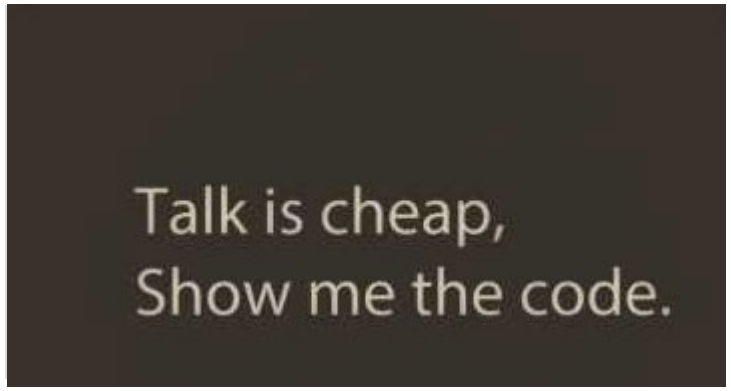
网络安全创新大会
Cyber Security Innovation Summit

壹钱包安全开发体系3.0落地实践

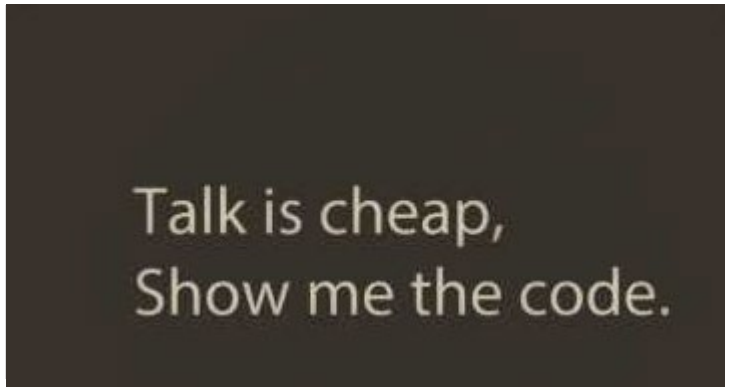
汪永辉　中国平安壹钱包安全架构师

三大痛点

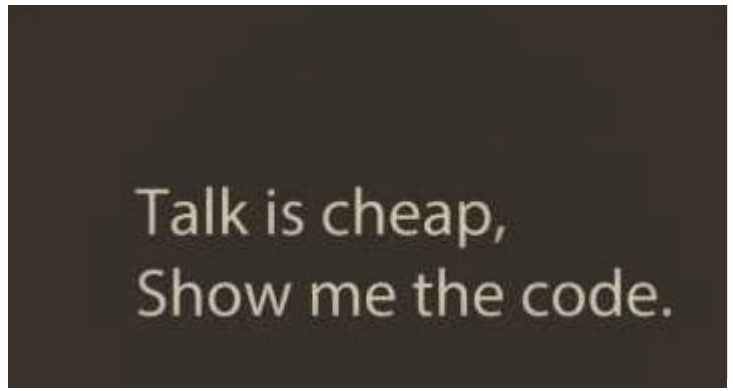
白盒工具误报多



跨领域沟通成本高



