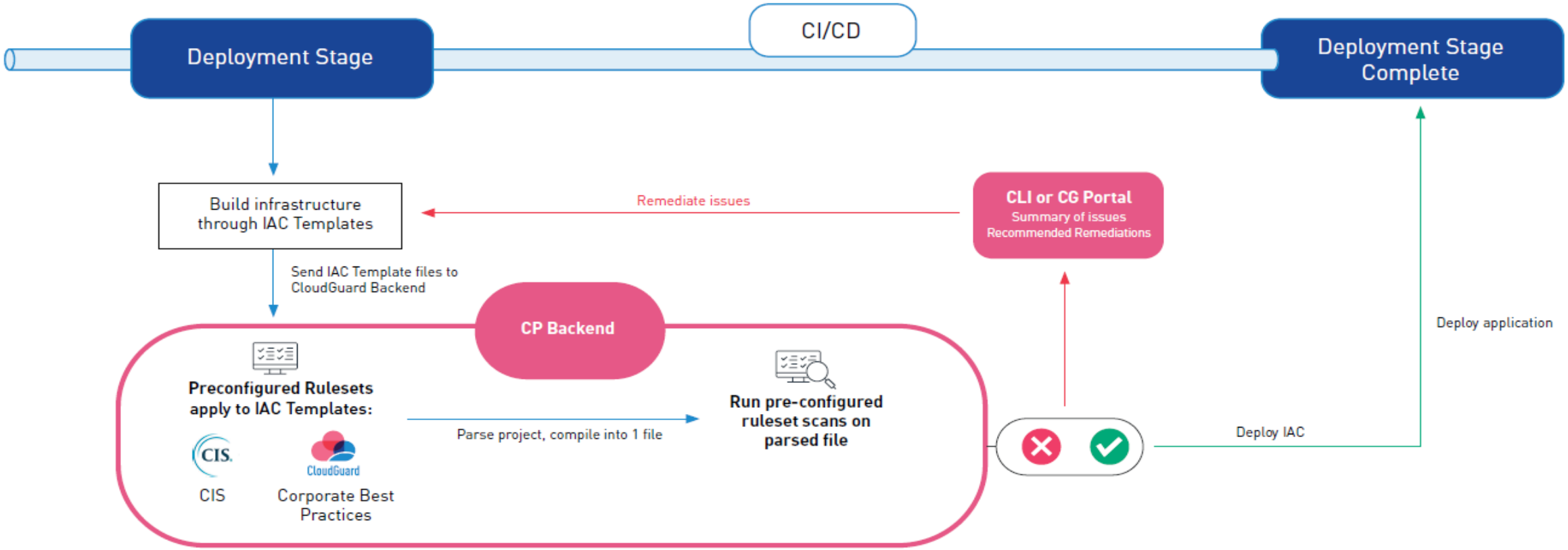
ShiftLeft – Overview do Image Scanner

- Depois das análises:
  - Sistema Operacional
  - CVEs
  - Aplicações e Depencências
  - Arquivos
  - Conteúdo Sensível no código-fonte



