云原生社区 Cloud Native Community　火线　CODING CLOUD DEVELOPMENT

云原生社区 meetup
第七期·深圳站

使用IAST构建高效的DevSecOps流程

董志勇（火线平台-洞态产品负责人）

CLOUD NATIVE COMPUTING FOUNDATION　THE LINUX FOUNDATION　Broadview® www.broadview.com.cn　腾讯游戏 Tencent Games

为什么要做安全测试？

国家法律法规的出台

《中华人民共和国网络安全法》
《中华人民共和国网络隐私保护法》
《中华人民共和国数据安全法》
《中华人民共和国个人信息保护法》

...

为什么要做安全测试？

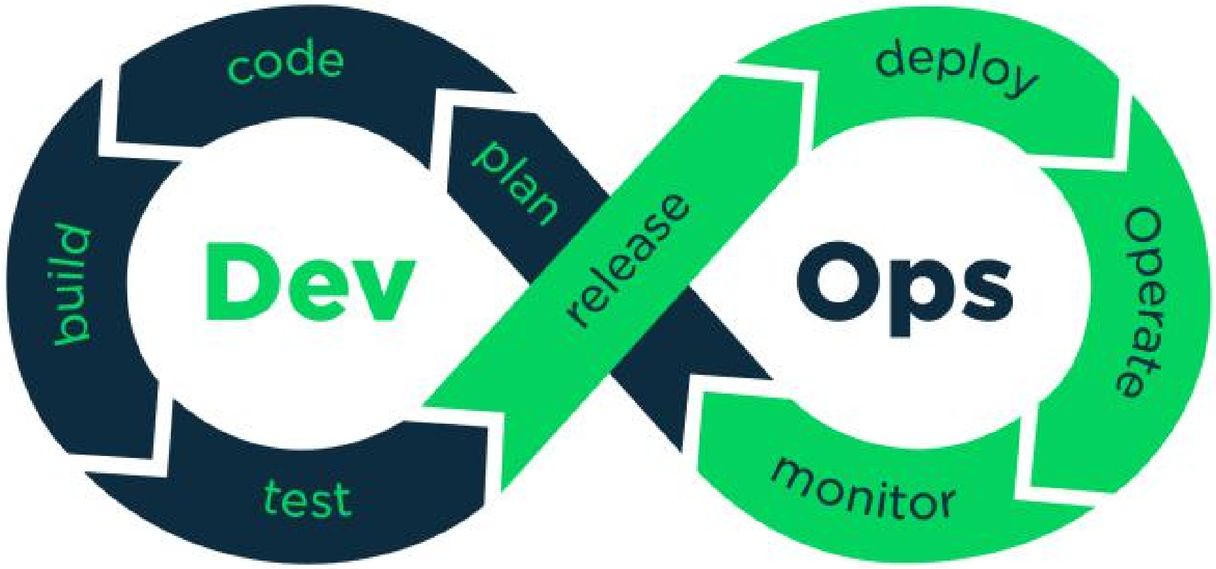
- 勒索软件：2017年“永恒之蓝”
- 数据泄漏：2020年以色列640万选民数据泄漏
- 服务器被入侵等等

