Face the challenge,Embrace the best practice

EISS-2021
企业信息安全峰会

北京站

2021.05.14
BEIJING，CHINA

安世加

云原生安全：

基于 DevOps 基础设施的 Web 漏洞扫描实践

李相垚

2021.05.14

安世加

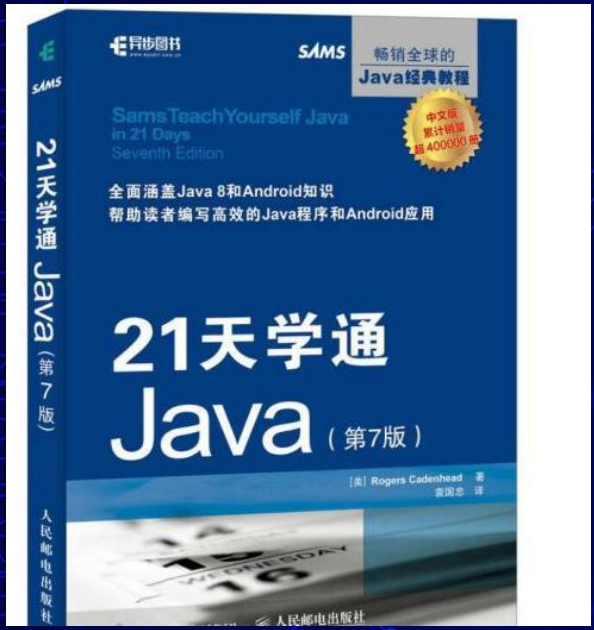
李相垚

腾讯安全平台部

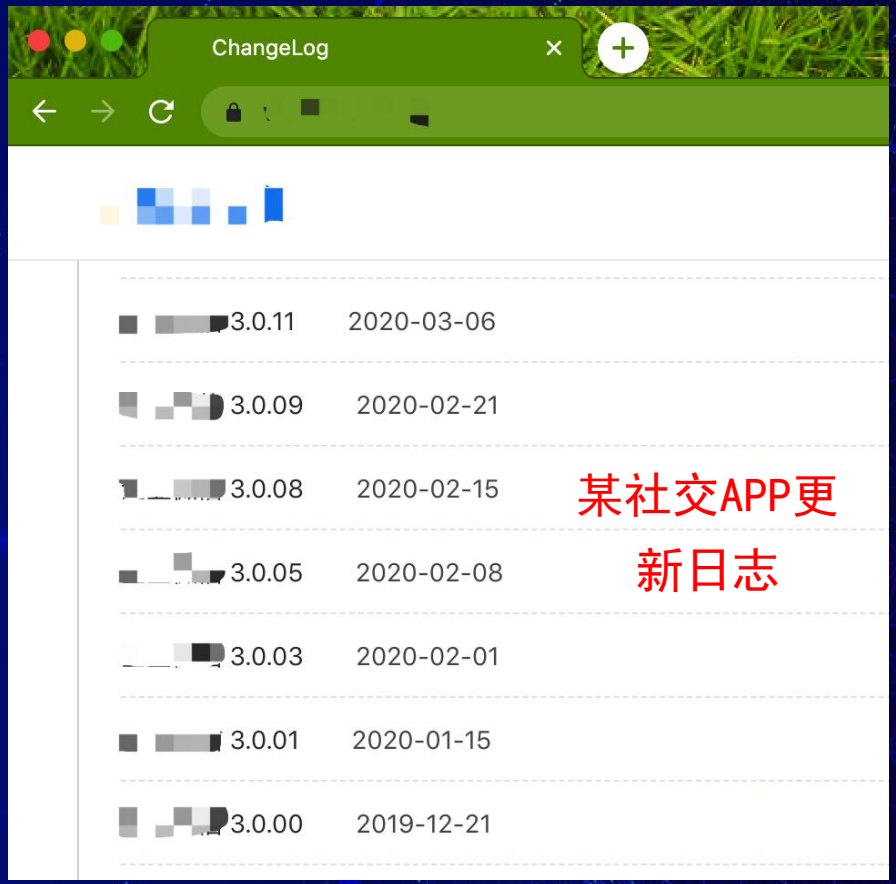
漏洞扫描产品负责人

安世加

互联网行业处处是“高效”

