GOPS 2022
shenzhen

招商基金DevSecOps建设探索与实践

王洋

目录 Contents

01

招商基金DevOps的建设实践

分享思路

GOPS 2022
shenzhen

01 不能做成一个纯技术的分享

02 深度结合我司实际情况

03 分享一些思路和“坑”

老生常谈DevOps是什么？

一千个人眼中有一千个哈姆雷特，十个人眼中估计会有大于十个对 DevOps 的理解。

DevOps 是什么？你是否有以下困惑：

一种精神？还是一套工具平台？看了很多文章讲 DevOps 结果还是不知道是什么，怎么做？

我对 DevOps 的理解：

它是一种工作方式，是一种打通了从业务需求到项目管理到开发到测试到部署到运营的一系列节点而形成闭环的工作方式。

这个闭环过程中涉及到的所有对 kpi、专项任务或者个人成长没有价值的人工操作都应该尽可能的自动化。
如果你仅仅是想听，代码是如何在开发测试生产环境流转或者 CI/CD 要如何配置，那么我讲的内容可能会让你失望。

我司DevOps建设的关键点

轻流程

互惠互利（吸引用户）

快速迭代（MVP）

工具能力（开放）

标准化落地

数据治理-CMDB

架构规划

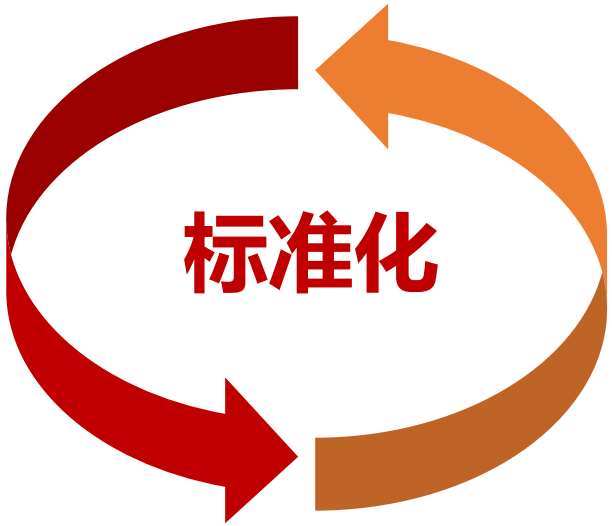
标准化是绕不过的“坎”！！

GOPS 2022
shenzhen

主机和操作标准
- 提供几种标准的配置规格
- 提供标准的操作系统模板
- 提供标准的系统参数
- 提供标准的操作系统版本

代码&打包&制品标准
- 代码管理标准
- 打包工具和路径标准
- 制品名称标准化
- 版本号标准化

变更/上线标准化
- 变更标准化分级
- 上线流程标准化



推进落地
- 共识
- 舍小取大

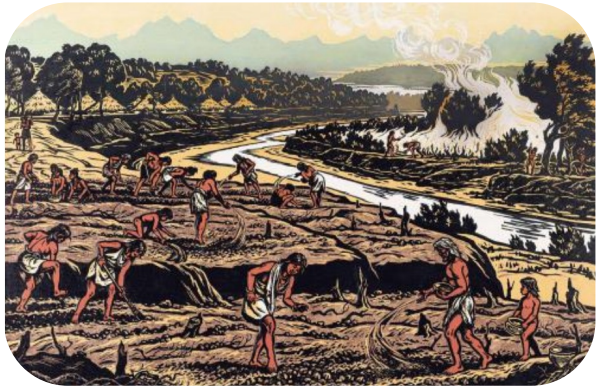
部署与发布标准
- 灰度发布标准
- 优雅发布标准
- 启动和停止脚本标准
- 部署路径和权限标准
- 状态监测标准
- 二进制包、配置、日志、行为目录标准