网络攻击频发

DevOps前的安全测试

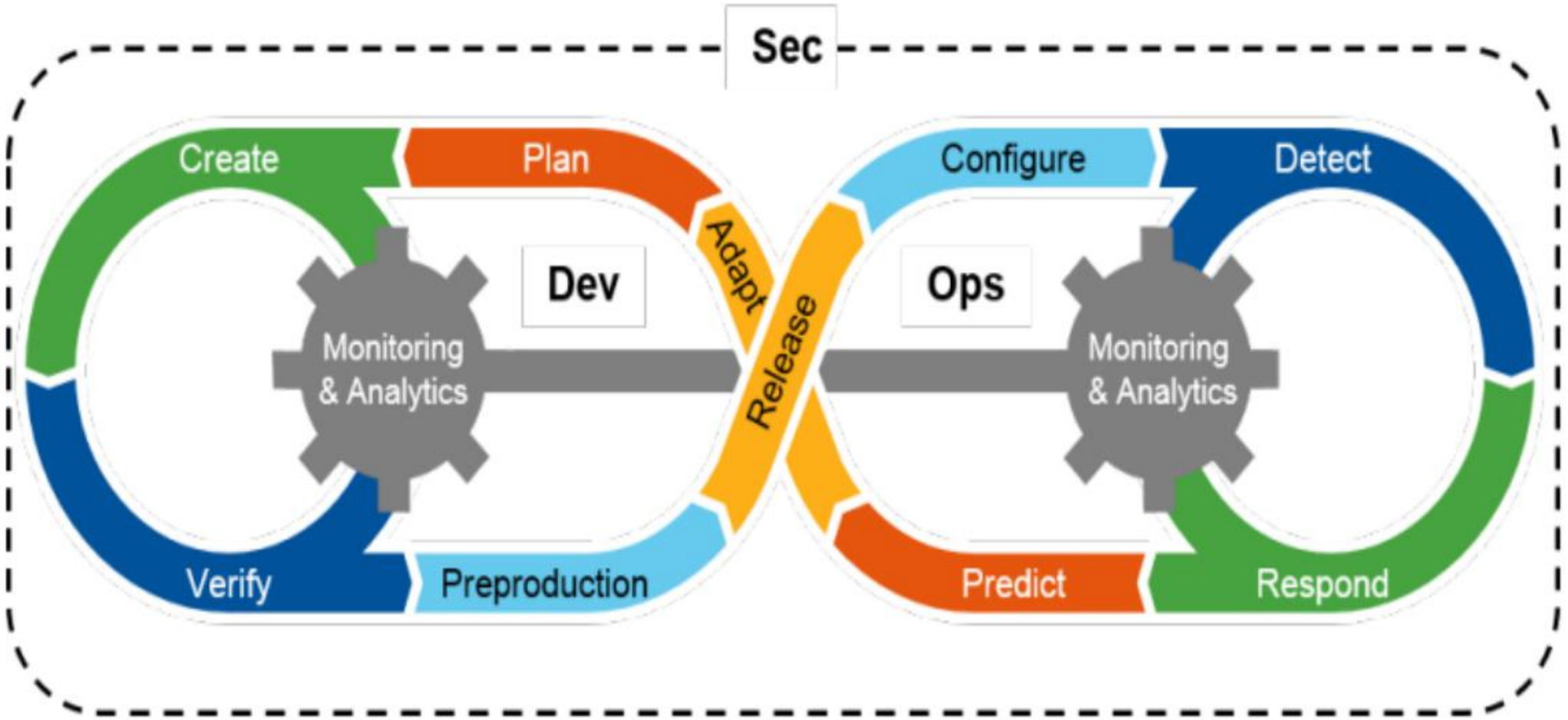
迭代速度慢、安全测试任务密度小

DevOps带来的新挑战



DevOps提高了企业的生产效率，实现了应用的快速迭代，但带来了待上线应用的数量与安全测试人员数量的严重不对等。**为了满足企业的生产效率需求，必须有同样高效的安全工具来解决安全测试人员数量不足给生产效率带来的影响。**

DevSecOps



Source: Gartner (September 2016)

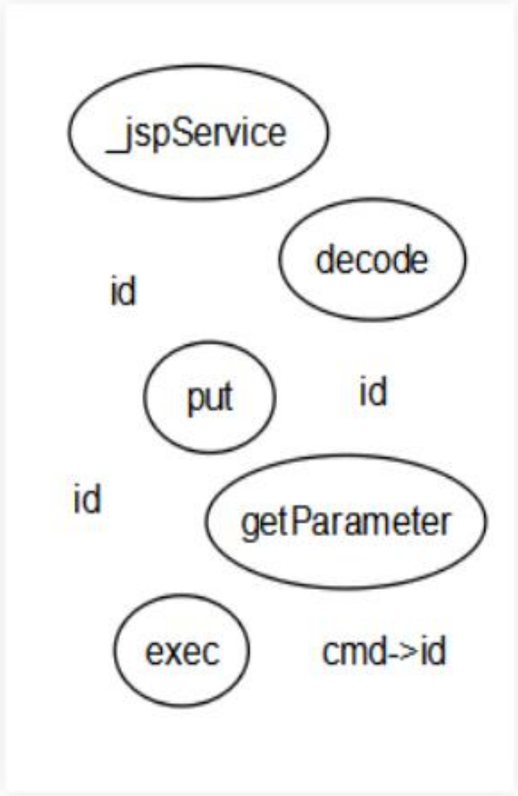
什么是IAST呢？

IAST全称Interactive Application Security Testing, 译为：“交互式应用程序安全测试”。

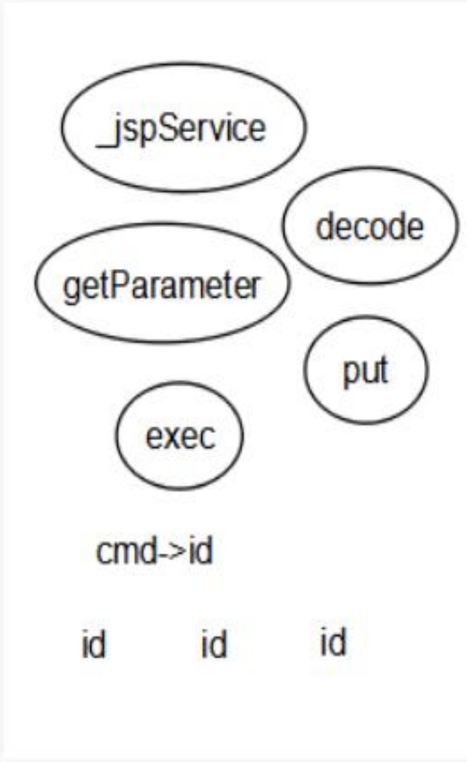
它通过Agent来监控应用程序运行时的函数执行情况，采集相关数据，并与服务端进行实时交互，从而**高效**、**准确**的**识别**出应用程序中的**漏洞**，同时可准确的**定位到**漏洞所在的**文件**、**行数**、**方法及参数**，**方便**开发团队及时的**修复漏洞**。

