58同城

2021

58同城 第2届 安全技术沙龙

业务风控建设 & 应用安全实践

58安全应急响应中心 Security Response Center | 58安全 58 CYBERSECURITY

DATE - 2021.12.17 线上直播

宋京浩 火线安全高级研发工程师

分享主题

洞态IAST与黑盒、白盒共建DevSecOps

议题介绍

本次分享分别从IAST检测原理，洞态IAST架构设计出发，阐述安全人员如何通过运营洞态IAST，完善 IAST 的检测能力，黑盒、白盒做旁路检测/辅助检测，实现自动化的检测并保证检出率、准确率，减少重复性的人工成本投入

01

洞态IAST与黑盒、白盒共建DevSecOps

02目录

03

IAST检测原理

03 IAST检测原理

IAST（Interactive AST，交互式扫描器）高频、高效、无脏数据

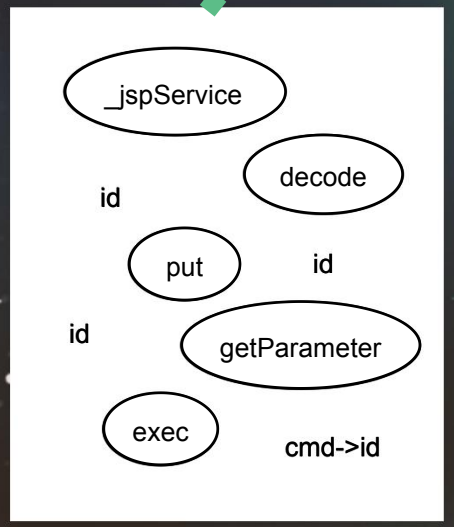
- 原理

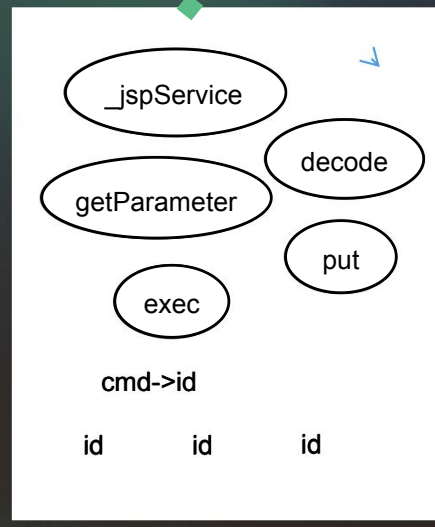
- 效果

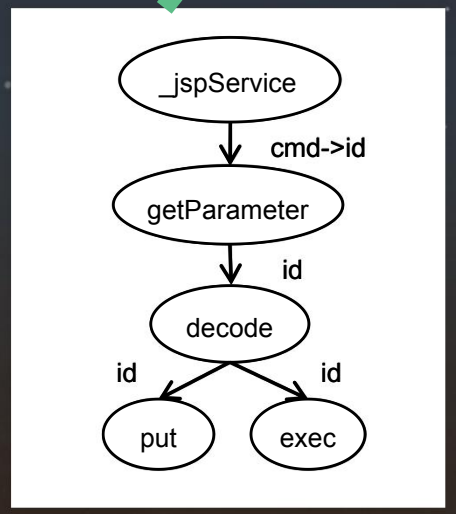