中间件标准
- Web
- Jvm容器
- 消息中间件
- 缓存
- 数据库

口径术语标准
- 平台、系统、应用
- 业务—IT开发—IT运维

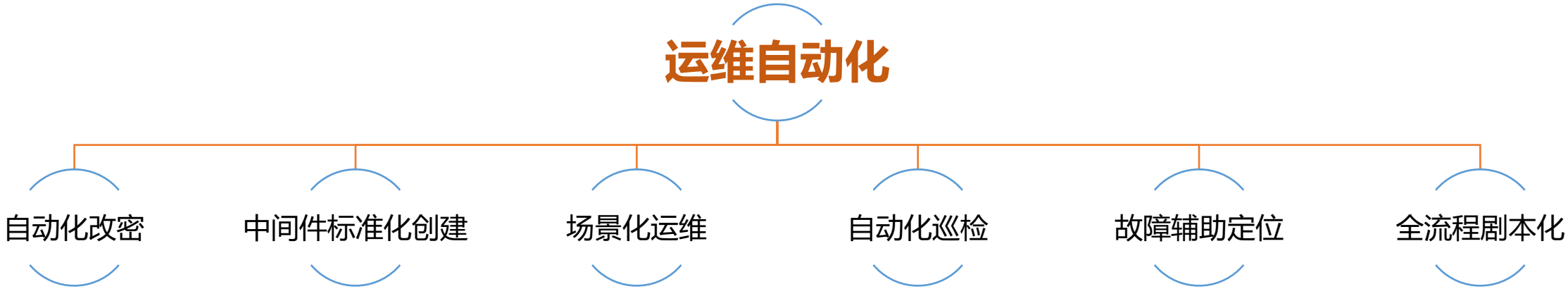
日常工作手工OR自动化？

- 主机创建/存储创建
- 应用配置
- 版本管理
- 监控配置
- 文件清理
- 需求管理
- 中间件安装
- 变更发布/优雅发布
- 优雅发布
- CMDB 数据维护

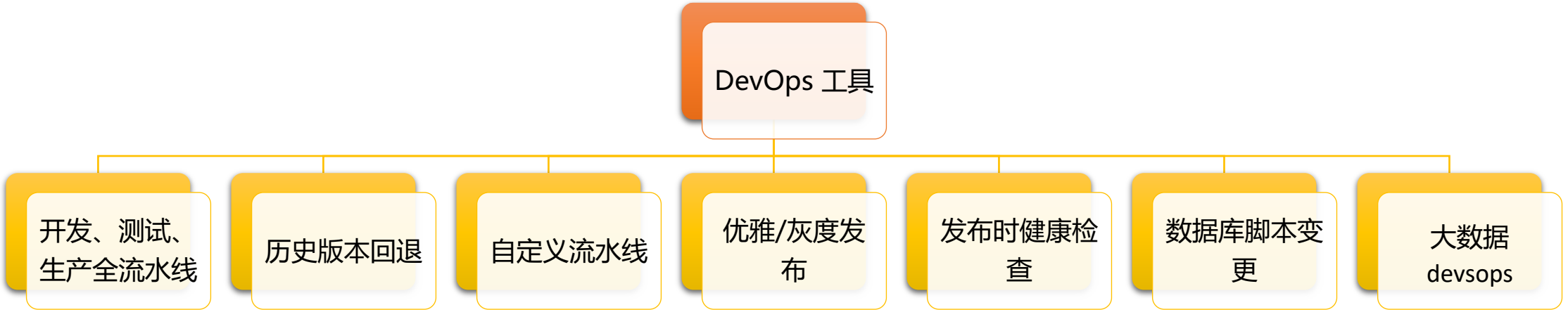


大家找找看
有没有自己的
影子？

我司现有自动化能力



我司现有CI/CD能力


DevOps 工具
开发、测试、生产全流水线
历史版本回退
自定义流水线
优雅/灰度发布
发布时健康检查
数据库脚本变更
大数据devsops

CI/CD近一年报表

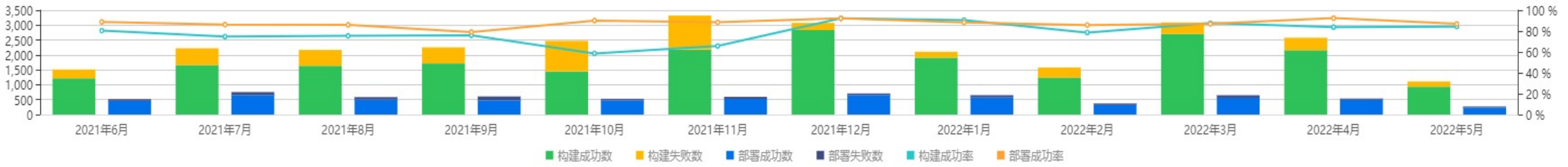
GOPS 2022
shenzhen

总览

近一年

27483 次 构建总数	79% 构建成功率
21639 次 构建成功数	5844 次 构建失败数
6767 次 发布总数	88% 发布成功率
5929 次 发布成功数	838 次 发布失败数

趋势图(每月)



02

招商基金从DevOps向DevSecOps演进的建设思路

顺“势”而为

GOPS 2022
shenzhen

01
行业之“势”

DevOps---
>DevSecOps演进

02
信息安全之“势”