IAST检测原理

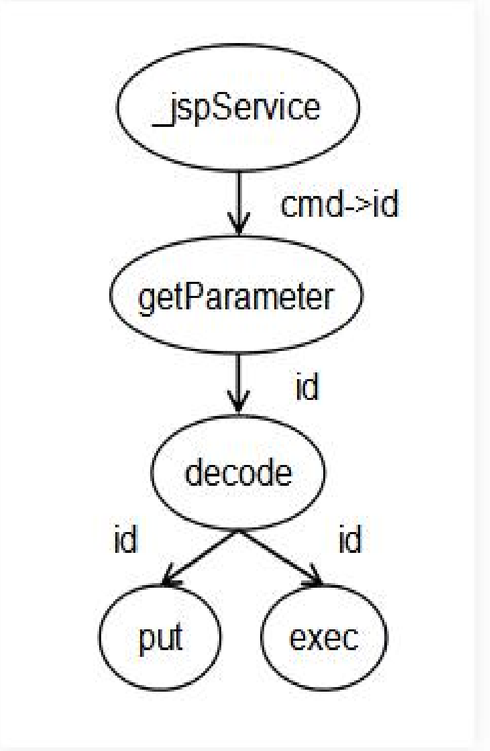
不可信数据采集



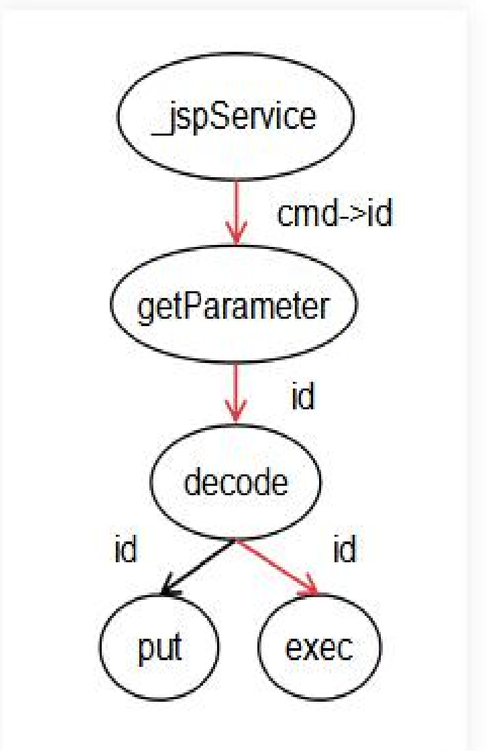
不可信数据预处理



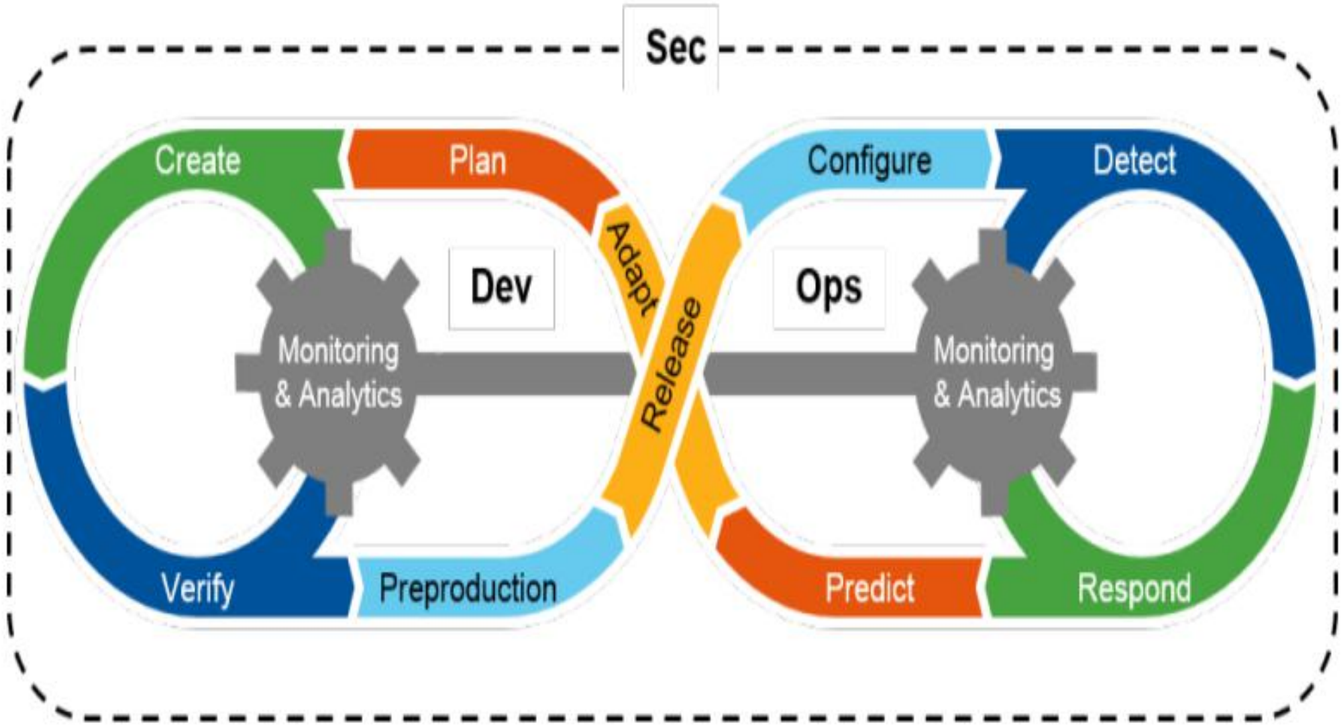
