
KubeCon
CloudNativeCon
OPEN SOURCE SUMMIT
China 2023


KubeCon | CloudNativeCon

OPEN SOURCE SUMMIT

China 2023

自动化云原生应用的零信任

Erin Quill & Raul Mahiques

自动化云原生应用的零信任

KubeCon CloudNativeCon
OPEN SOURCE SUMMIT
China 2023

SUSE

Raul Mahiques
技术营销经理

SUSE

Erin Quill
技术营销经理

自动化云原生应用的零信任

KubeCon CloudNativeCon OPEN SOURCE SUMMIT China 2023

议程

1. 概述
2. 实施
3. 演示
4. 结论
5. 问答

概述

自动化云原生应用的零信任

零信任概念

它是关于什么的?

- 无隐含的信任
- 信任必须被明确定义

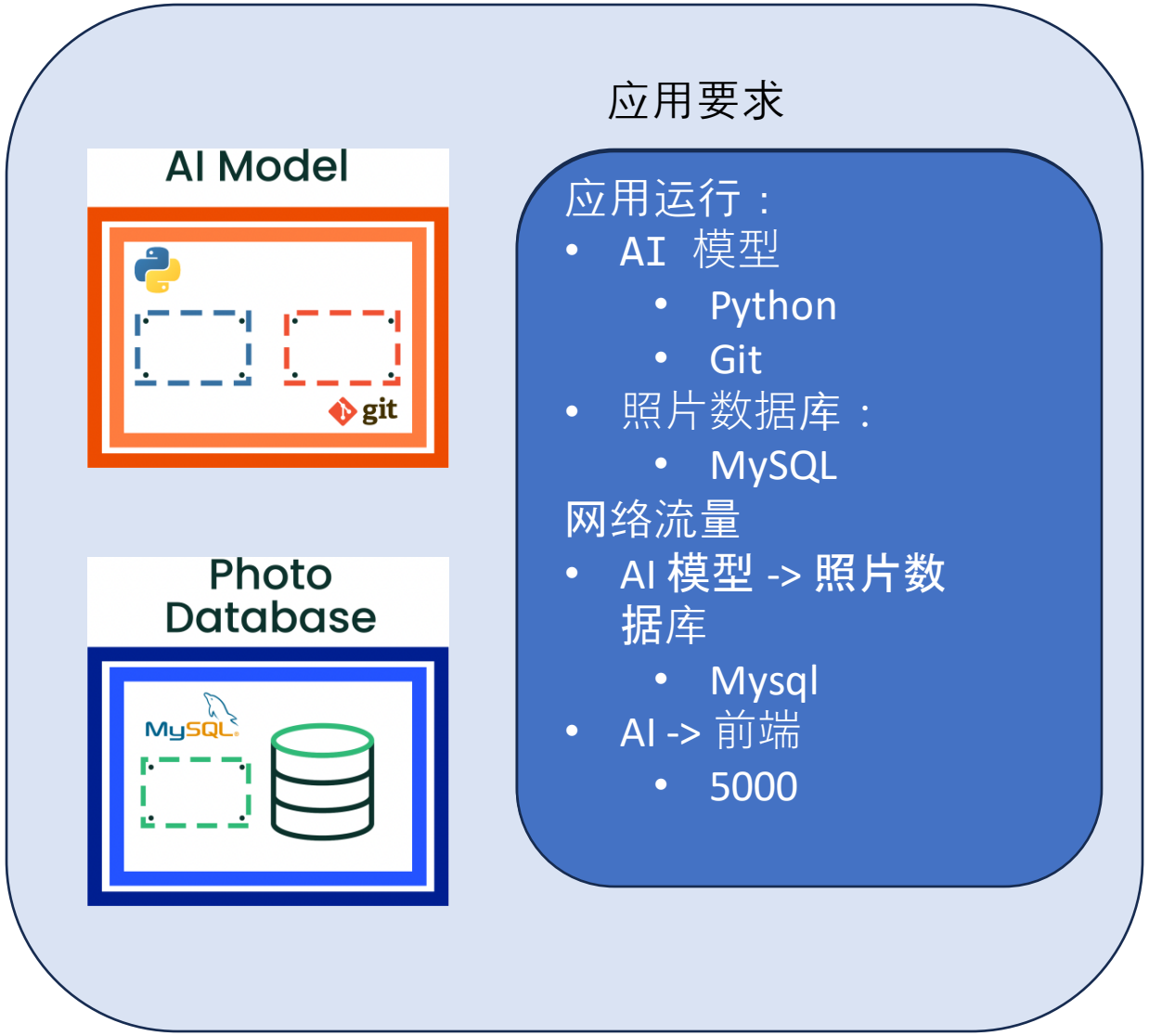
自动化云原生应用的零信任

零信任概念

但是信任谁/什么？为了做什么？何时？从哪里？

信任

- 一个网络数据包，
- 为了访问我的后端应用，
- 当使用mysql协议时，
- 来自我的前端应用。



自动化云原生应用的零信任