覆盖度完整　准确率高　效率高　无脏数据*

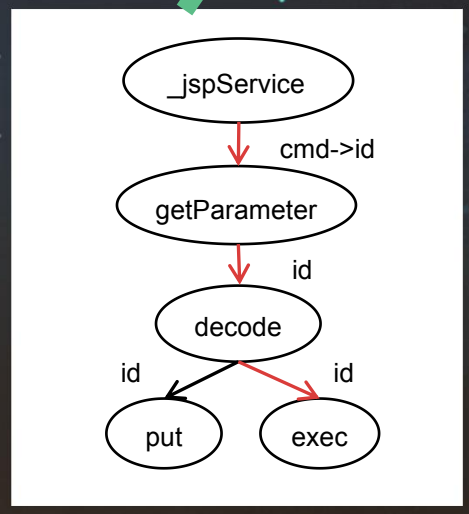
03 IAST检测原理 污点跟踪算法

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









04

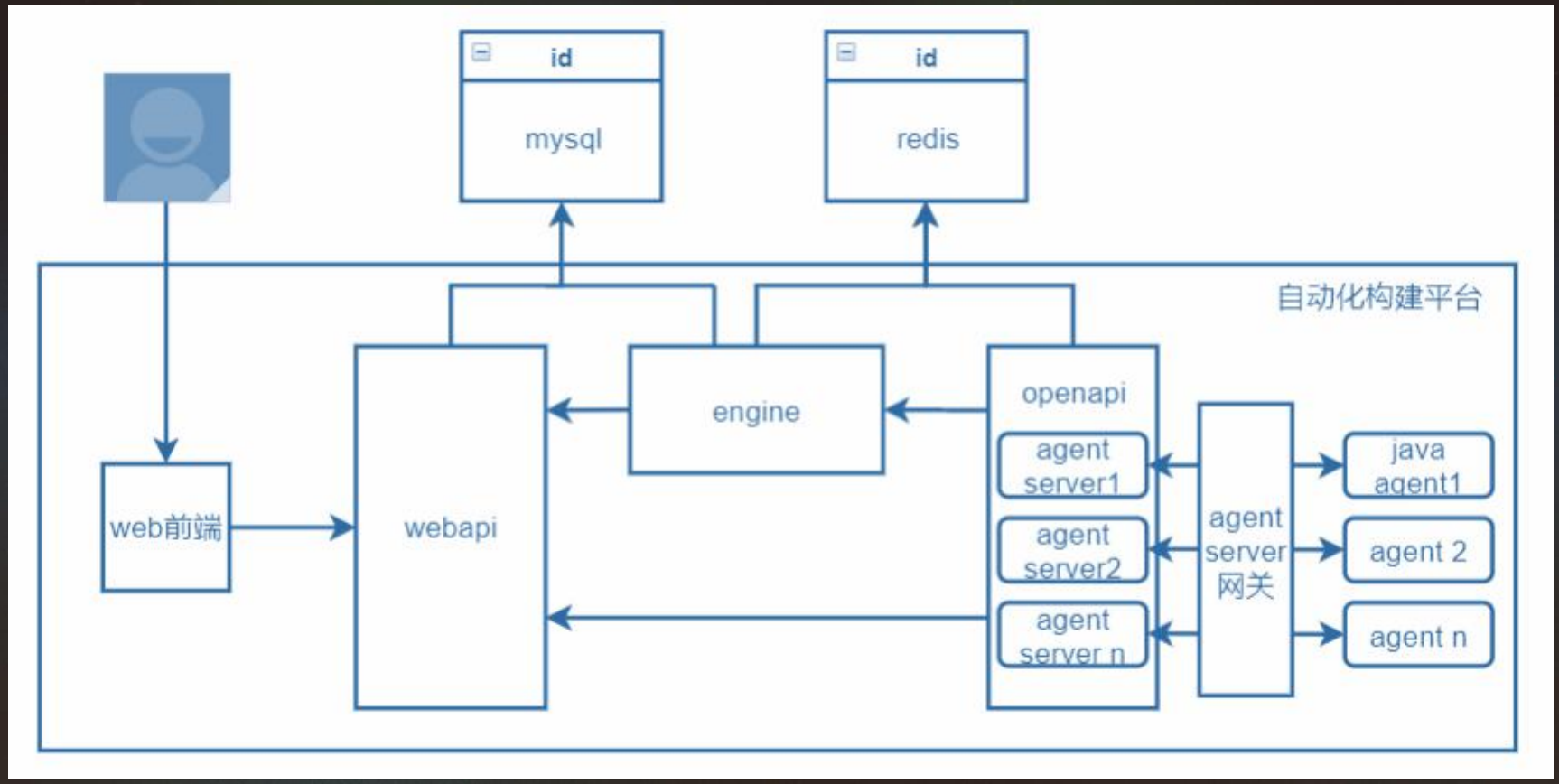
洞态IAST架构设计

04洞态IAST架构设计 整体架构

- 更低的使用成本及更强大的检测能力

类型	架构	分析
一般IAST	重Agent端+轻服务端 数据监听和漏洞检测全部在Agent端完成。	1.需频繁升级Agent端； 2.未检测出漏洞的Agent端数据直接丢弃，若产品检测能力升级，需联系功能测试团队重新发起测试； 3.无法实现跨请求关联分析。
洞态IAST	轻Agent端+重服务端 Agent端仅实现数据监听，漏洞检测全部在服务端完成	1.Agent端代码和逻辑简单，单点故障率更低，极少升级； 2.所有数据保存在服务端，可在服务端直接进行回归测试； 3.服务端可动态加载检测引擎，并可实现跨请求关联分析。