不可信数据传播图



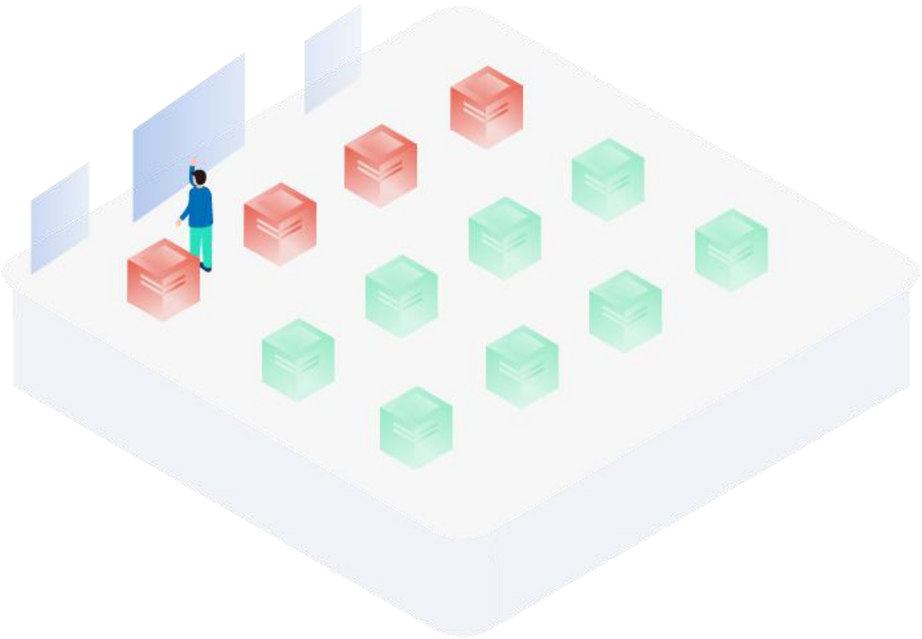
数据调用链路查找



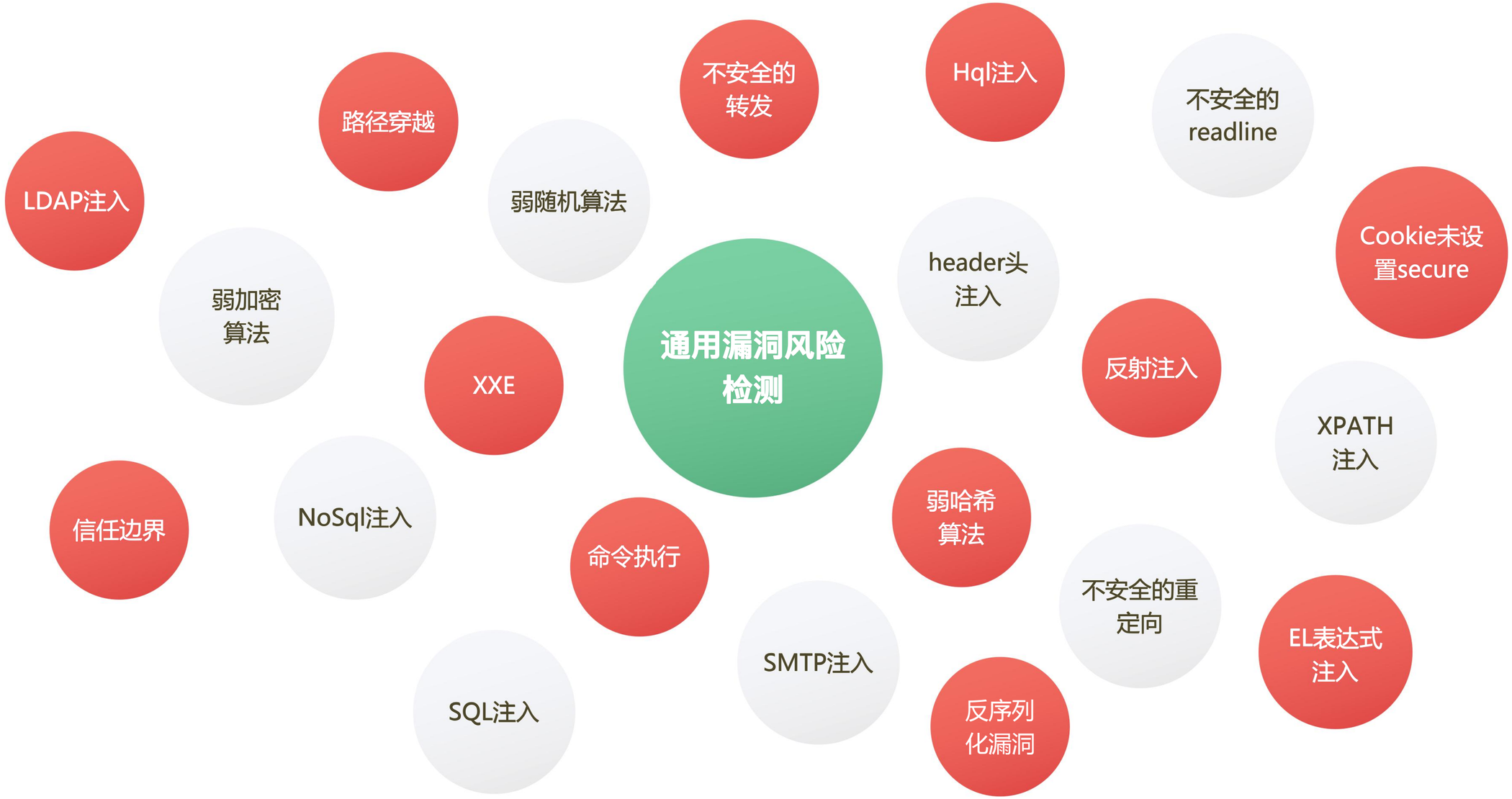
IAST+DevSecOps



Source: Gartner (September 2016)