KubeCon CloudNativeCon OPEN SOURCE SUMMIT China 2023

零信任概念

怎样？

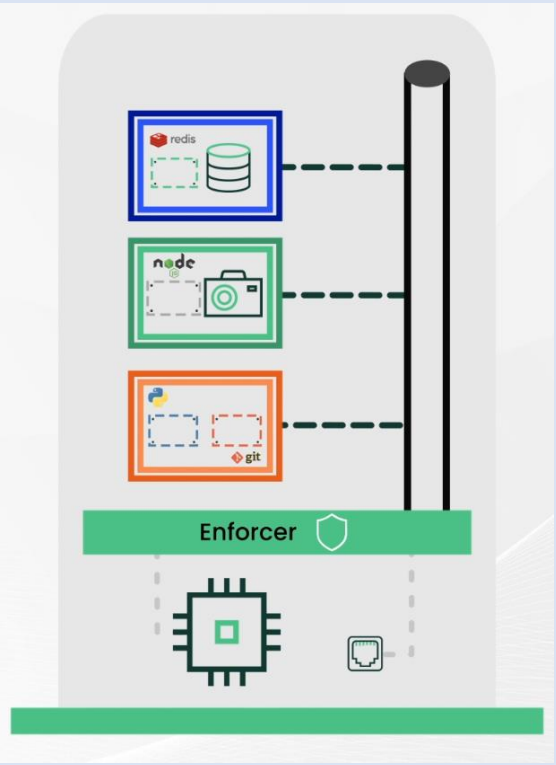
- 定义安全策略
  - 应用需要什么才能正常工作
- 由安全平台执行和管理。

Security Policy

应用要求

应用运行：
- AI 模型
  - Python
  - Git
- 照片数据库：
  - MySQL

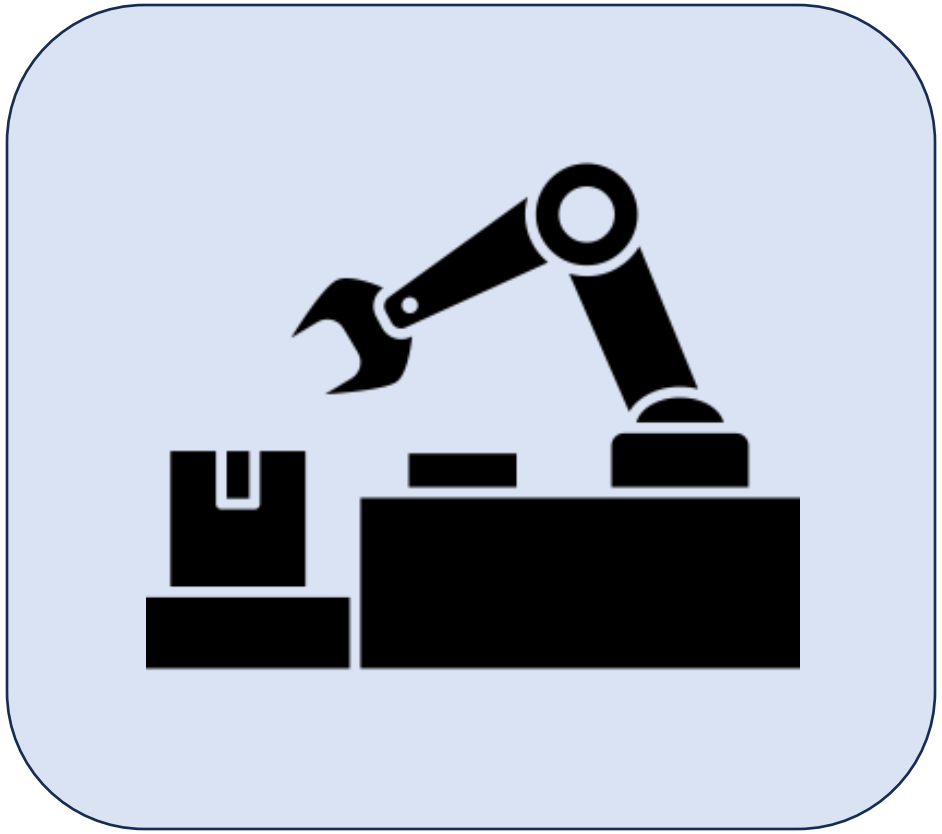
网络流量
- AI 模型 -> 照片数据库
- Mysql
- AI -> 前端
  - 5000



自动化

为什么我们需要自动化？

- 手工操作容易出错
- 手动干预使过程变慢
- 安全性很复杂
- 快速响应威胁的重要性
- 应用程序始终在发展
  - 功能开发中的安全集成
- 不要拖慢开发进度
- Kubernetes是自动化的理想中心化平台



自动化云原生应用的零信任

NeuVector

容器原生安全平台

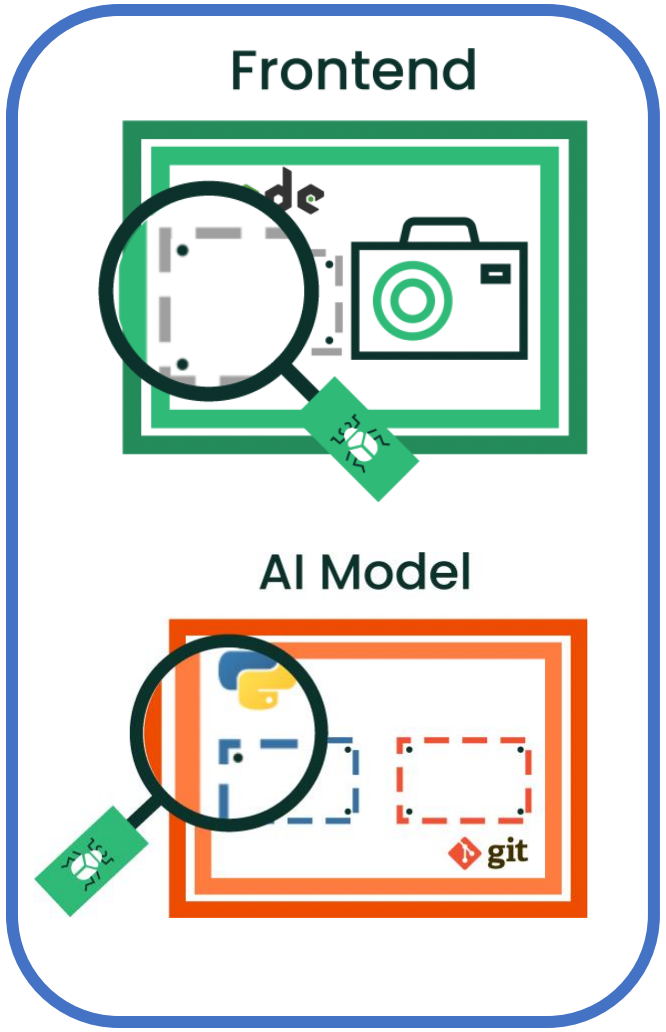
- 基于行为的零信任
- CI/CD集成 & 准入控制
- 数据丢失预防和WAF（Web应用防火墙）
- 运行时漏洞扫描
- 合规性 & 审计
- 端点/主机安全
- 多集群管理