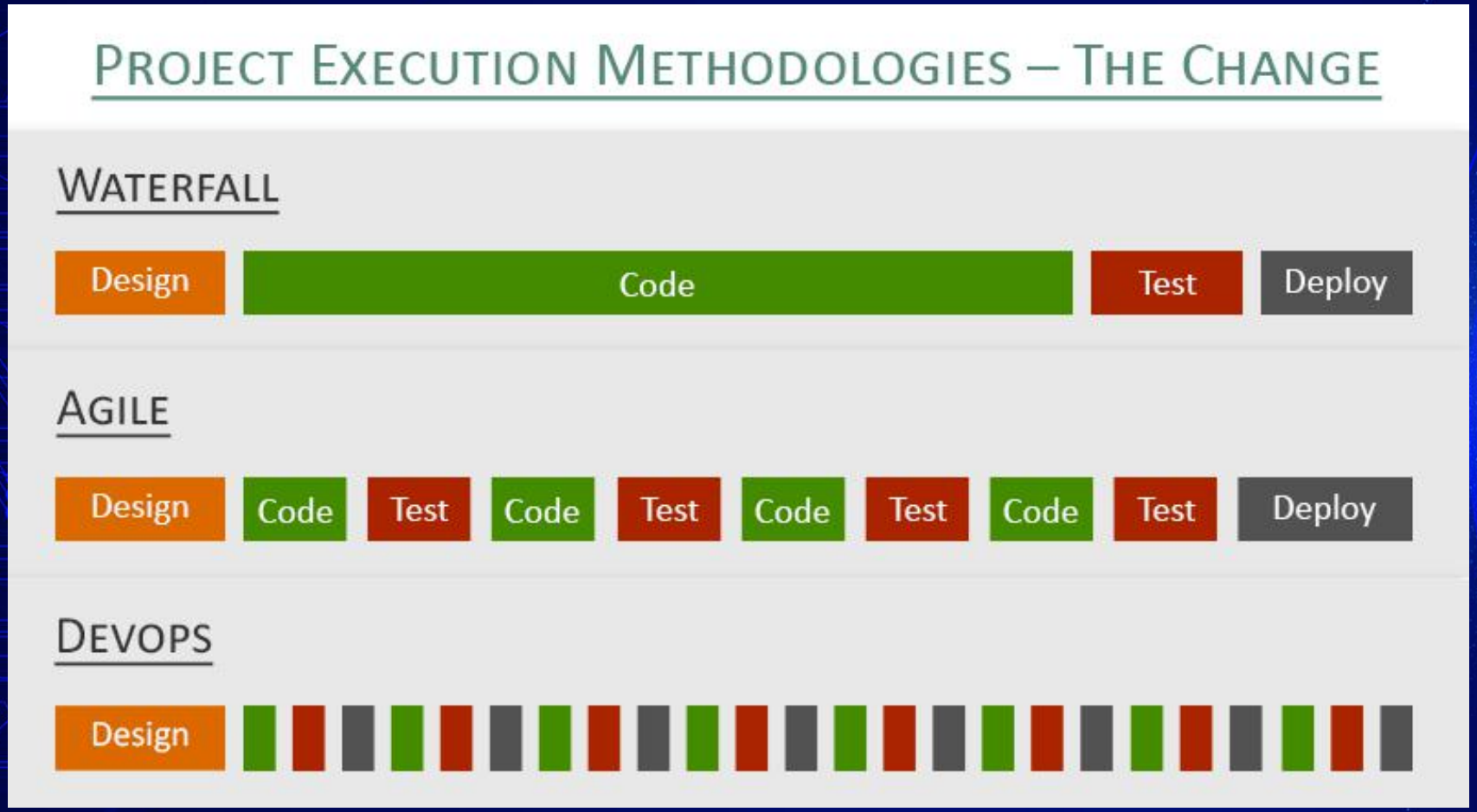

SAMS
畅销全球的
Java经典教程
SamsTeachYourself Java
in 21 Days
Seventh Edition
全面涵盖Java 8和Android知识
帮助读者编写高效的Java程序和Android应用
21天学通
Java（第7版）
[美] Rogers Cadenhead 著
人民邮电出版社