漏洞修复周期长



内嵌工具，非外挂

✓ 理念转变，外挂的安全工具服务于安全团队，而内嵌的工具服务于开发团队。

赋能研发，更高效

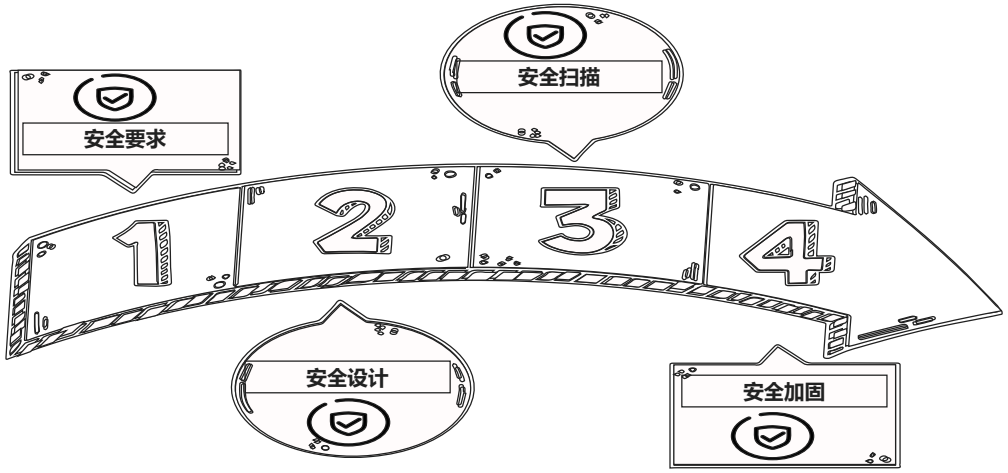
✓ 经过学习，研发同学能够快速掌握安全工具的使用方法，基本不用安全介入。

设立关卡，强管控

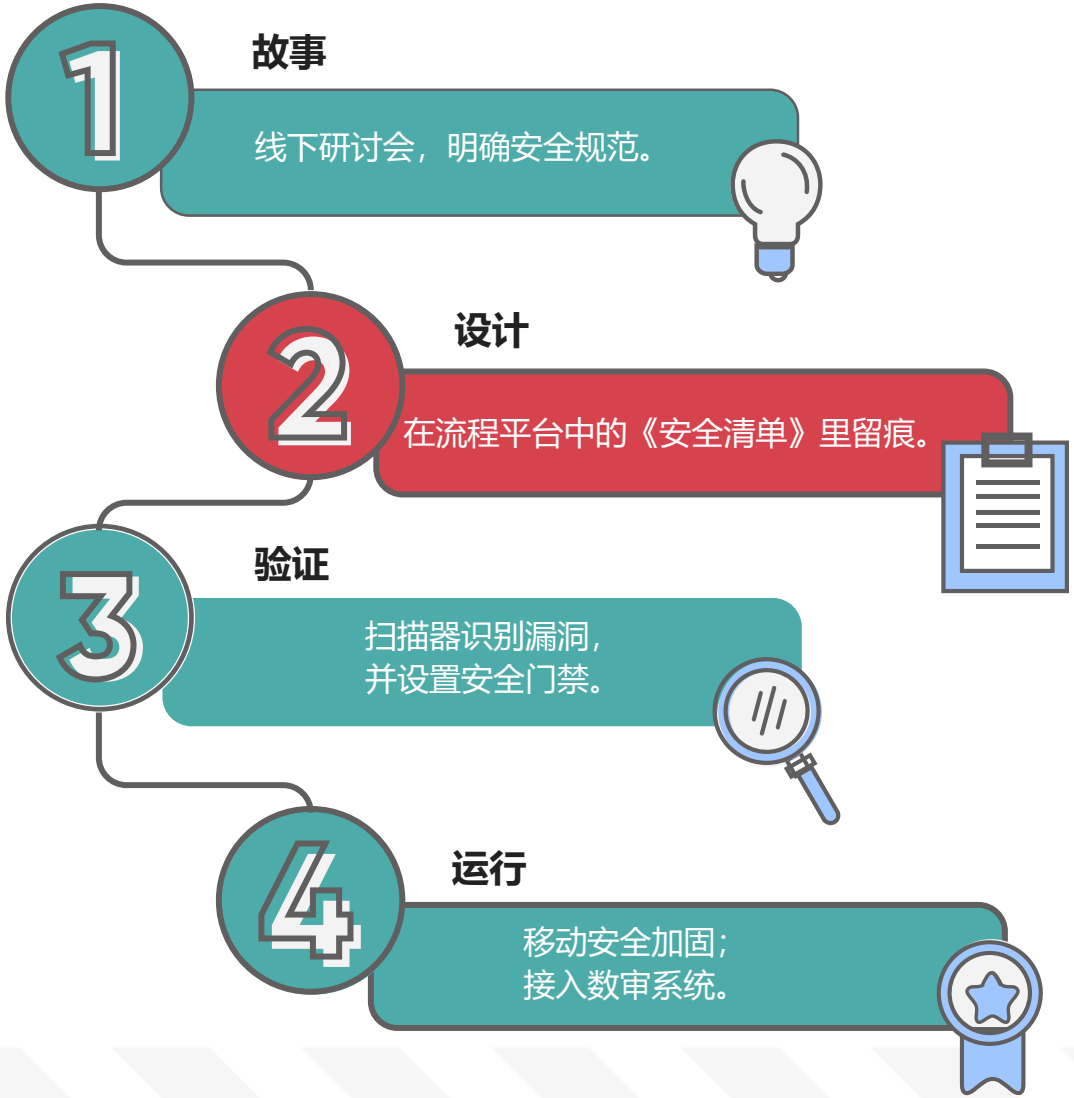
✓ 达成共识，明确安全红线，自动化卡版。

融入DevOps文化