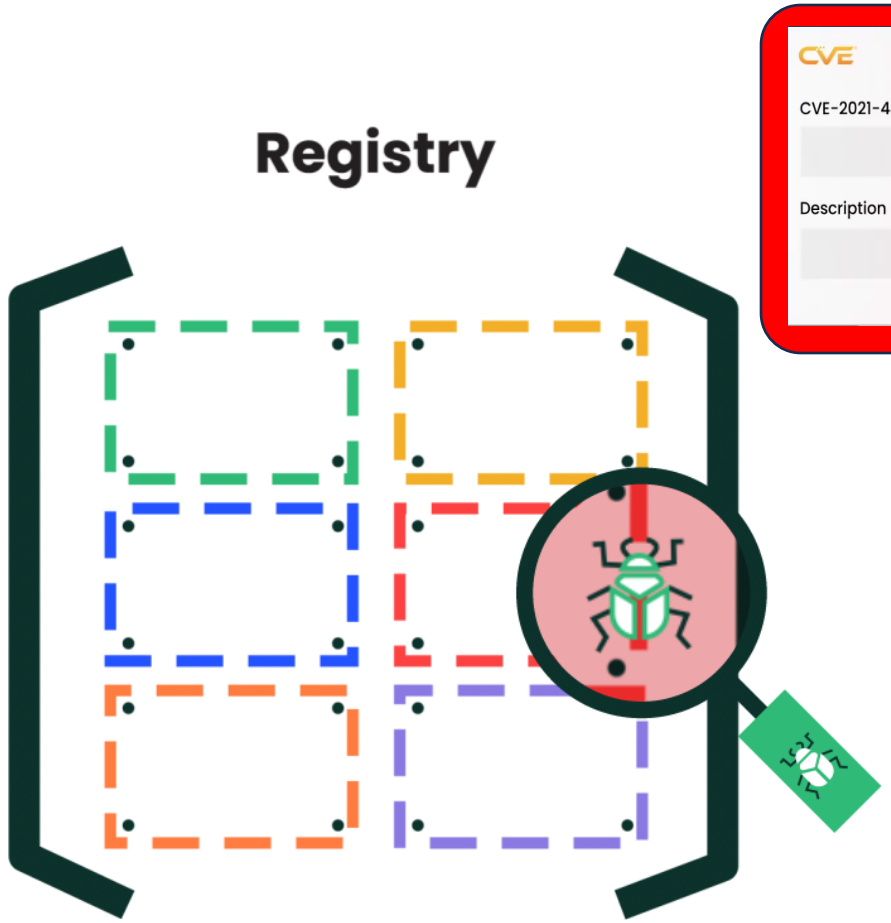
https://github.com/neuvector/neuvector

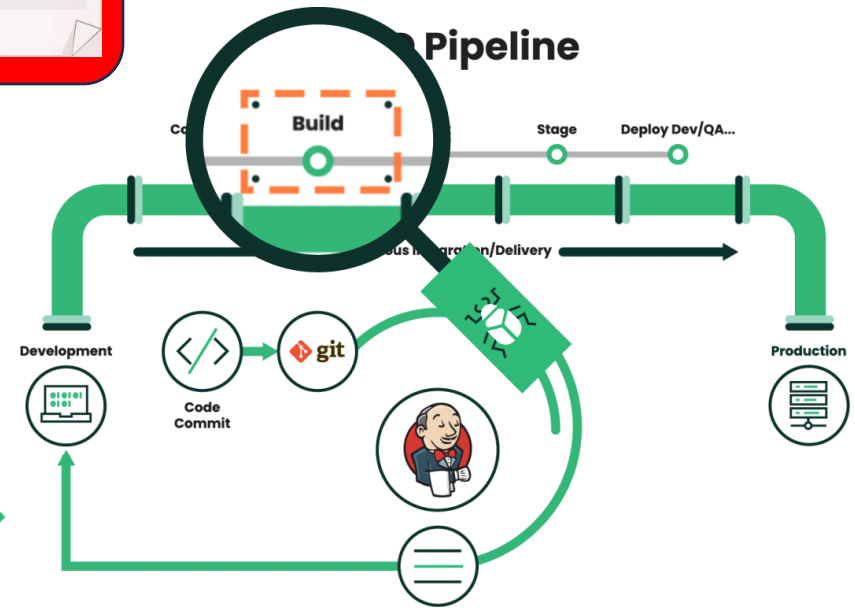
NeuVector
BY SUSE

防御已知威胁

Protecting against the Known
Scanning for Vulnerabilities

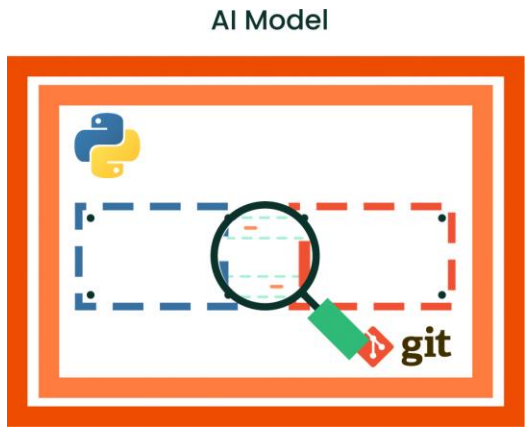


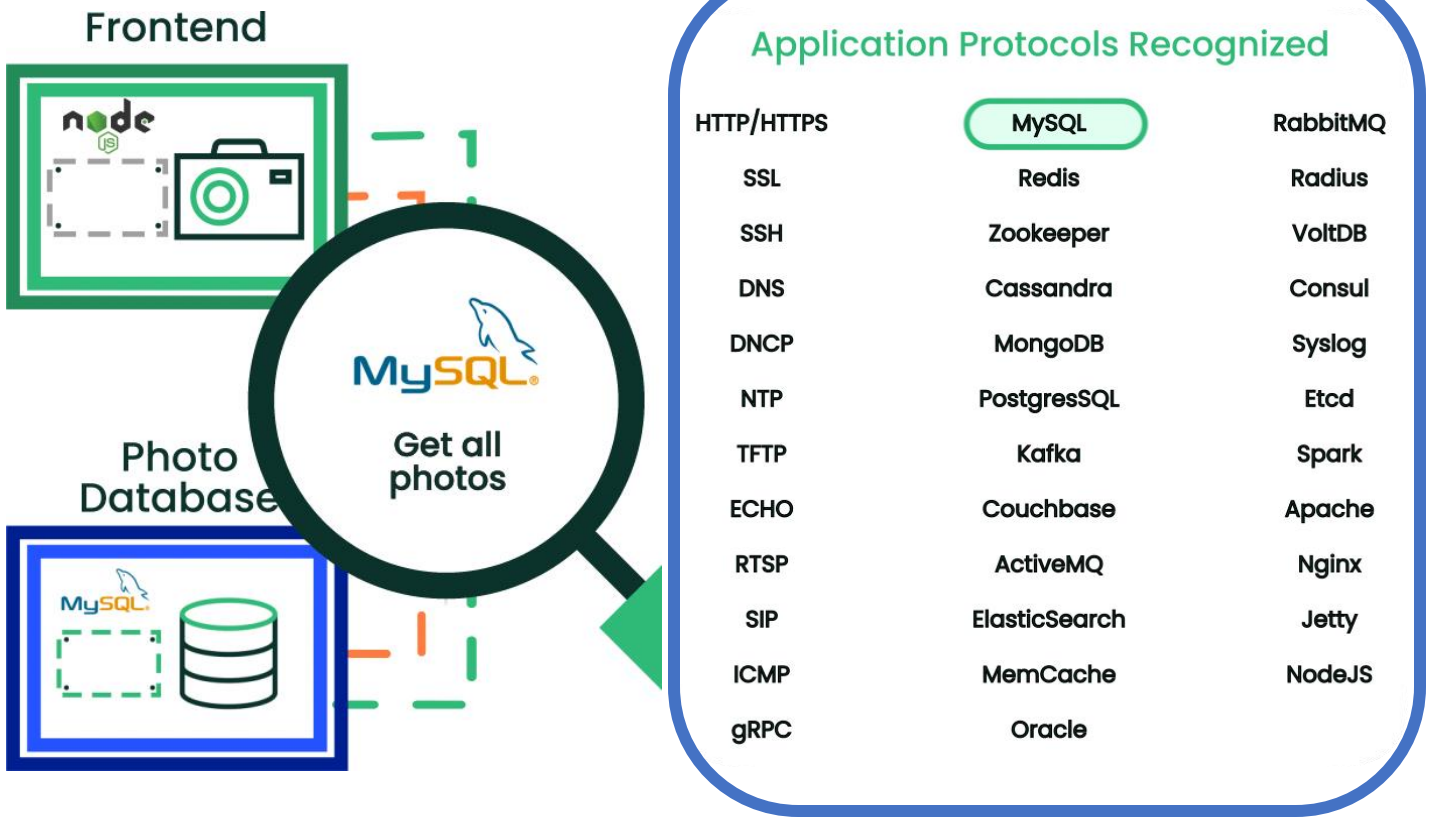