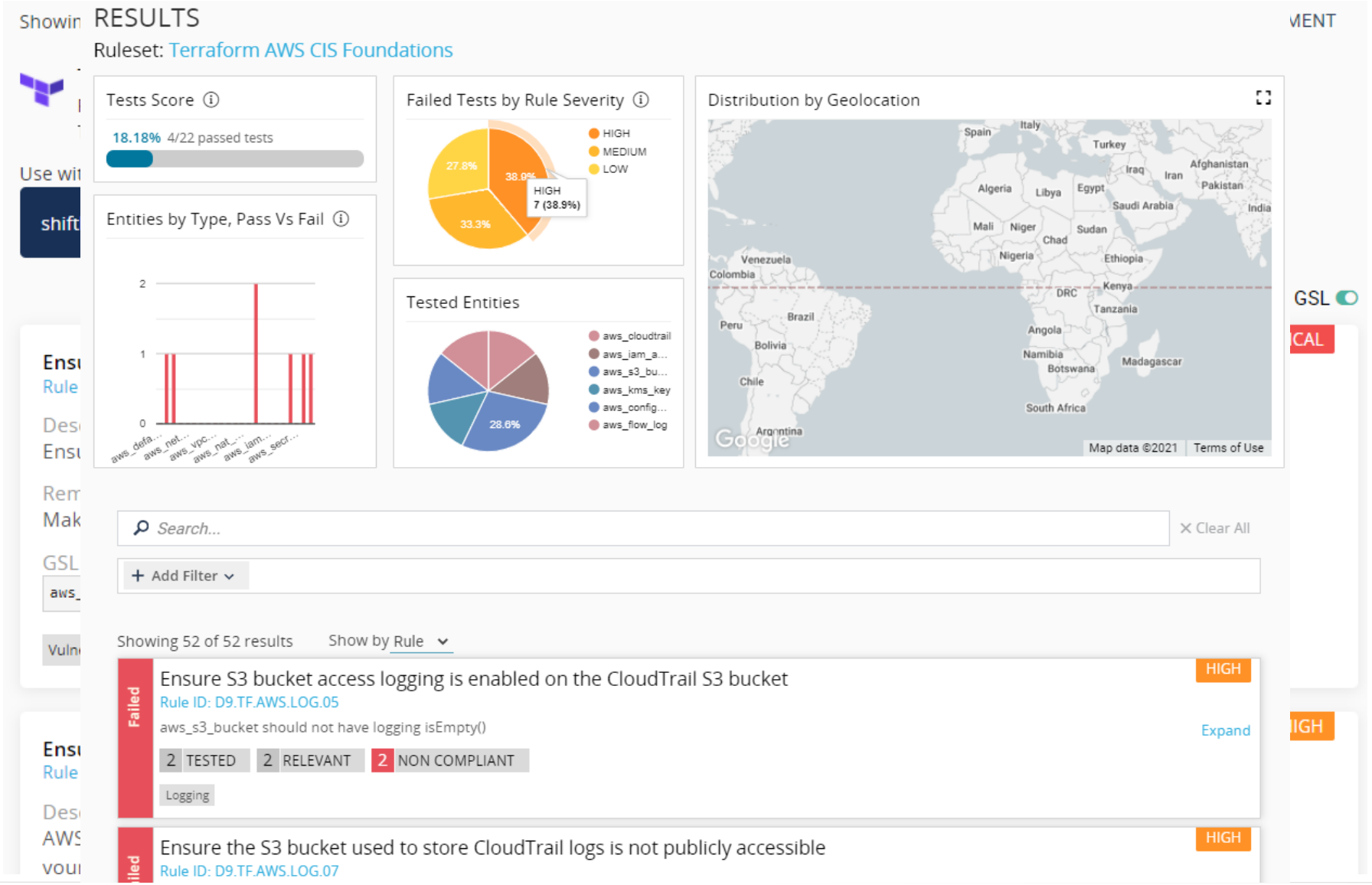
[Internal Use] for Check Point employees
©2021 Check Point Software Technologies Ltd.