为什么选择洞态IAST



为什么选择洞态IAST

依赖组件的供应链风险检查

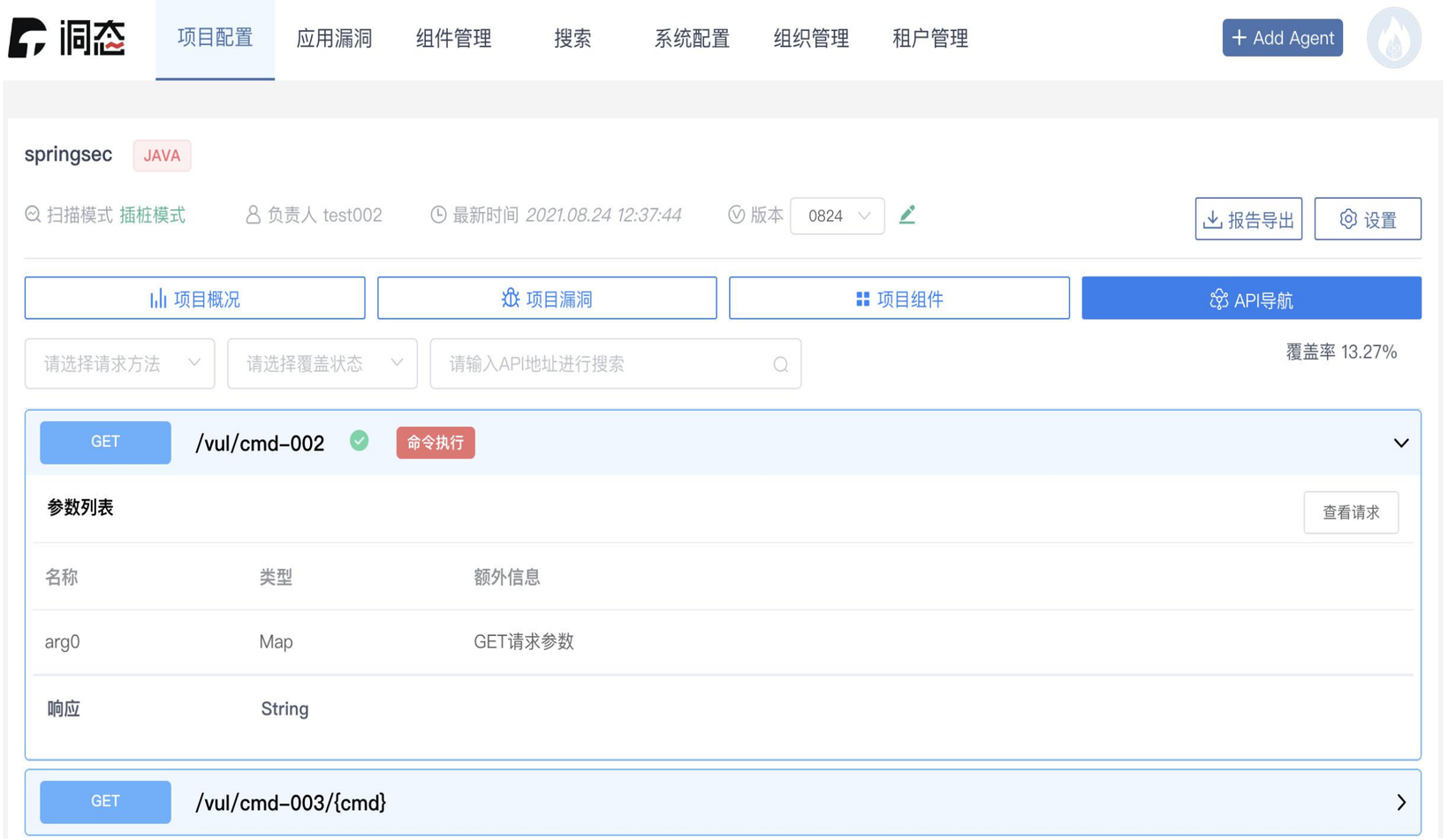
为什么选择洞态IAST

- 传统WEB应用
- 前后端分离场景下的漏洞检测
- 验证码场景下的漏洞检测
- 数据包加密场景
- 防重放签名等场景
- 分布式架构下的漏洞检测
- 微服务架构下的漏洞检测