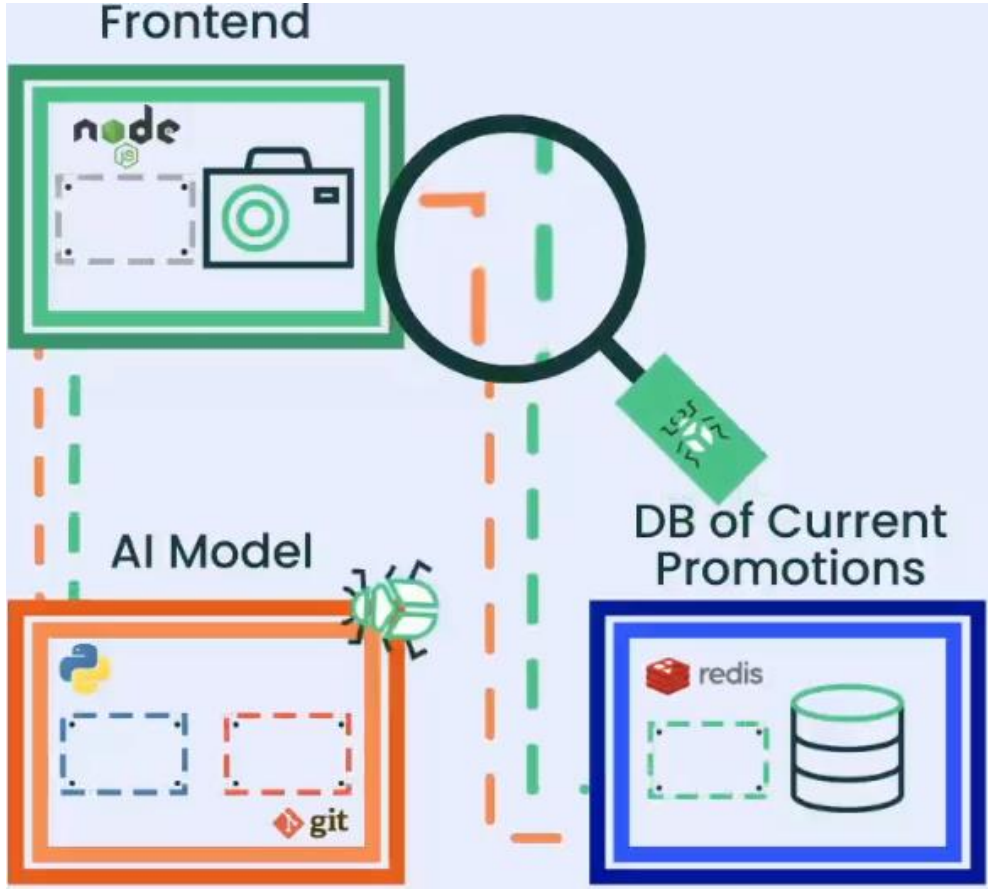
防御已知威胁
深度数据包检查

前端 -> AI 模型 - 端口 5000
互联网 -> 前端 – 端口 80





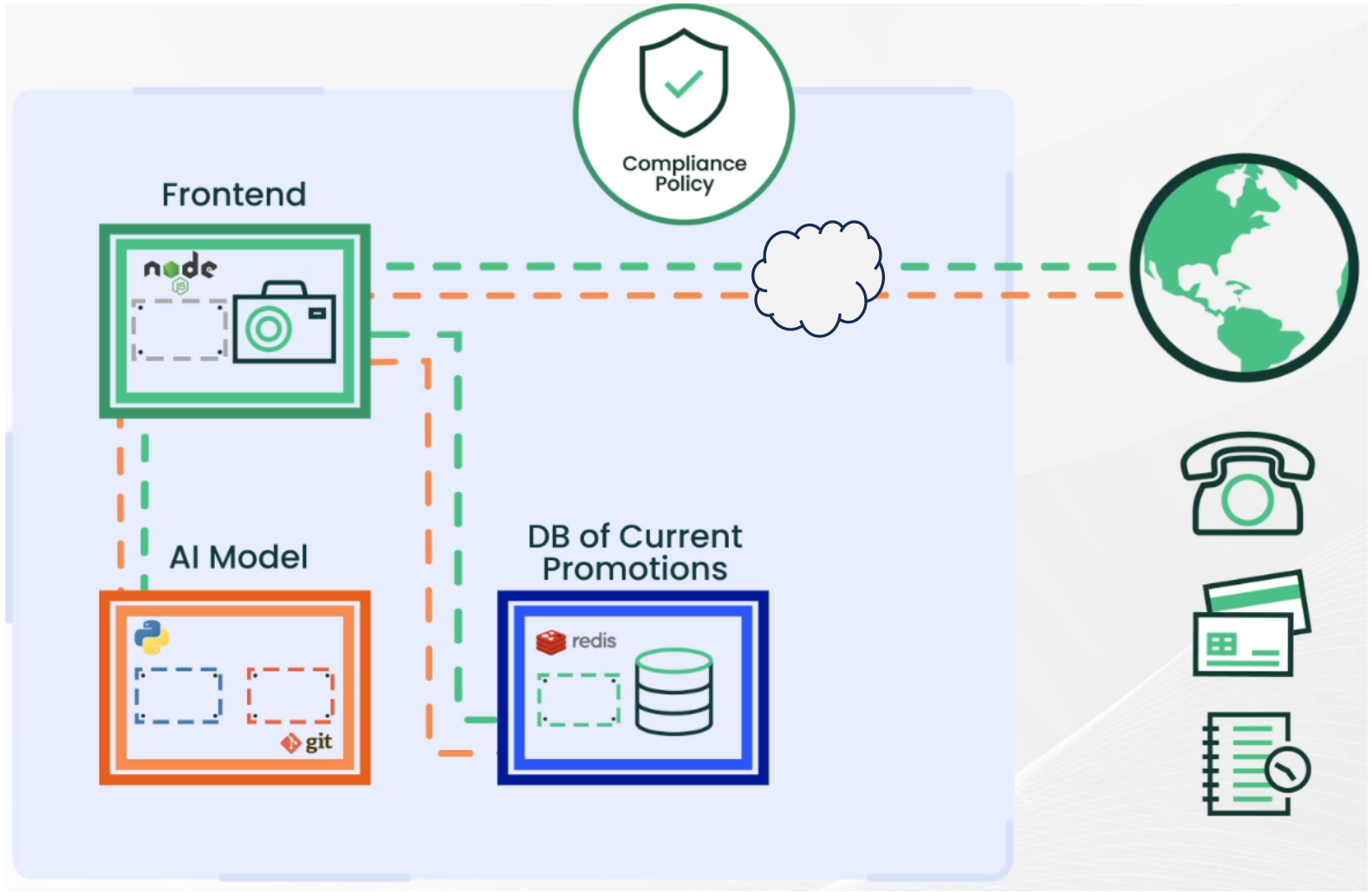
防御已知威胁
深度数据包检查



Automatically Detected Threats

SYN Flood	DNS Buffer Overflow
TCP Split Handshake	ICMP Tunneling
Detect SSH1, 2, or 3	Apache Struts RCE
HTTP Neg Content	Cipher Overflow
TCP small window	IP Teardrop
DNS Zone Transfer	DNS Flood DDoS
SQL Injection	SSL Heartbleed
TCP Small MSS	MySQL Access Deny
ICMP Flood	DNS Null Type
Ping Death	DNS Tunneling
Detect SSl TLS v1.0	K8's MitM
HTTP Smuggling	CVE-202-8554