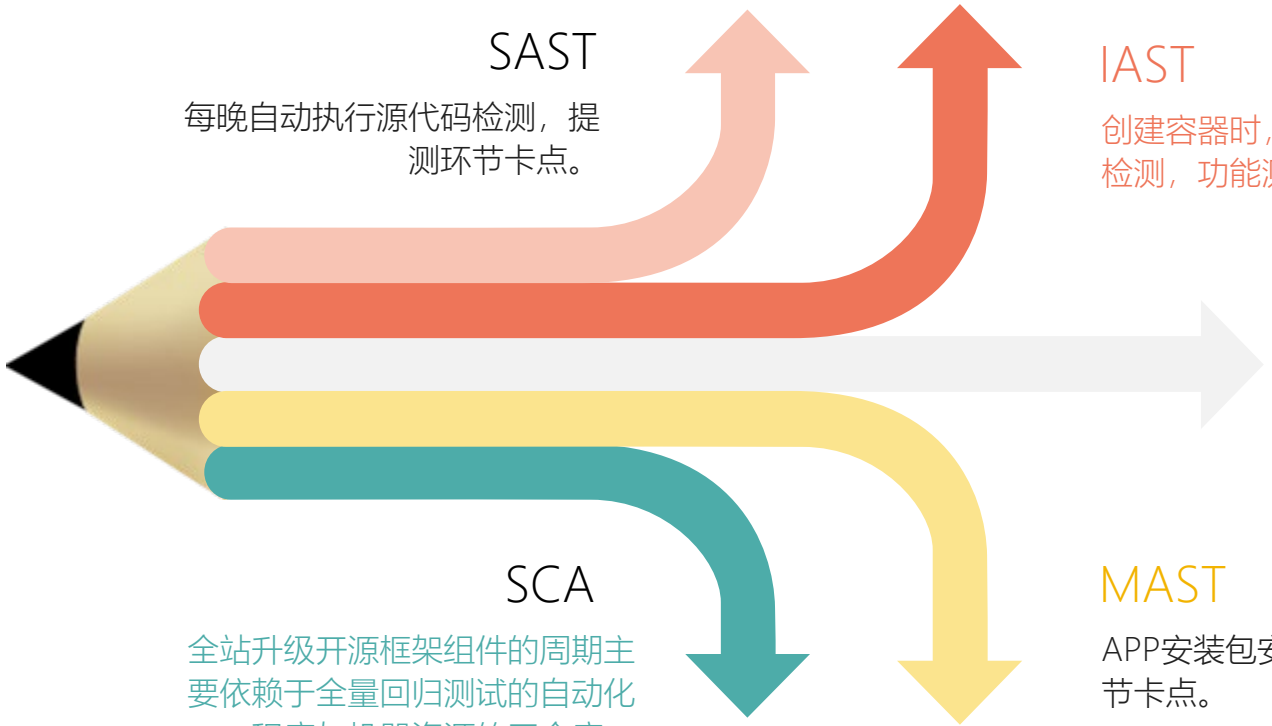
成立DevSecOps虚拟小组，由研发、产品、质量、运维和安全等角色组成，共同建设DevSecOps，推进每一个子任务融入流程平台。



落实非功能性设计


1
故事
线下研讨会，明确安全规范。
2
设计
在流程平台中的《安全清单》里留痕。
3
验证
扫描器识别漏洞，
并设置安全门禁。
4
运行
移动安全加固；
接入数审系统。

漏洞修复时效的瓶颈在哪里?