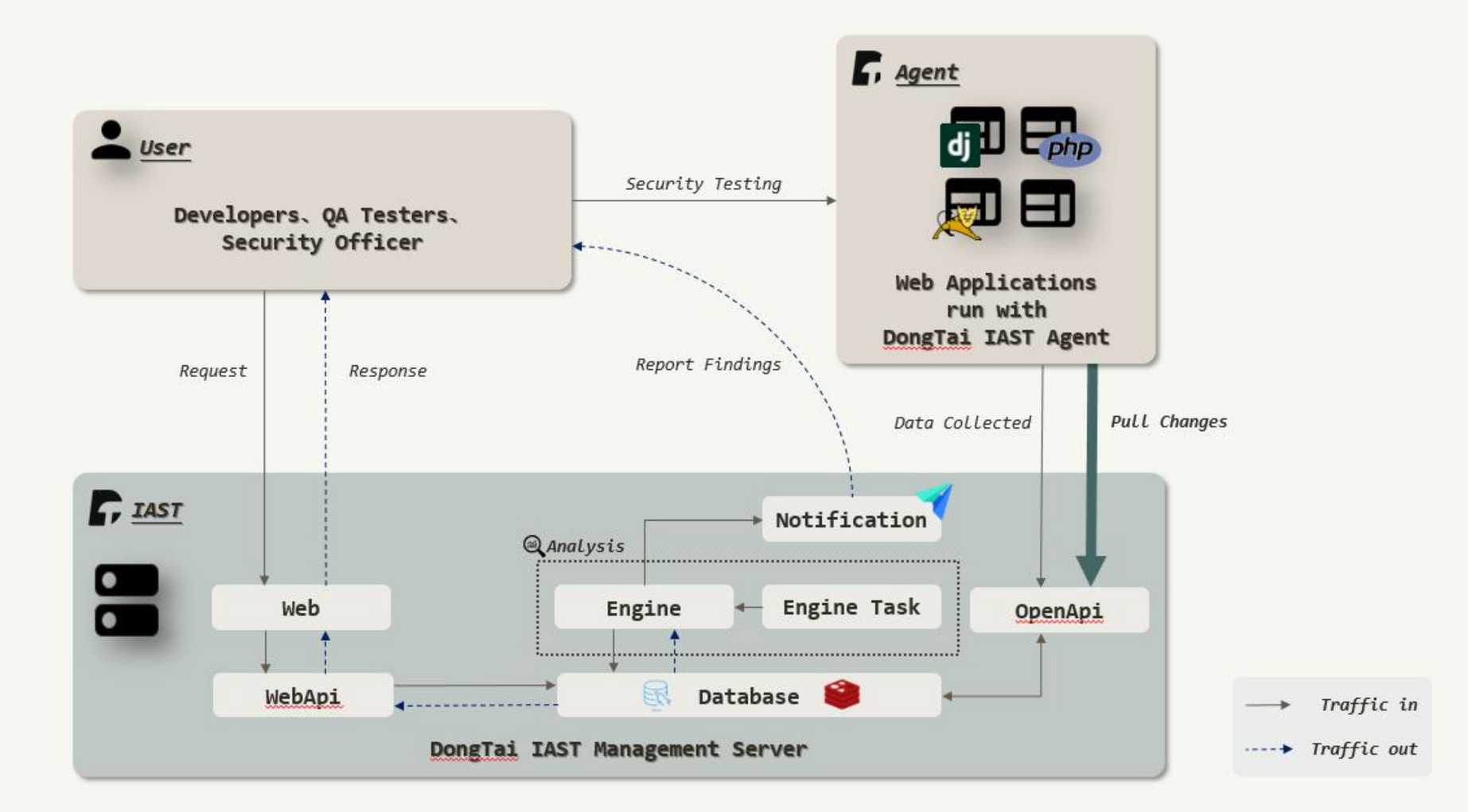
支持各种业务场景

为什么选择洞态IAST

- 类的API Sitemap，方便各部Swagger门人员查看
- 提供测试覆盖率，精确的反馈出未测试到的接口
- 准确的参数名称及数据类型，可用于直接发送HTTP请求，提高接口覆盖率