防御已知威胁
深度数据包检查



自动化云原生应用的零信任

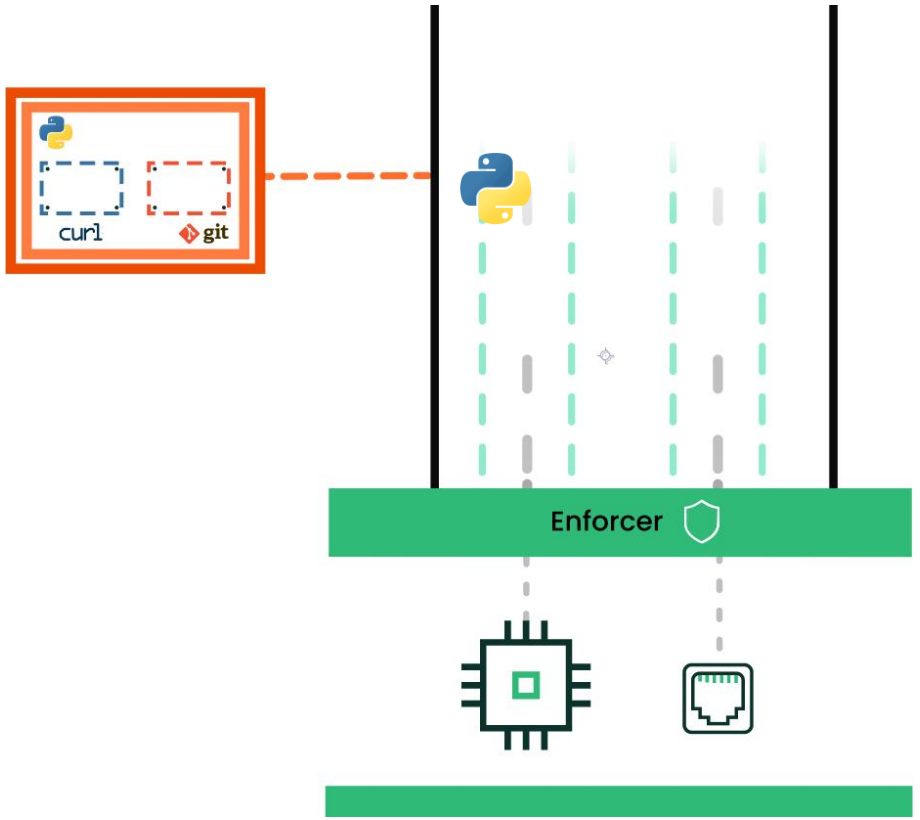
防御未知威胁
云原生应用的零信任

Discovery Mode

识别应用行为（学习模式）

进程执行

网络访问



应用运行：

- AI 模型
  - Python
  - Git
- 照片数据库：
  - MySQL

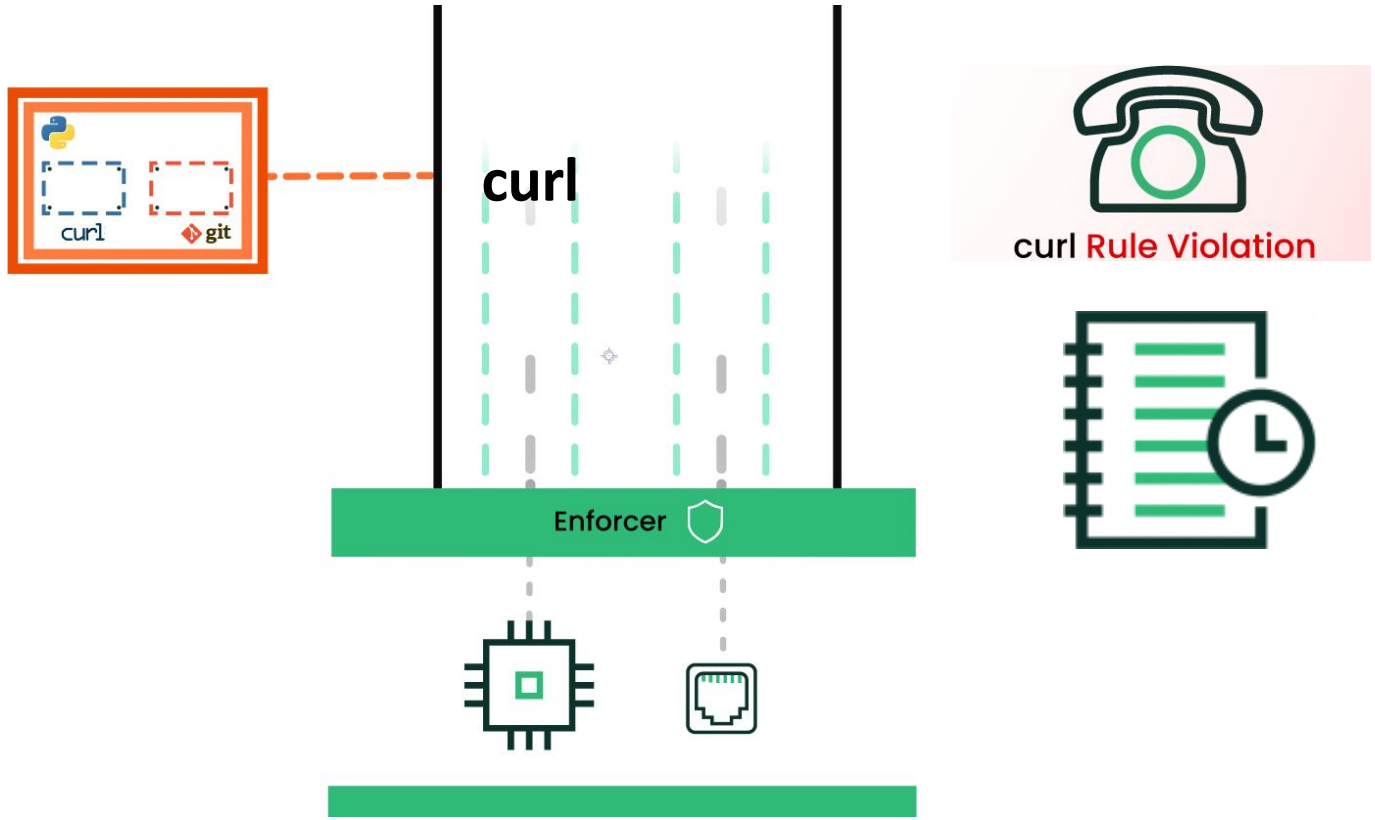
网络流量

- AI 模型 -> 照片数据库
  - Mysql
- AI -> 前端
  - 5000

防御未知威胁
云原生应用的零信任

Monitor Mode

对任何异常的应用行为发出警报。



应用运行：