Segurança Integrada ao Pipeline - IaC



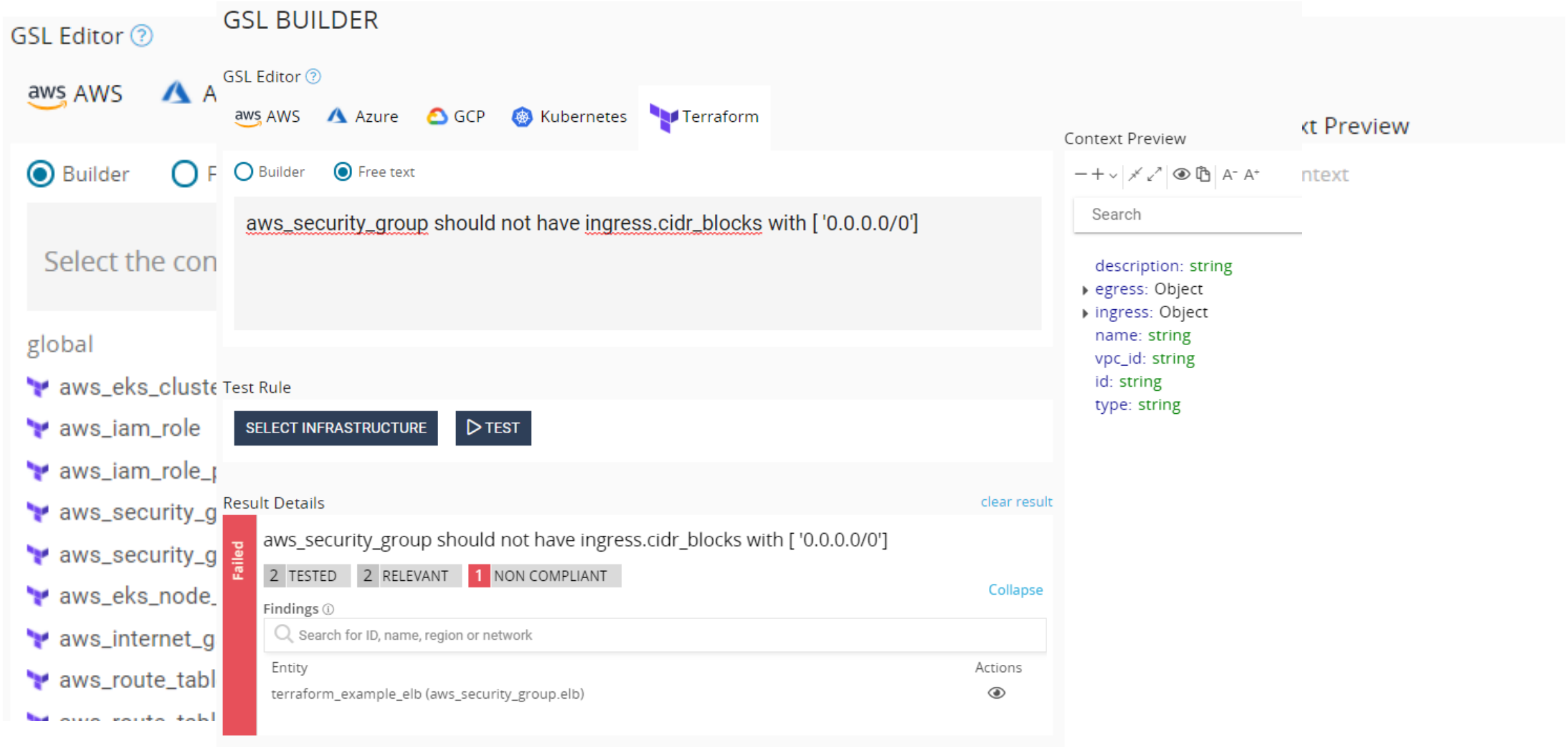
[Internal Use] for Check Point employees
©2021 Check Point Software Technologies Ltd.

ShiftLeft – IaC Assessment – Framework Ruleset



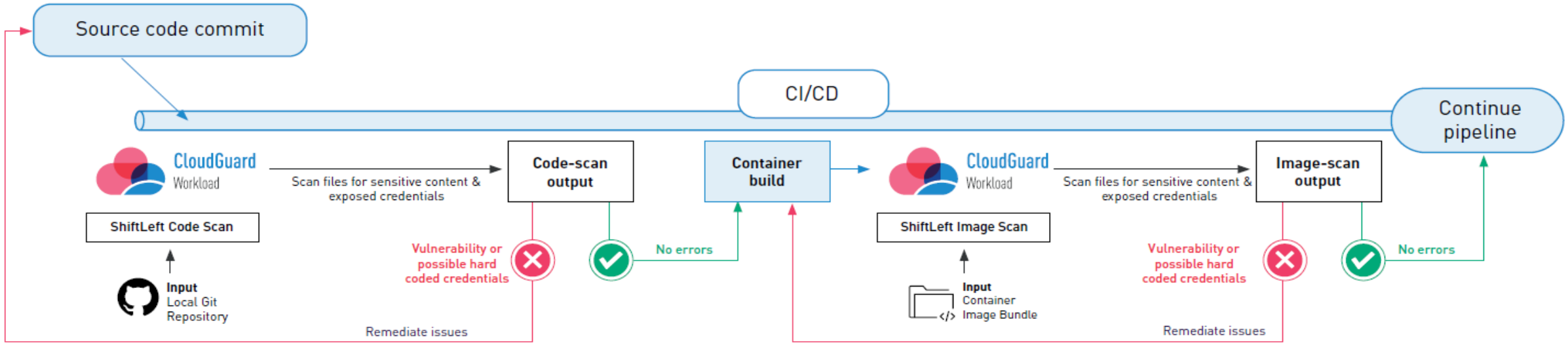
©2021 Check Point Software Technologies Ltd.