04洞态IAST架构设计 部署架构



05

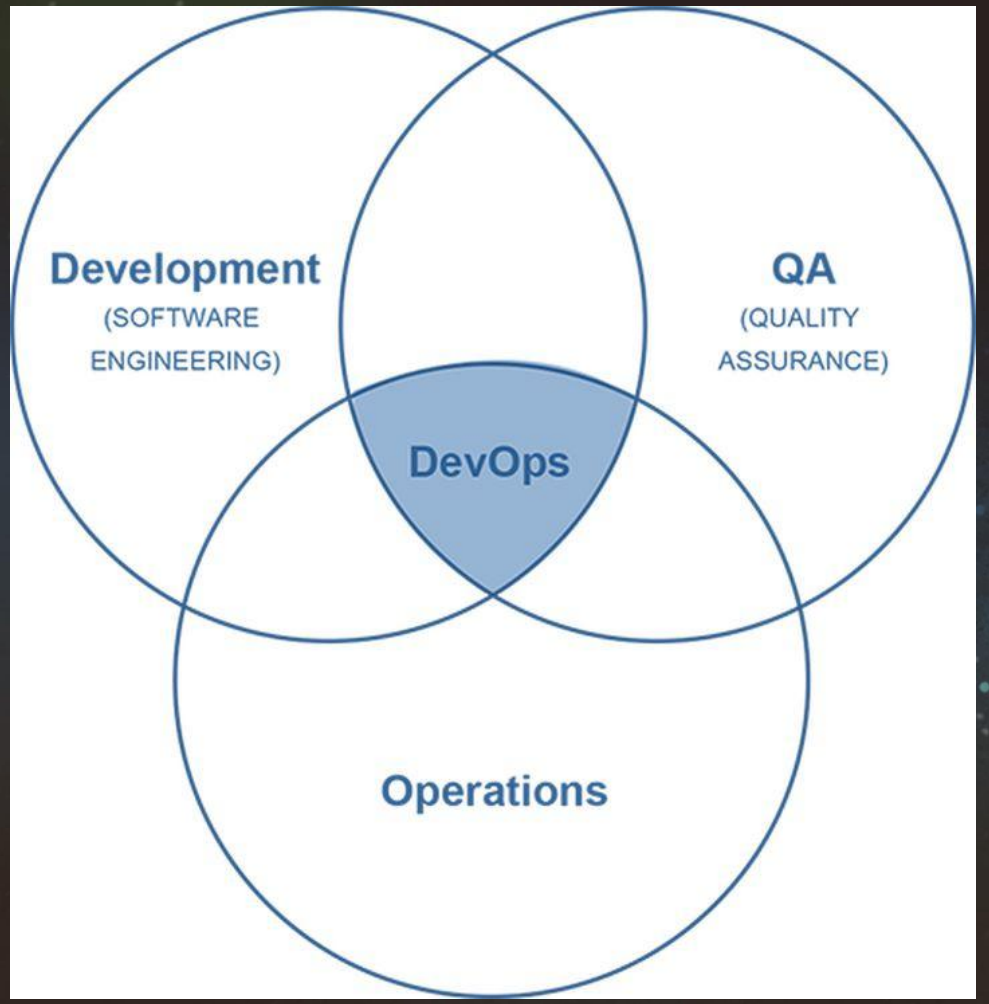
灰盒、黑盒、白盒共建
DevSecOps

共建DevSecOps

什么是DevOps

从字面上来理解，DevOps 只是Dev（开发人员）+Ops（运维人员），实际上，它是一组过程、方法与系统的统称

DevOps目前并没有权威的定义，DevOps 强调的是高效组织团队之间如何通过自动化的工具协作和沟通来完成软件的生命周期管理，从而更快、更频繁地交付更稳定的软件。