- AI 模型
  - Python
  - Git
- 照片数据库：
  - MySQL

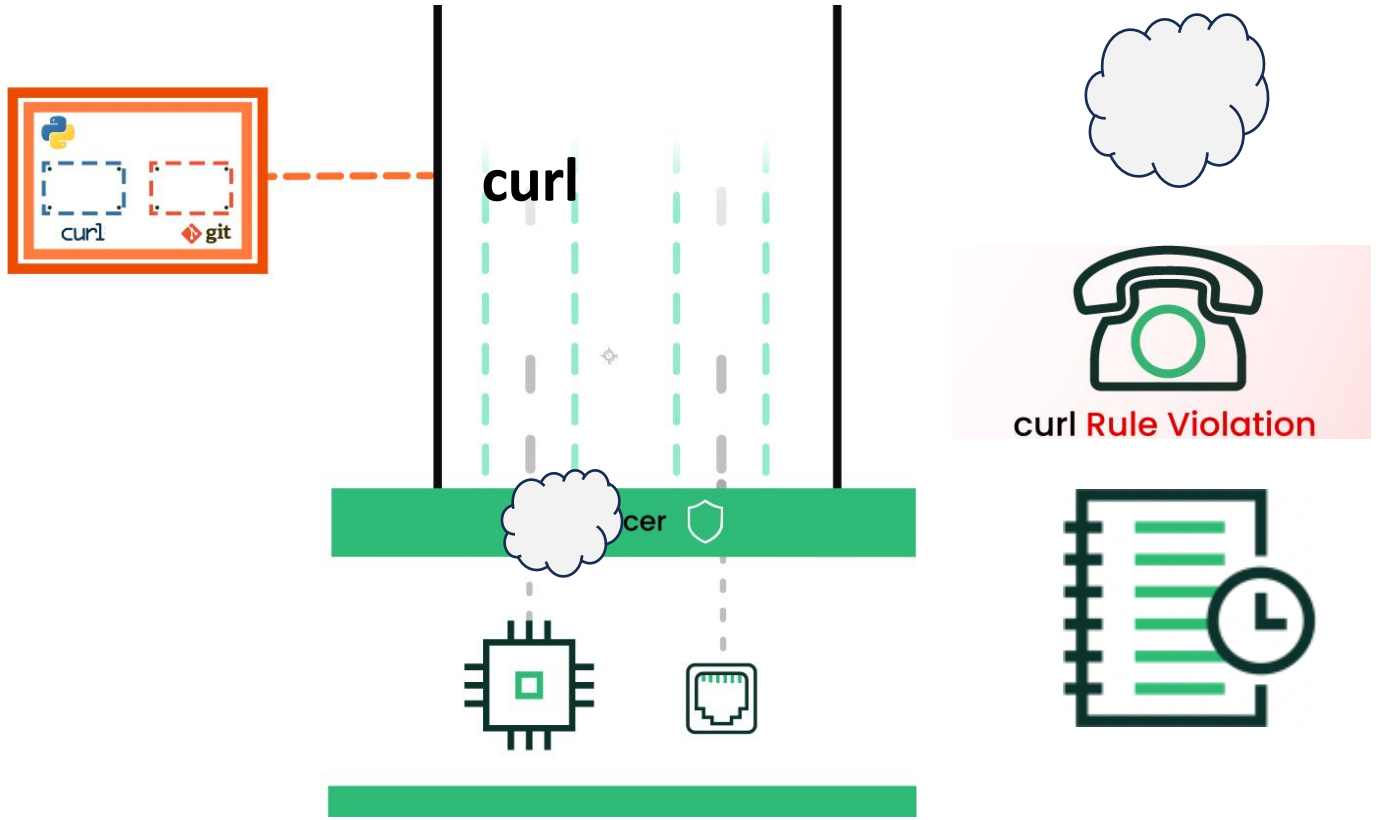
网络流量

- AI 模型 -> 照片数据库
  - Mysql
- AI -> 前端
  - 5000

防御未知威胁
云原生应用的零信任

Protect Mode

对任何异常的应用行为进行拒绝



应用运行：

- AI 模型
  - Python
  - Git
- 照片数据库：
  - MySQL

网络流量

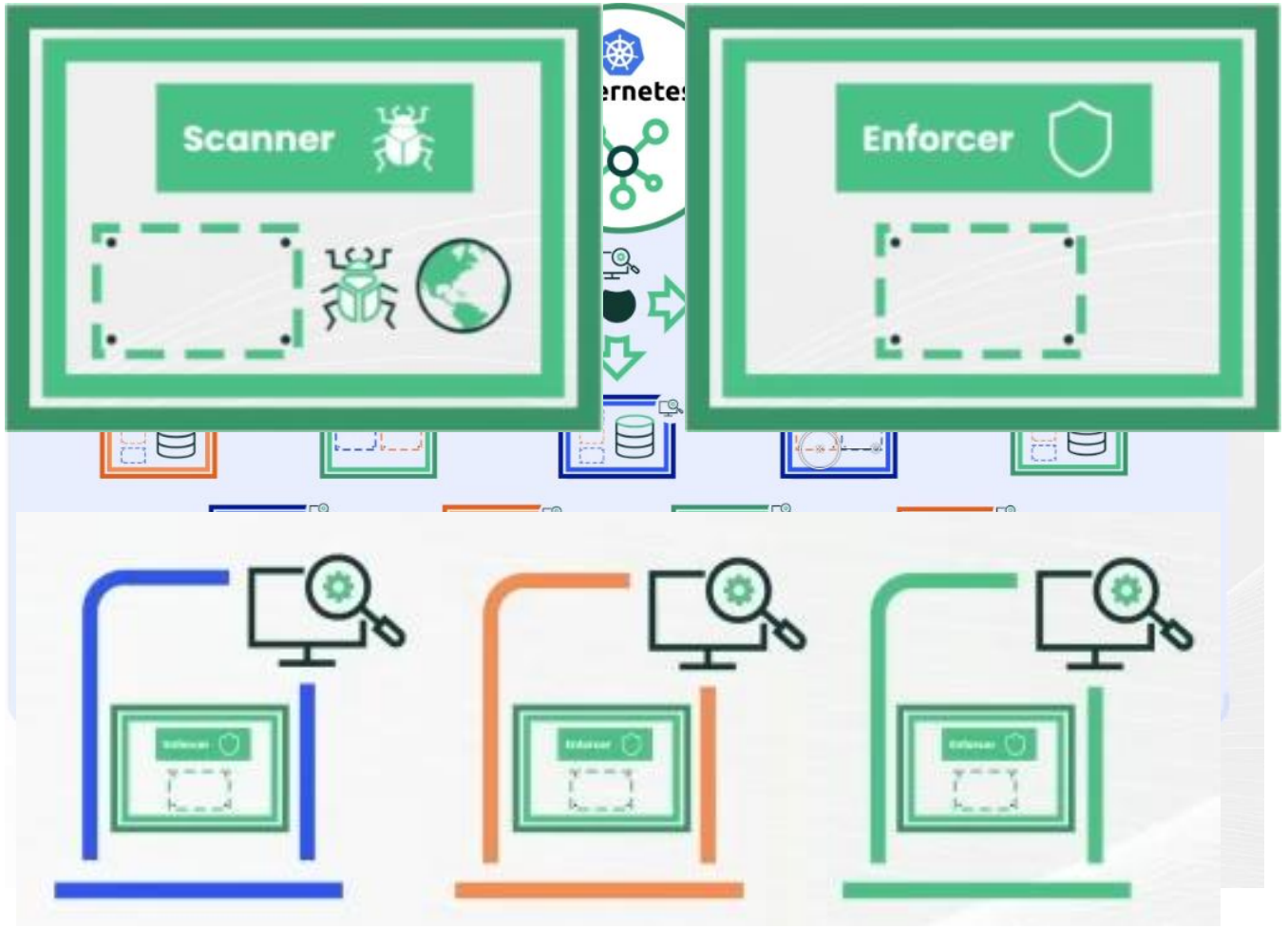
- AI 模型 -> 照片数据库
  - Mysql
- AI -> 前端
  - 5000