监管要求

03
我司实际需求之“势”

1、业务发展对信息安全要求的提升
2、高效运营管理需求-内部大量“零散”的安全能力或者工具整合
3、架构安全倒逼

招商基金的DevSecOps建设指导思想

03

招商基金DevSecOps具体建设实践

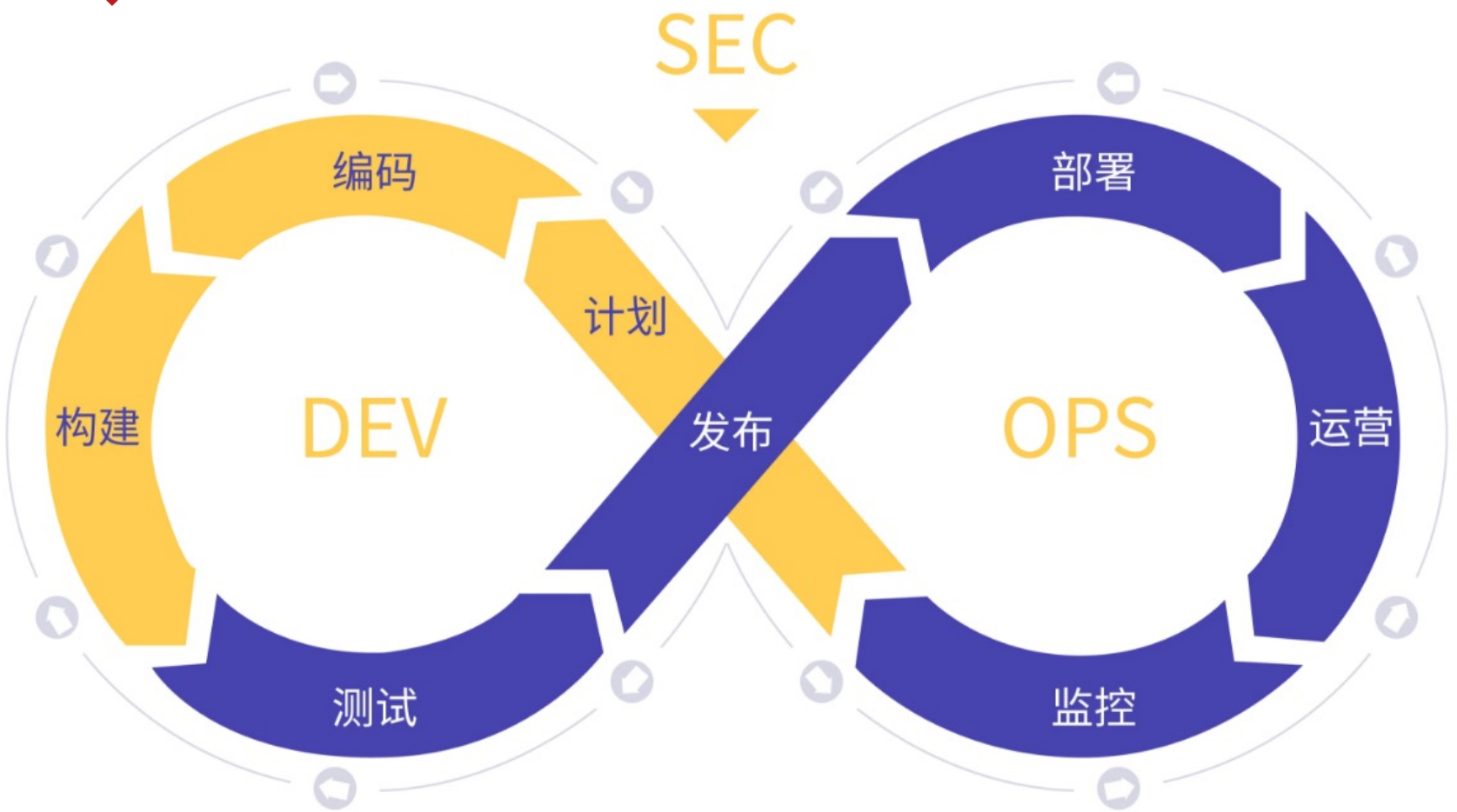
现有的安全能力

GOPS 2022
shenzhen

整理“家底”

- Sonar代码扫描
- 静态代码安全扫描
- 防火墙
- 开源组件管理
- 密码管理
- API安全扫描
- 主机安全
- 缺陷跟踪
- 操作系统基线检测
- API网关（架构安全）