为什么选择洞态IAST

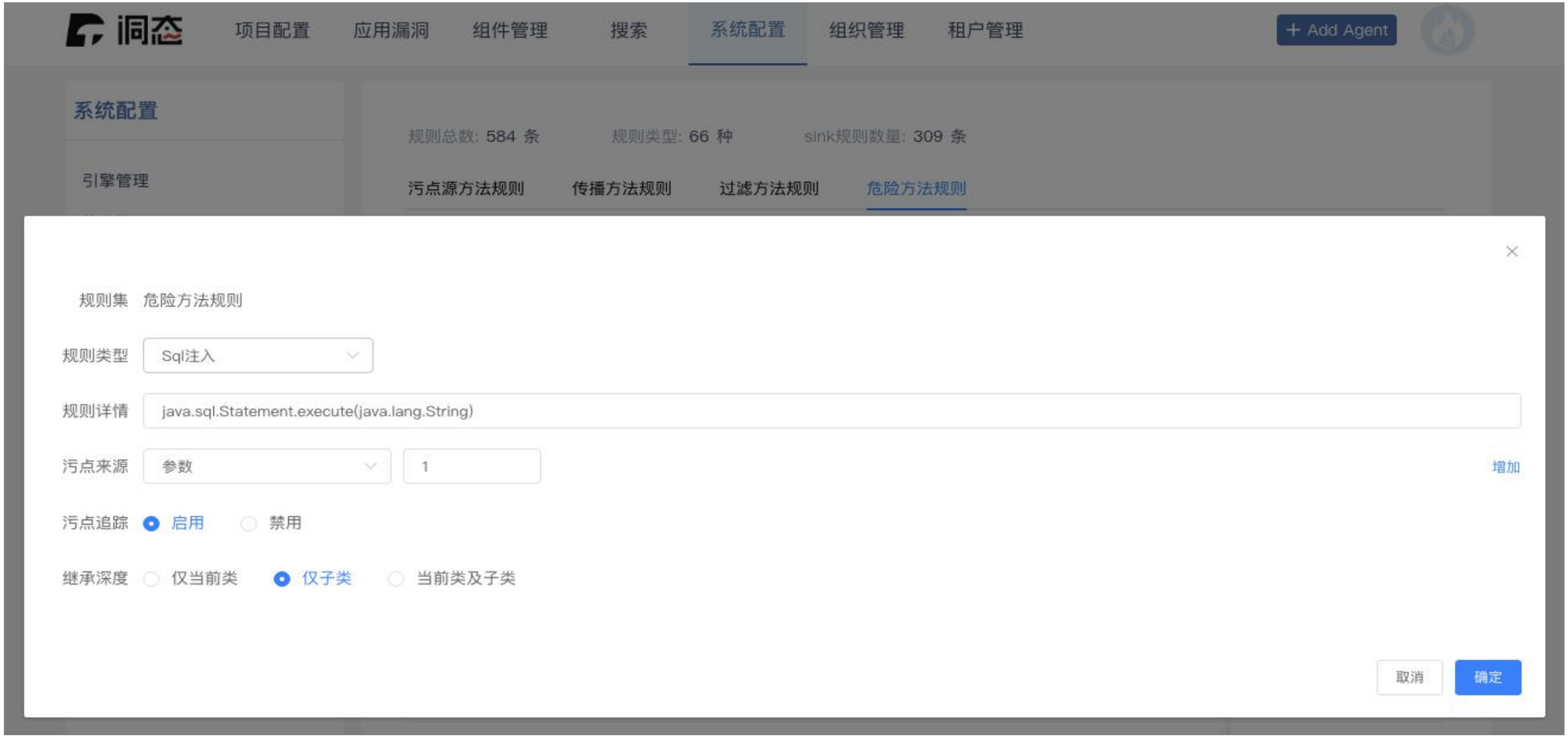


统一探针上报的数据格式、构建数据底座、利用数据分析实现漏洞的离线检测

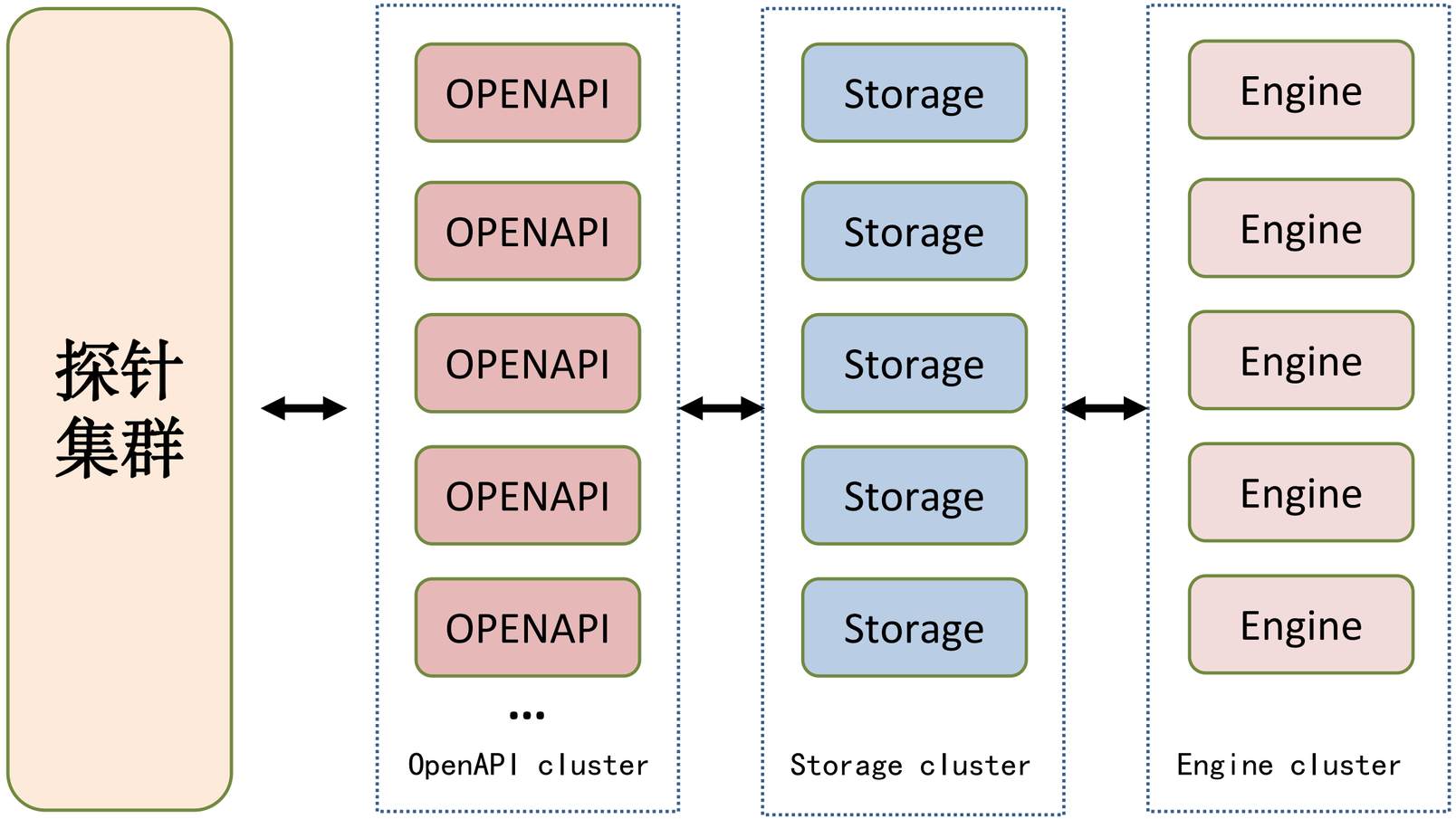
为什么选择洞态IAST

为什么选择洞态IAST

为什么选择洞态IAST



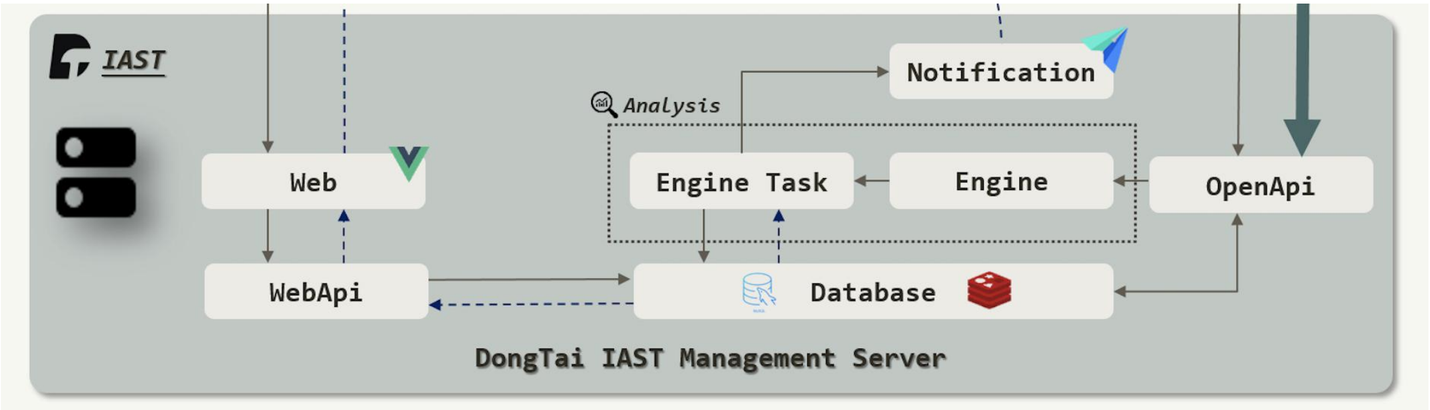
洞 态 I A S T + K u b e r n e t e s



无状态、弹性扩容、自动伸缩

洞态IAST + Kubernetes

```yaml
# dongtai-webapi服务
apiVersion: apps/v1
kind: Deployment
metadata:
  name: dongtai-webapi
  namespace: CHANGE_THIS_NAMESPACE
  annotations:
    kubesphere.io/description: dongtai-webapi接口
  labels:
    app: dongtai-webapi
spec:
  replicas: 1
  selector:
    matchLabels:
      app: dongtai-webapi
  template:
    metadata:
      labels:
        app: dongtai-webapi
    spec:
      containers:
        - name: dongtai-webapi-container
          image: registry.cn-beijing.aliyuncs.com/huoxian_pub/dongtai-webapi:latest
          imagePullPolicy: IfNotPresent
```