一周学会PHP入门教学视频


ChangeLog
3.0.11 2020-03-06
3.0.09 2020-02-21
3.0.08 2020-02-15
3.0.05 2020-02-08
3.0.03 2020-02-01
3.0.01 2020-01-15
3.0.00 2019-12-21
某社交APP更新日志


1小时快速搭建一个网站
分类专栏：
快速建站

研发模式的升级令产品迭代愈加频繁



瀑布模型

敏捷模型

DevOps 模型

速度越来越“快”，安全怎么办

安世加

新的安全理念诞生 —— DevSecOps

1. 培训	2. 需求	3. 设计	4. 实施	5. 验证	6. 发布	7. 响应
核心安全培训	确认安全要求	确认安全要求	使用批准的工具	动态分析	事件响应计划	执行事件响应计划
	创建质量门限/BUG 栏	分析攻击面	弃用不安全的函数	模糊测试	最终安全评审	
	安全和隐私风险评估	威胁建模	静态分析	攻击面评审	发布存档	

- ✓ 人工成本高
- ✓ 由安全团队负责

- ✓ 高度自动化
- ✓ 所有角色共同参与

安世加

上线前漏洞扫描是 DevSecOps 重要一环

上线前扫描为什么重要?

- 漏洞发现时机早
- 修复效率高
- 扫描的范围全面

安世加

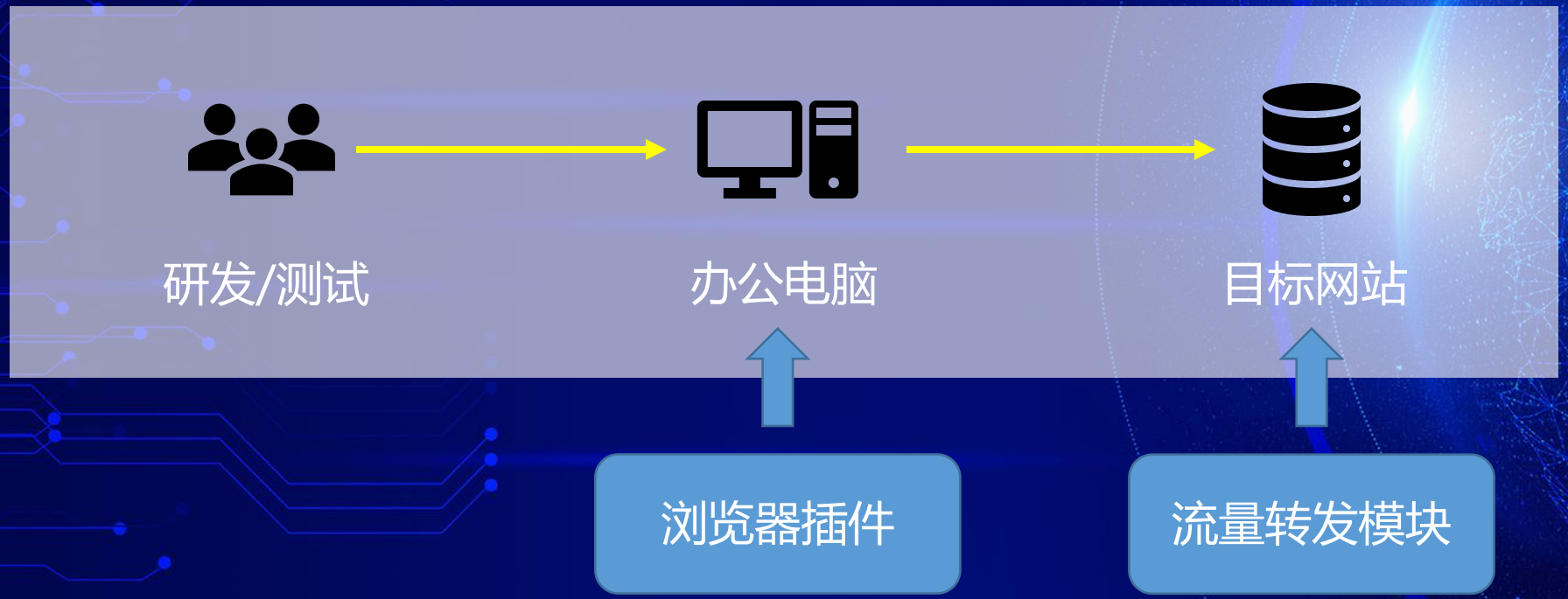
上线前漏洞扫描实施方式 —— 从主动到被动

扫描模式	参与者	耗时	优势	缺点
单条提交	安全	1-3d	能用	收集成本高
爬虫	测试/安全	1d	只需提供入口地址	爬虫能力是瓶颈
浏览器插件	测试/安全	0.5h-2h	全面+自动	只适用于前端部分测试
被动扫描	测试	0.5h-2h	实时扫描	有一定部署成本