ShiftLeft – IaC Assessment – Custom Rules



©2021 Check Point Software Technologies Ltd.

Exposição de Credenciais



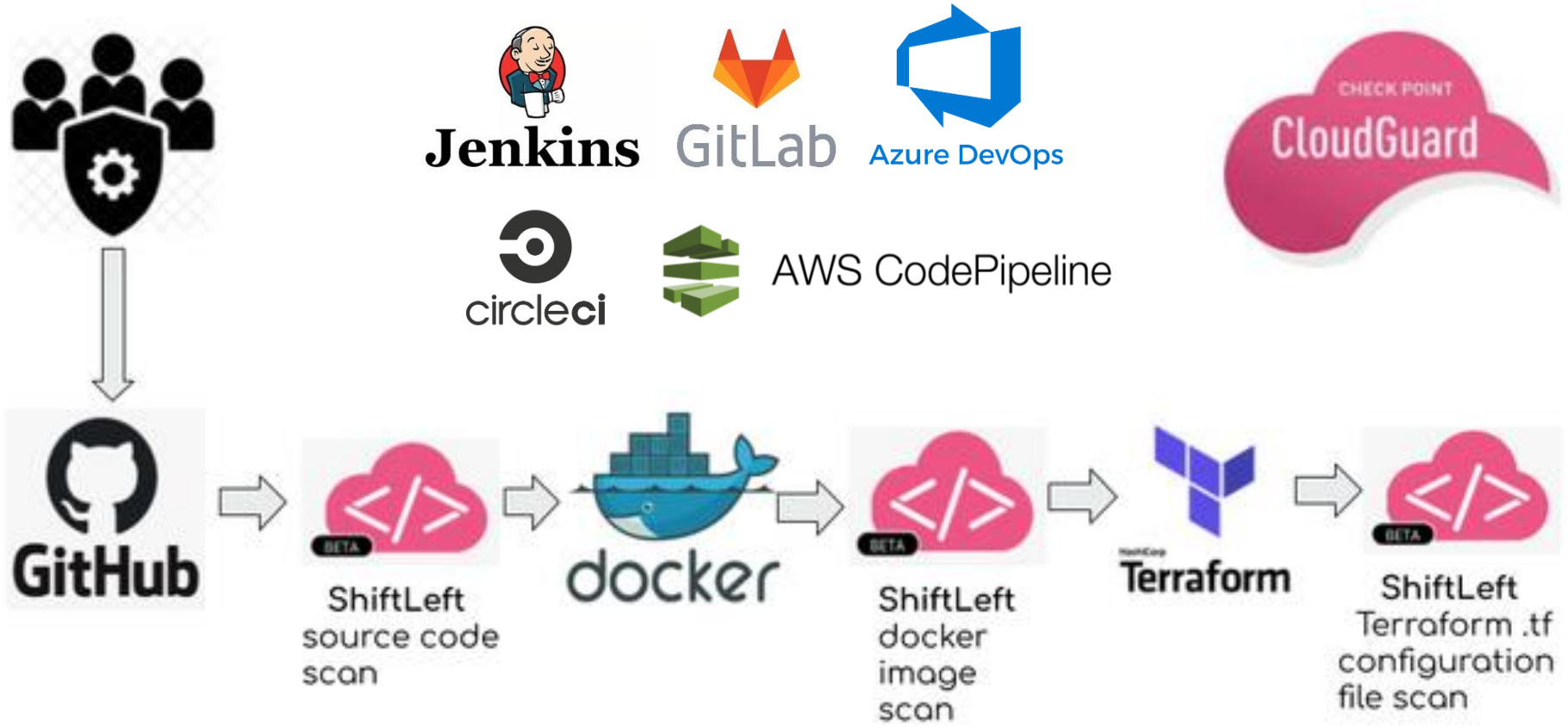
[Internal Use] for Check Point employees
©2021 Check Point Software Technologies Ltd.

Check Point
SOFTWARE TECHNOLOGIES LTD

DEMO

[Internal Use] for Check Point employees

Integração Simples com seu Pipeline CICD



[Internal Use] for Check Point employees
©2021 Check Point Software Technologies Ltd.