洞态IAST Agent + Docker

```
FROM huoxian_pub/dongtai-java-agent:1.0.4-jdk8

#.... build your java application
```

洞态IAST Agent + Kubernetes

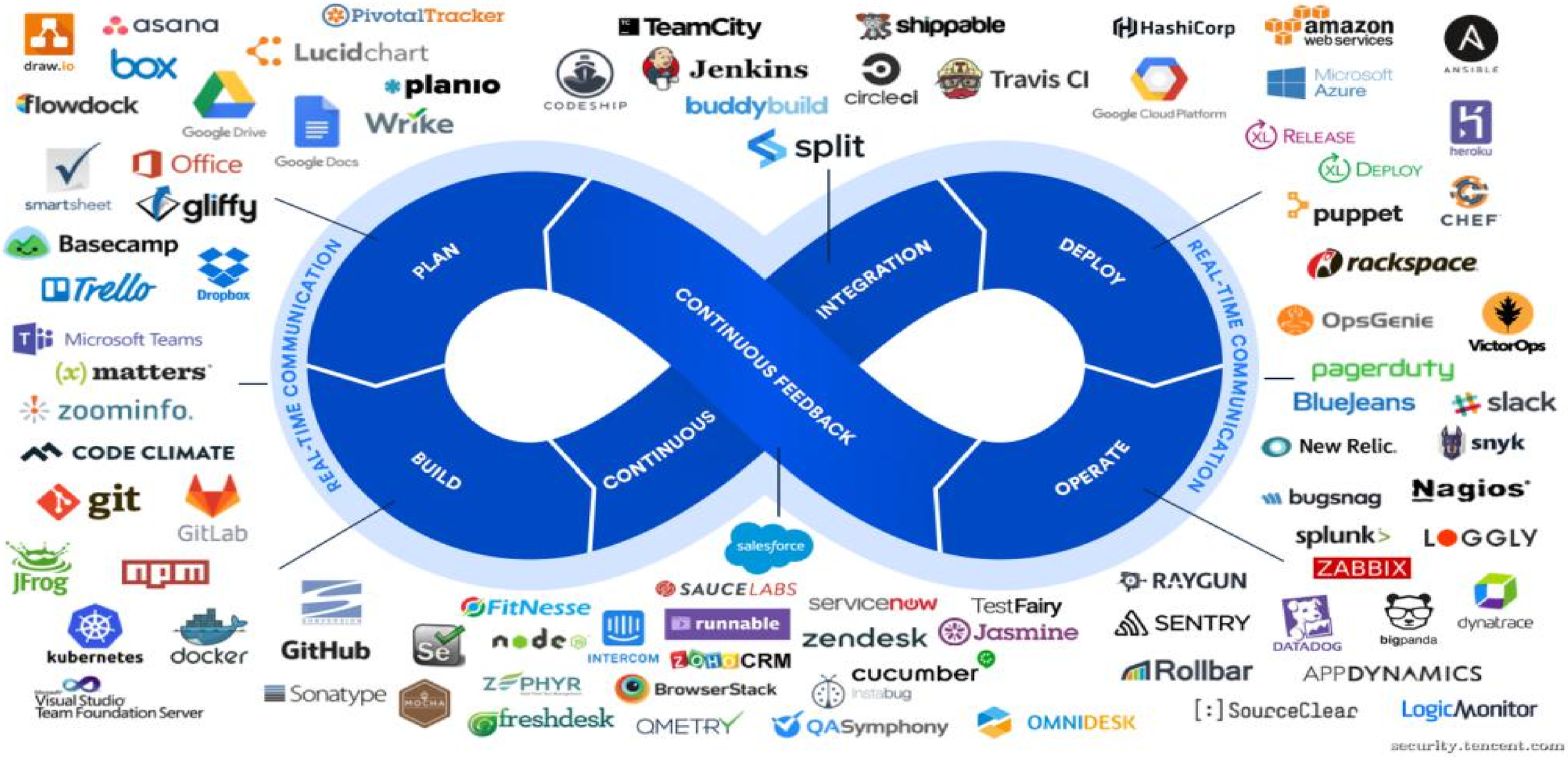
```yaml
apiVersion: v1
kind: Pod
metadata:
  name: agent-as-sidecar
spec:
  restartPolicy: Never

  volumes:
    - name: skywalking-agent
      emptyDir: {}

  containers:
    - name: agent-container
      image: huoxian_pub/dongtai-java-agent:1.0.4-alpine
      volumeMounts:
        - name: dongtai-agent
          mountPath: /agent
      command: [ "/bin/sh" ]
      args: [ "-c", "cp -R /dongtai/agent /agent/" ]

    - name: app-container
      image: apache/Spring-Boot-Example:latest
      volumeMounts:
        - name: dongtai-agent
          mountPath: /agent
      env:
        - name: JAVA_TOOL_OPTIONS
          value: "-javaagent:/dongtai/agent/agent.jar"
```

洞 态 I A S T + D e v O p s



想了解更多，请关注我们的公众号或点击

https://cloudnative.to

云原生社区

Cloud Native Community