安世加

被动式扫描在资产覆盖和易用性上优势巨大

- **资产收集：**业务测试覆盖度 = 网站资产覆盖度
- **实施成本：**旁路采集，侵入性低



- **执行效果：** **80%+**业务使用 nginx 插件接入， **60%+**漏洞由被动扫描发现

被动式扫描不断遭受业务挑战

01 部署成本偏高

02 测试环境负载不稳定

03 测试环境写入脏数据

04 影响开发人员调试

安世加

被动式扫描不断遭受业务挑战

- **核心矛盾**：争抢环境，无法调和
  - 测试环境扩容
  - 接口加白
  - 便捷地停扫入口

安世加

业务全面“上云”，注重研效提升

技术变革

业务上云

研效提升

安全变革
的机会

标准化部署

容器化技术

自动化流程

安世加

云原生被动式扫描方案 —— 有效地采集流量

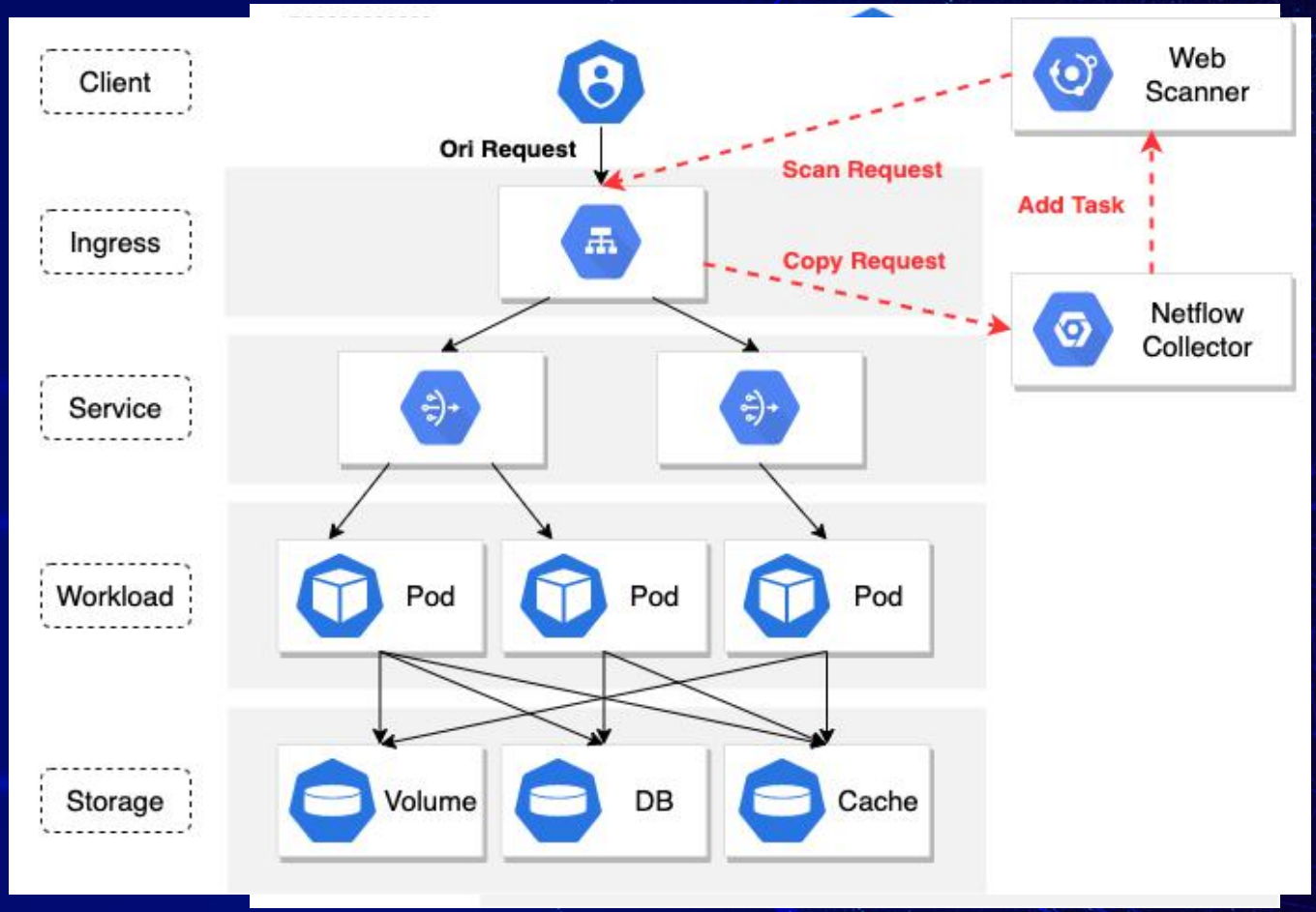
➢ **矛盾点①：流量采集难**

- Pods（容器内）
- Services（集群路由）
- Ingress（外部访问网关）

Ingress 使用覆盖度

业务应用侵入性

https 解密流量



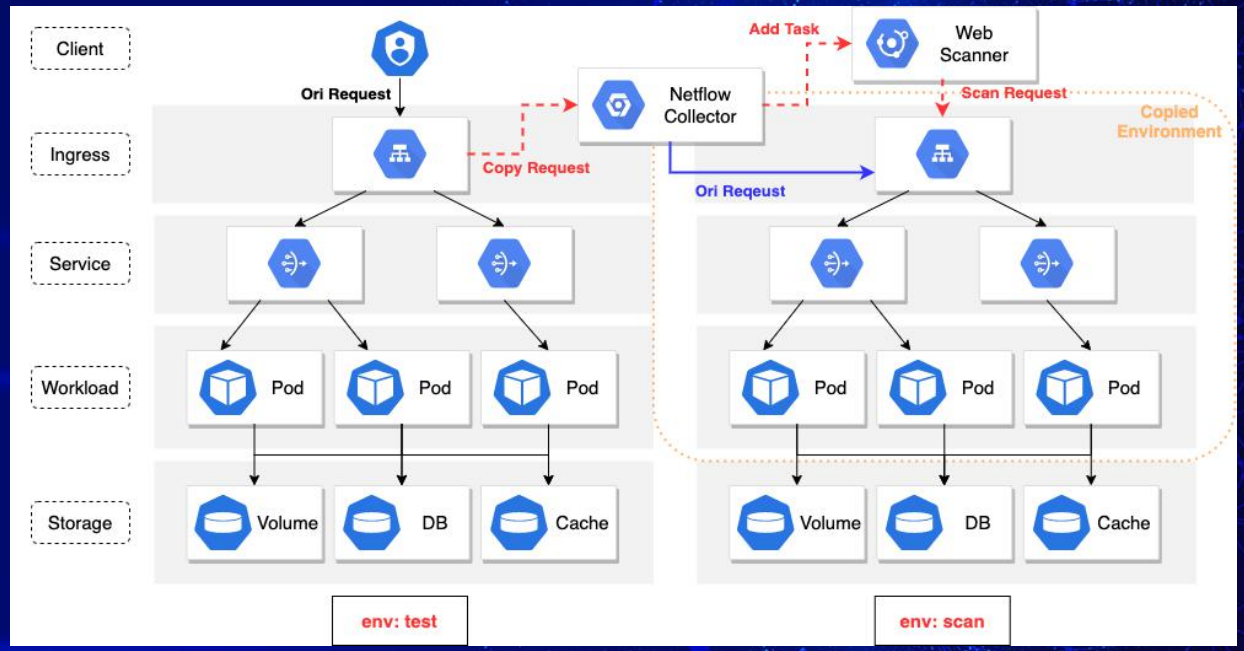
✓ **核心优势：**借助云原生基础设施，节省流量采集开发&维护工作

云原生被动式扫描方案 —— “专属”扫描环境

- **矛盾点②**：环境争抢

  TKE -> 快速扩容 -> 环境复制

建立扫描专用环境