共建DevSecOps

安全如何更好的加入

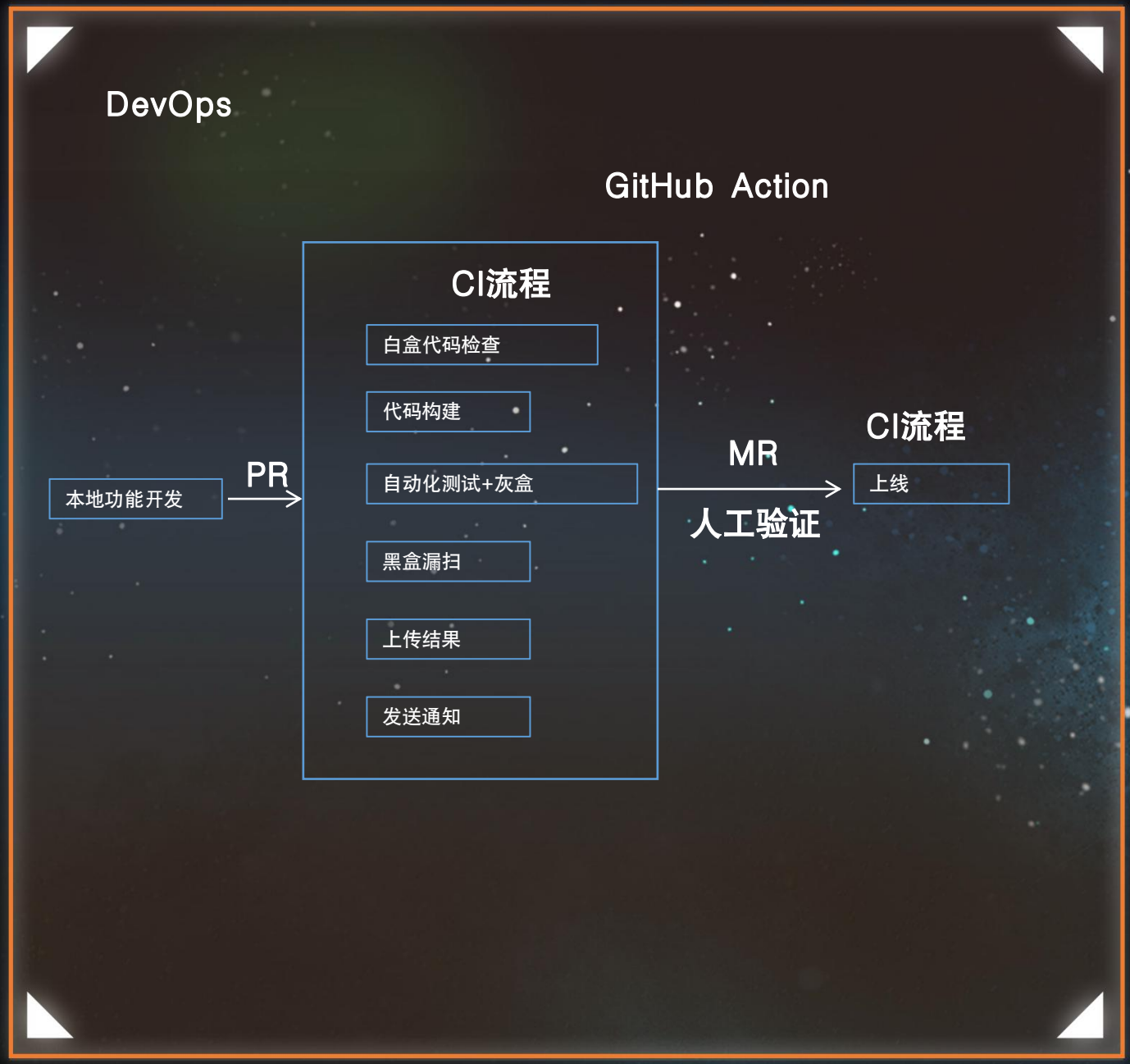
- DevOps并非旨在以牺牲安全性为代价来最大化速度；
- 安全去适应特性：简单、快捷、持续
- 在CI-自动化测试环节引入安全检查（Sec）