经典的“8”字图



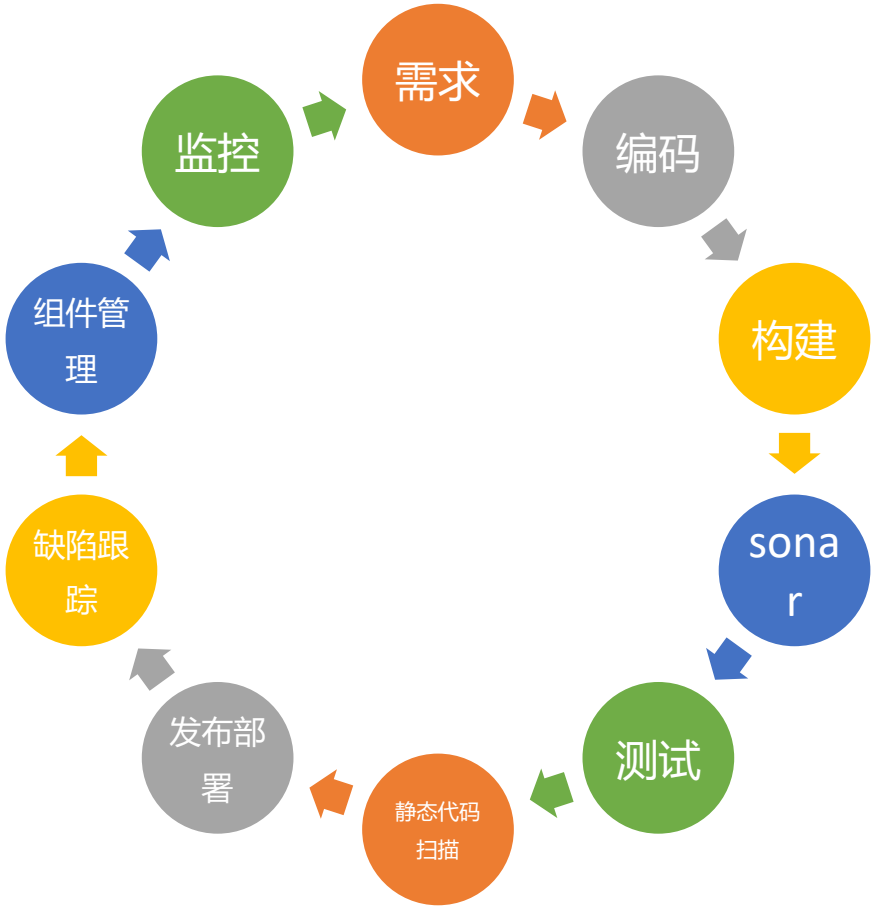
一千个人眼中
有一千个哈姆雷特

SEC要如何注入？单纯的左移？

我司落地的“8”字图

API网关
（架构安全）

API安全 OWASP Top10
（运行时安全）



代码周期性扫描

安全基线安全

CMDB/流程引擎/自动化

细说之代码扫描

扫描的“左移”--sonar和静态代码安全扫描

1 周期扫描

sonar：对所有系统，按照30分钟的频率对指定的代码分支进行扫描，若发现问题，邮件通知项目经理进行修复；

静态代码安全扫描：对于重要核心系统，会周期性的在夜间进行代码安全扫描，发现高危漏洞会邮件通知项目经理进行修复；

2 串行扫描

sonar：对所有系统，在版本构建阶段进行扫描，如有问题通知开发人员；

静态代码安全扫描：对于重要核心系统需要封板变更前完成一次扫描，对于某些系统在变更后按需再完成一次扫描；

为什么要有的在变更前？有的在变更后？

细说之缺陷跟踪

针对安全扫描出的漏洞要如何消除？
---安全缺陷跟踪

1 问题

1、某个项目引入了哪些安全漏洞？
2、这些安全漏洞是在哪个版本引入的？谁引入的？在什么位置？
3、这些安全漏洞有什么危害？要怎么修复？
4、这些安全漏洞是在哪个版本修复的？
5、这些安全漏洞是在哪个时间修复的？

2 解法

基于我司的“朱雀”平台（运维一体化平台），利用cmdb、流程引擎、自动化能力，打通sonar、静态代码安全扫描平台，将这些融入我司的devsecops流水线中，从而实现对安全缺陷的全生命周期管理。