SAST

每晚自动执行源代码检测，提测环节卡点。

IAST

创建容器时，同步自动化插装检测，功能测试环节卡点。

DAST

常态化实时监测，从业务系统到生产环节中的全部应用系统。

SCA

全站升级开源框架组件的周期主要依赖于全量回归测试的自动化程度与机器资源的冗余度。

MAST

APP安装包安全检测，打包环节卡点。

驱动全站升级的下一个挑战

通用漏洞主动修复时长（漏洞平均），范围：RCE漏洞（命令执行、远程执行等）、0day、cvss7.0分以上或厂商发布漏洞定级为高危及以上。

1、外网漏洞：<=8小时，不扣分；

2、内网漏洞：<=1星期，不扣分；

未完待续

网络安全创新大会 Cyber Security Innovation Summit

计划 | 构建 | 测试 | 预发布 | 发布 | 配置 | 检测 | 响应 | 预测 | 自适应

Dev

Ops

打造一个动态化的控制台

需求分析
威胁建模
安全编码规范
安全开发组件
开源软件检测
SAST
渗透测试
DAST
IAST
MAST
回归测试
二进制插桩
APK加固
RASP
安全基线
系统安全加固
容器安全加固
安全监控
WAF
UEBA
漏洞应急响应
安全事件响应
威胁情报
数据情报
业务情报
态势感知
业务风控

统一需求管理工具
自动化威胁建模
安全设计自动化
安全开发框架
安全自动化扫描
开源软件检测
CI自动化测试框架
ASP自动化扫描
统一缺陷管理工具
自动化回归测试
APK自动化加固
RASP自动化安全防护
自动化安全基线扫描
资产检测自动化
自动化监控
用户行为分析自动化
漏洞自动化监测
安全事件自动化分析
红蓝对抗
自动化威胁情报分析
业务风控自动化

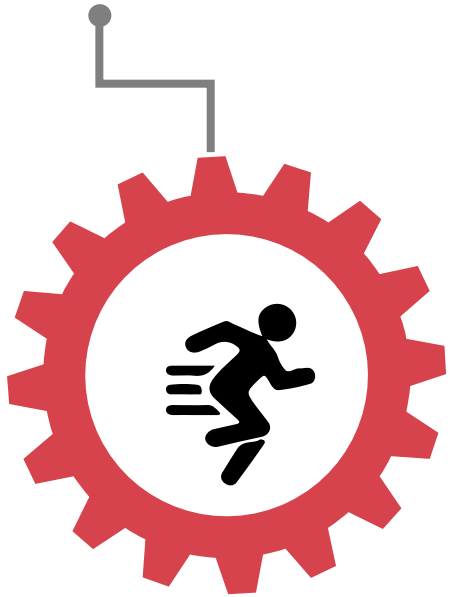
需求分析平台 | 研发安全管理平台 | 安全测试平台 | 安全加固平台 | RASP防护平台 | 基线扫描平台 | 安全监控平台 | 应急响应平台 | 威胁情报平台 | 业务安全平台