✓ **核心优势**：借助云原生基础设施，快速获得独立的业务环境

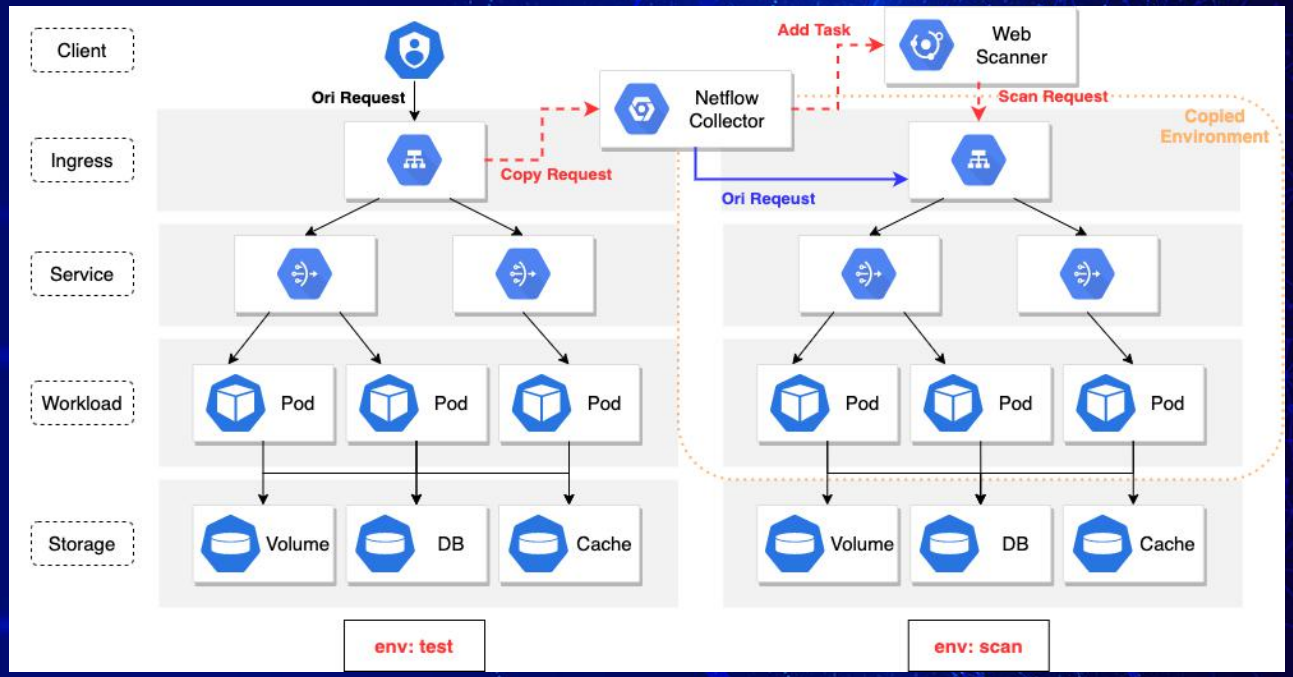
关键点

- 环境创建时机
- 环境一致性

安世加

云原生被动式扫描方案 —— 还能做些什么

- **提升扫描效率**
  - 合理扩容 → 提升扫描速度
- **探索 IAST**
  - 独立环境 → 部署监听程序



Thank you

安世加

专注于安全行业，通过互联网平台、线下沙龙、培训、峰会、人才招聘等多种形式，致力于创建亚太地区最好的甲乙双方交流、学习的平台，培养安全人才，提升行业整体素质，助推安全生态圈的健康发展。

官方网站：
https://www.anshijia.net.cn
微信公众号：asjeiss

安世加