共建DevSecOps

IAST在DevSecOps中是如何工作的

方式一：先白盒审计，覆盖率高，后灰盒接入，初步解决误报问题，黑盒针对性扫描再次确认，避免脏数据与性能压力，最终上报，人工确认

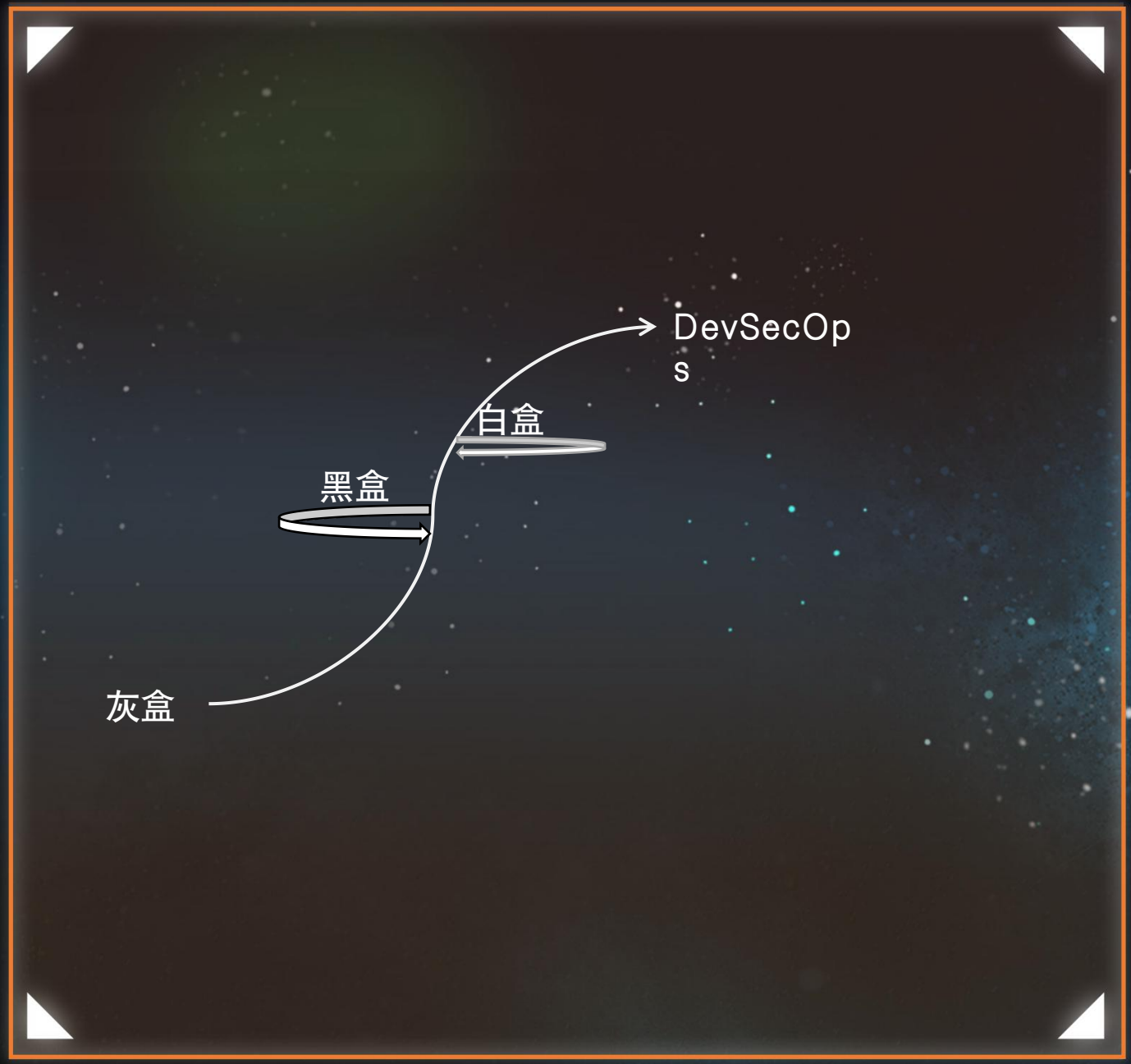
方式二：若不介意性能压力问题，三者同时进行，三者结果匹对，最终上报，人工处理



共建DevSecOps

持续提升IAST检测能力

灰盒做 DevOps 中的同步检测，
黑盒、白盒做旁路检测/辅助检测，
持续运营，提升 IAST 的检测能力，
实现自动化的检测并保证检出率、准确率



06

部署与落地

06 部署与落地

洞态IAST部署

Server端部署

- docker
- K8s – Manifest
- K8s - helm

Agent端部署

- Base Docker Image
- K8s initContainer

洞态IAST官方文档：https://doc.dongtai.io/zh/

06 部署与落地

DongTai-Agent-Java 如何集成到 DevOps

需求：

在每次提交代码时，自动将靶场的测试数据存入特定的项目、特定的版本中，方便直接根据项目及版本进行数据的对比分析。

Java Agent 在 GitHub Action 及 DevOps 流程中的建议启动命令：

```
java -javaagent:/path/to/agent.jar -Dproject.create=true -Dproject.name=WebGoat -Dproject.version=8.2 -Dresponse.length=1000 -Diast.server.mode=local -jar app.jar
```

洞态IAST官方文档：https://doc.dongtai.io/zh/

06 部署与落地

同程IAST的推广

- 发挥安全的主动性，主动去贴合业务流程

  - 培训和文章推广：在公司内部开展周期性的安全培训和安全发文，介绍IAST；
  - 根据发现的安全事件，主动推动和提供给业务线安全能力；
  - 与测试团队合作，推动SDL安全能力融入测试流程；

提问环节