自动化云原生应用的零信任

KubeCon CloudNativeCon OPEN SOURCE SUMMIT China 2023

零信任网络

- 每个主机上部署的特权Pod
  - 无侧斗操作
- 作为应用程序与其源/目的地之间的中介
- 除了第3和第4层外，还能识别多个第7层协议

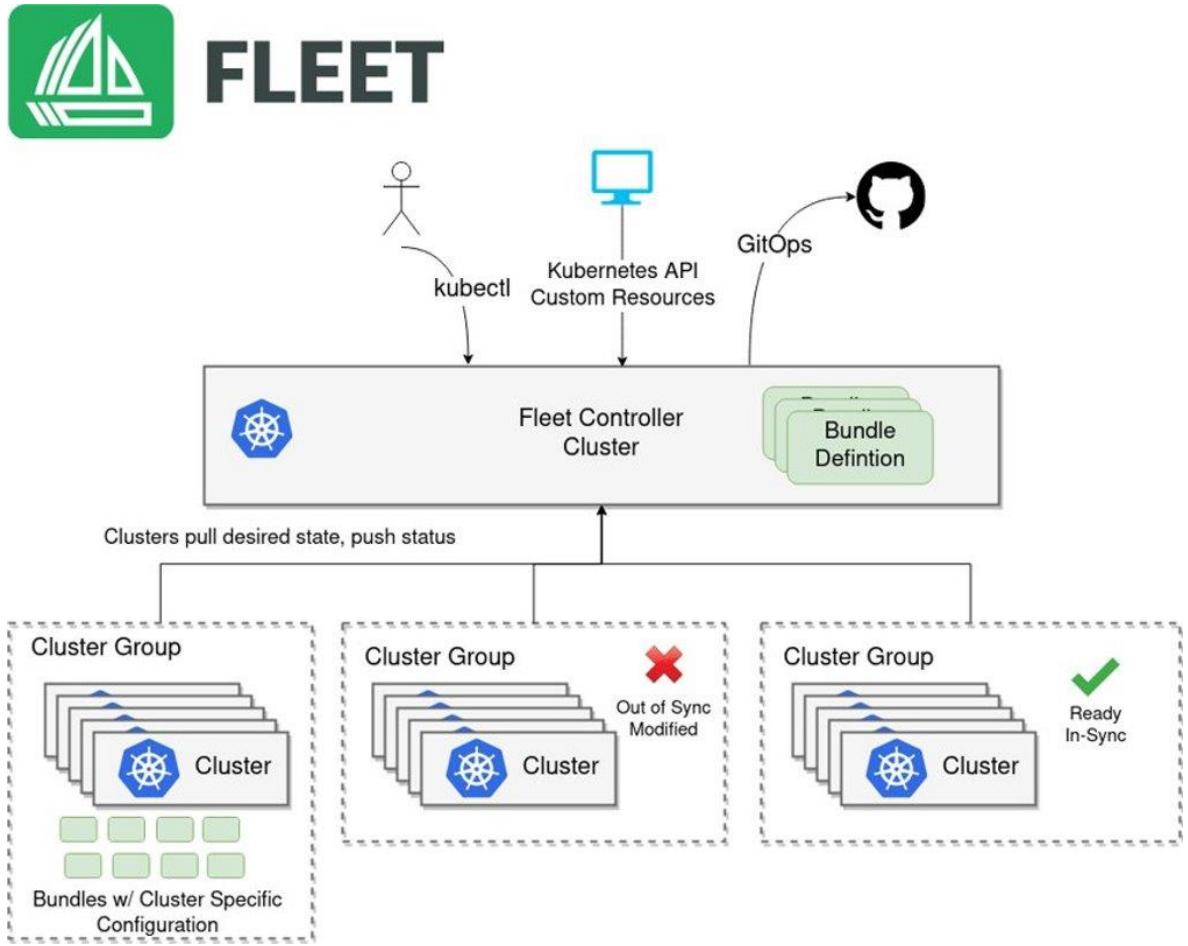


Fleet

管理Kubernetes集群的大规模应用部署

- 多集群管理
- 通过原始Kubernetes YAML、Helm图表、Kustomize或混合进行部署。
- 轻量级
- 大规模的GitOps

https://github.com/rancher/fleet



实施

使用NeuVector创建安全策略

- 学习模式
- 运行您的用例
- 监控模式
- 调整或加固
- 导出它

使用Fleet创建您的CI/CD流水线

- 配置`Fleet`
- 准备您的资源定义
- 创建存储库结构
- 将所有内容上传到仓库

演示

更新您的应用程序

- 我们的应用有一个重大更新
- 更新安全策略
- 阻止我们的第一次攻击

结论

谢谢！

源代码及更多:

- NeuVector: https://github.com/neuvector/neuvector
- Fleet: https://github.com/rancher/fleet
- 演示材料: https://github.com/SUSE-Technical-Marketing/kcknoss-2023-China

欢迎随时在其中一个地方与我们见面  SUSE 展位!


问答