为什么要有的在变更前？有的在变更后？

细说之lib库组件管理

GOPS 2022
shenzhen

devsecops建设中的一环

log4j事件的催化

1 解法

在变更部署后抓取到该应用本次版本所使用到的所有组件，更新到“朱雀”平台的lib库组件管理模型中，并进行基线比对。

2 收益

能够知悉每个组件包是在哪个版本引入的，组件包的路径信息，所属哪个应用，开发负责人是谁，当前组件是否满足版本基线要求，当爆发安全问题时能够快速定位哪些应用受影响，从而对lib库组件实现精细化管理。

细说之API网关与安全

GOPS 2022
shenzhen

API在数智化转型中的核心位置凸显

外购系统不提供API接口直接不考虑

1 **API网关（架构安全）**

对于东西和南北向的跨系统或者应用的API调用，都需要通过API网关来进行统一的身份鉴权、调用方式鉴别、调用时间鉴别、调用频率鉴别、调用格式鉴别等，将非业务特性的网关安全需求和网关需求统一放在一级网关（伏羲）上进行，并且凡是对外暴露的API都要符合我司的API规范，对于规范的校验也会在网关上进行。

2 **API安全扫描**

通过API安全扫描平台（乾坤镜），发现应用调用API期间的安全问题，例如明文密码传输、暴力破解、高频调用、大流量请求、调用时间异常、越权访问、低响应成功接口、响应内容有敏感信息等，周期性的将问题通过邮件发个相应的项目经理。

细说之防火墙、密码管理、堡垒机

细说之主机安全和操作系统模板

细说之应用密码自动改密

GOPS 2022
shenzhen

监管要求定期改密，怎么破？

停止应用 → 修改数据库密码 → 按照加密算法对修改后的密码加密 → 将明文和密文写入密码保险箱 → 修改目标应用的密码配置 → 启动应用 → 应用健康检查

整个过程自动化，从原来的改一次密码需要15-20分钟缩短至5分钟以内。

细说之应用密码自动改密

04

招商基金在DevSecOps建设中的总结

招商基金在DevSecOps建设中的总结

理想化的安全左移当然是好的，但是公司现有的安全能力能否支持（投入产出比）？推广起来阻力是否会很大？寻找最优的结合点。

DevSecOps虽然是一种工作理念，但是还是需要强有力的工具支持，不然就是无源之水，无本之木，变成了空洞低效的人肉流程，工具支撑尤为重要，这里工具包括支撑DevSecOps主流程的工具以及周边需要对接的所有工具，都要能融入并且符合自身的建设需求。

安全与便捷本就是一对矛盾，所以在devsecops建设过程中，就更加需要采用敏捷思维，快速响应使用者的需求，这样在推广的过程中才能将阻力降至最低，才有利于devsecops这件事能够以互利共赢的方式进行推广。

招商基金在DevSecOps建设中的总结

建设模式

优点

- 技术栈完全自主可控；
- 本地化适应性好；
- 按需自定制性强；
- 省钱？

缺点

- 人力投入资源多；
- 整个链条中涉及的诸多能力都要自建不可预见性强；
- 对实际的目标效果没有明显的可以预见的预期；

纯自研？

招商基金在DevSecOps建设中的总结

建设模式

纯外购？

优点

- 不用从头开始造轮子；
- 实施效果预见性强（参考案例以及合同约束）；
- 节约内部人力资源；

缺点

- 可能会有厂商依赖；
- 本地自定义适应性较差；
- 贵？；

招商基金在DevSecOps建设中的总结

GOPS 2022 shenzhen

建设模式

各种满足我司本地化需求和监管要求的DevSecOps能力

购买扩展性强的平台（具备API能力、自定义工具能力、流程引擎能力等）

+

具备对公司本地化需求能够熟悉的项目经理加基于平台的开发人员

外购

自研

05

基金行业科技化建设中的一些思考

基金行业科技化建设过程中的一些思考

GOPS 2022
shenzhen

一些现实问题引发的思考

国际局势

供应链安全

未来技术方案的演进和选型

金融行业属于国计民生的重要行业！

基金行业科技化建设过程中的一些思考

GOPS 2022
shenzhen

A

坚持***业务导向***。实现IT价值与业务价值协同一致发展。

B

继续用***互联网技术和思维，结合实际行业情况***对现有的技术能力进行改造，取长补短，提升收益。

C

注重***运营***。从业务的视角统计出每个业务的资源使用情况，便于进行费用分摊，或者统计每个业务的基础成本消耗。

D

强化***用户体验***。要梳理清楚我们服务对象有哪几类，每类用户的真实需求是什么？针对性的有的放矢。

Thanks

开放运维联盟
高效运维社区 **荣誉出品**
DevOps 时代

想第一时间看到高效运维社区的新动态吗？

高维在线