CAMADAS E HIERARQUIA DA PLATAFORMA DE SEGURANÇA EM NUVEM

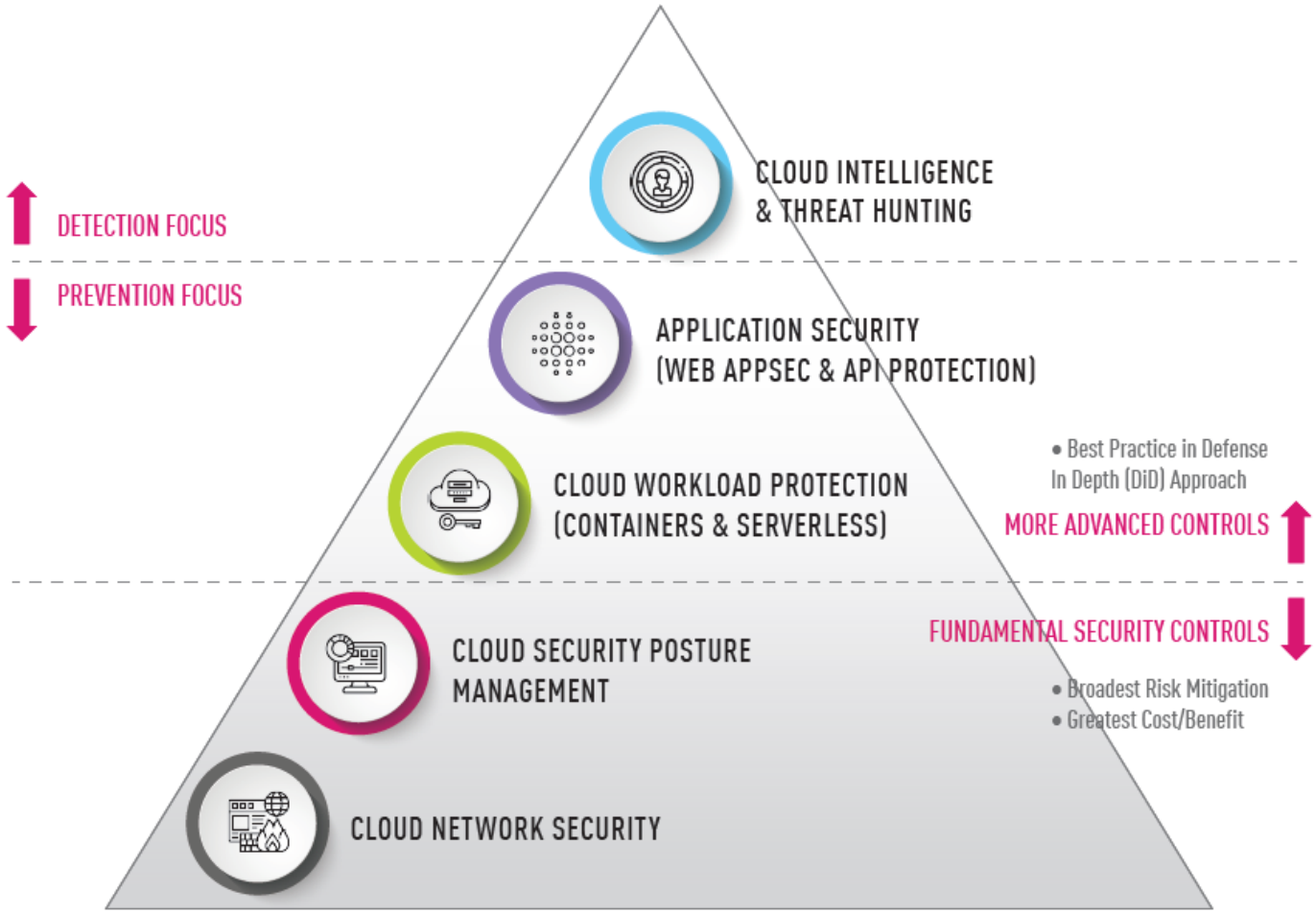


Figure 1: The Multiple Layers of a Unified Cloud Native Security Platform

©2020 Check Point Software Technologies Ltd.

OBRIGADO!

Henrique Moisés | hmoises@checkpoint.com | Check Point Security Engineer

José Irapuan | jfilho@checkpoint.com | Check Point Security Engineer

[Internal Use] for Check Point employees