安全需求智能化分析
编码智能化安全监测
安全漏洞智能化挖掘
RASP智能化防护
智能化安全监控
威胁情报分析智能化
智能化风控

技术革新让安全响应更加迅速

机遇

极大地缩短了打补丁的周期

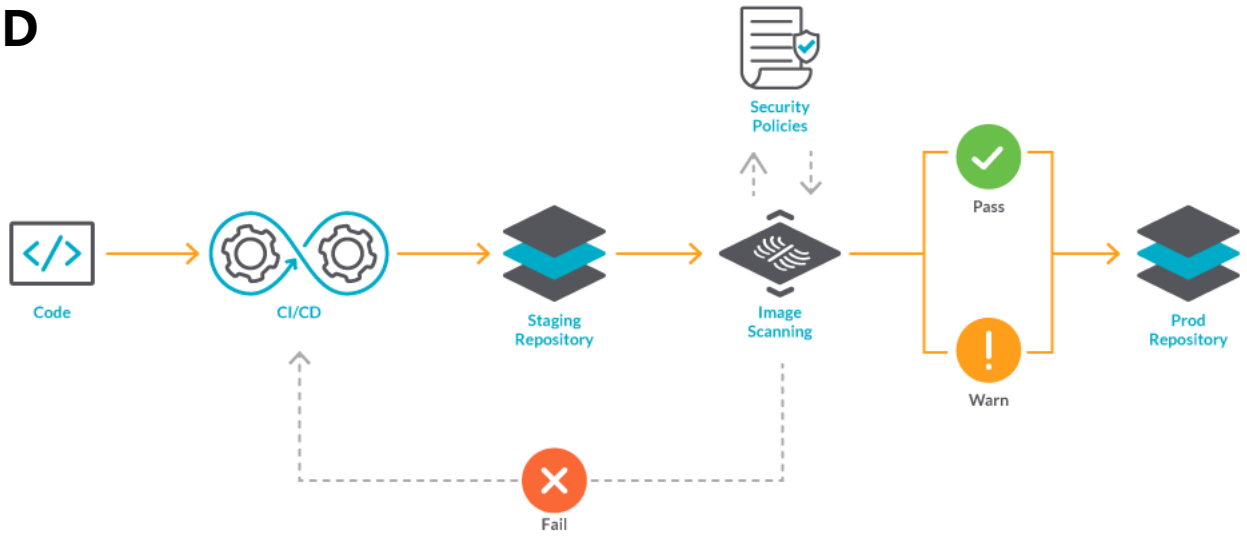


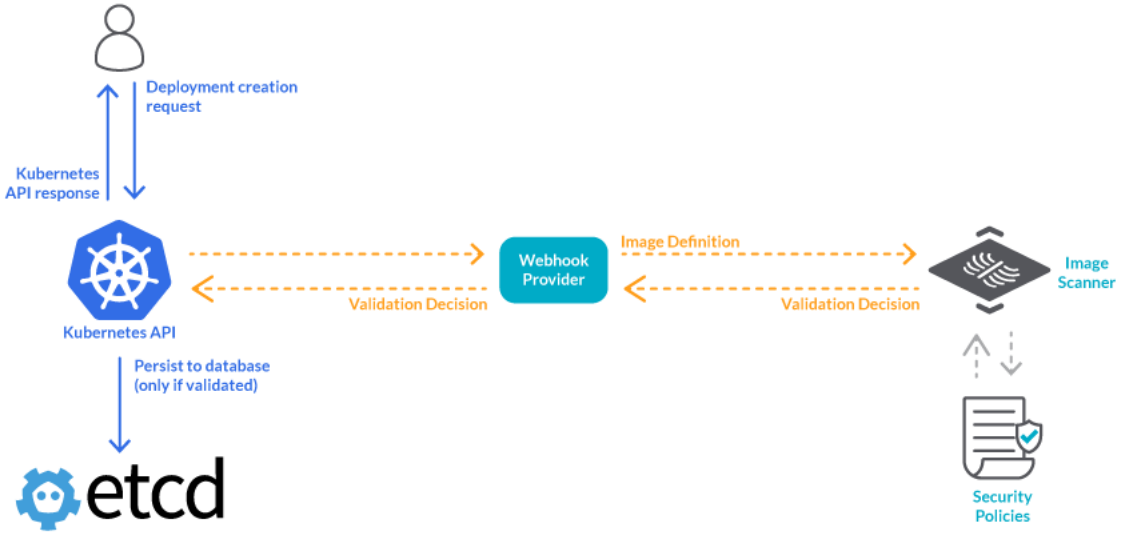
DevSecOps

挑战

花样繁多的容器逃逸

把容器安全融入CI/CD





信息安全人人有责

- DevOps强调如何促使团队之间更具协作性、更高效的关系，也注重让研发同学更多地控制生产环境。
- ✓ DevSecOps应当更加关注安全意识的宣导，如对钓鱼邮件攻击的识别与防范能力等。

代码

IDC

数据

最后，必须强调的是，让安全意识流行起来！

网络安全创新大会
Cyber Security Innovation Summit

THANKS