TOP1

主办方 msup

从SDL到DevSecOps的混沌式演进之路

武鑫 奇安信 产品安全高级经理

讲师简介

aerfa

百慕大

扫一扫上面的二维码图案，加我为朋友。

虎符智库专家，曾兼负责公司内部安全防护、运营和蓝军工作。

网络尖刀Z小队成员，BCS 2020、INSEC WORLD 2020、EISS 2021、DevOpsDays 2022等会议分享嘉宾。擅长从攻防视角进行甲方企业安全建设，在软件开发安全、供应链安全、攻防对抗方面有一定研究。业余时间喜欢思考与总结沉淀，主理个人微信公众号“我的安全视界观”，将安全实践输出成文，并对外分享与交流。

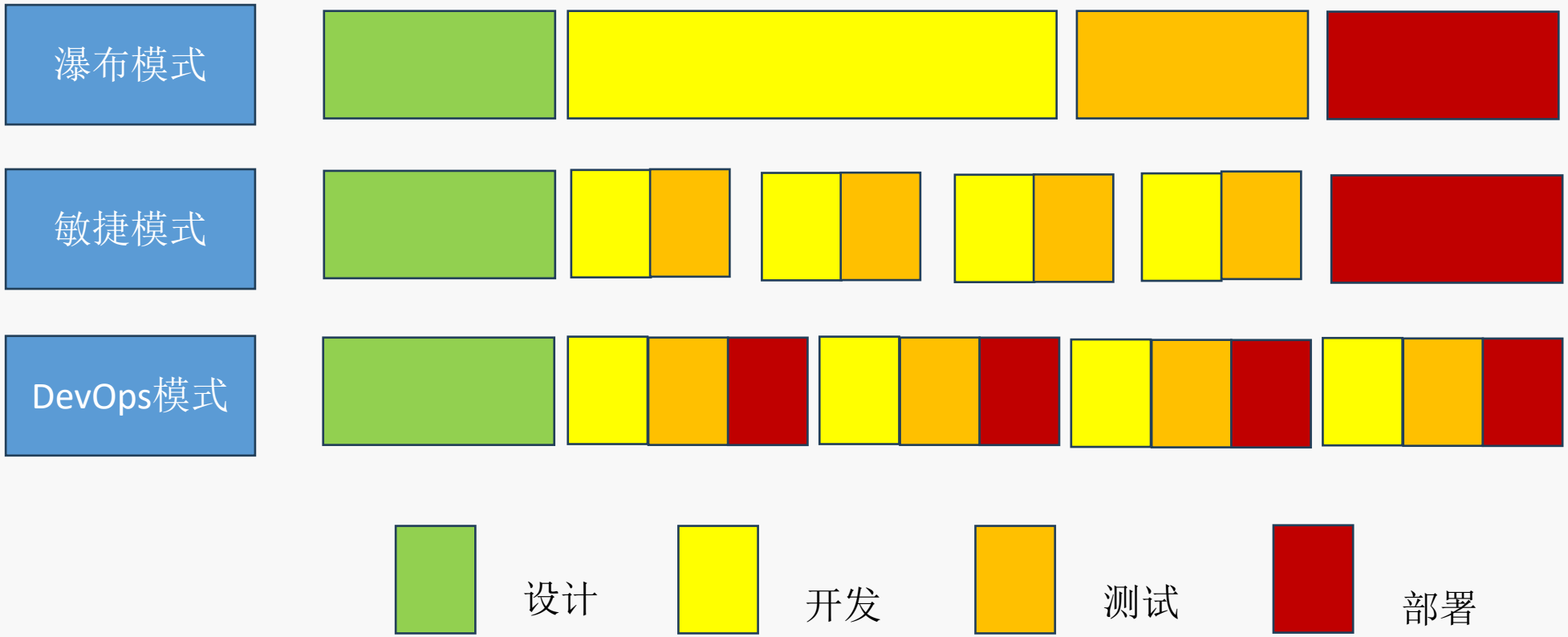
目录
Contents

01 数字化转型下的痛点

市场对业务的快速交付需求

抢占市场先机，倒逼业务快速集成与交付。

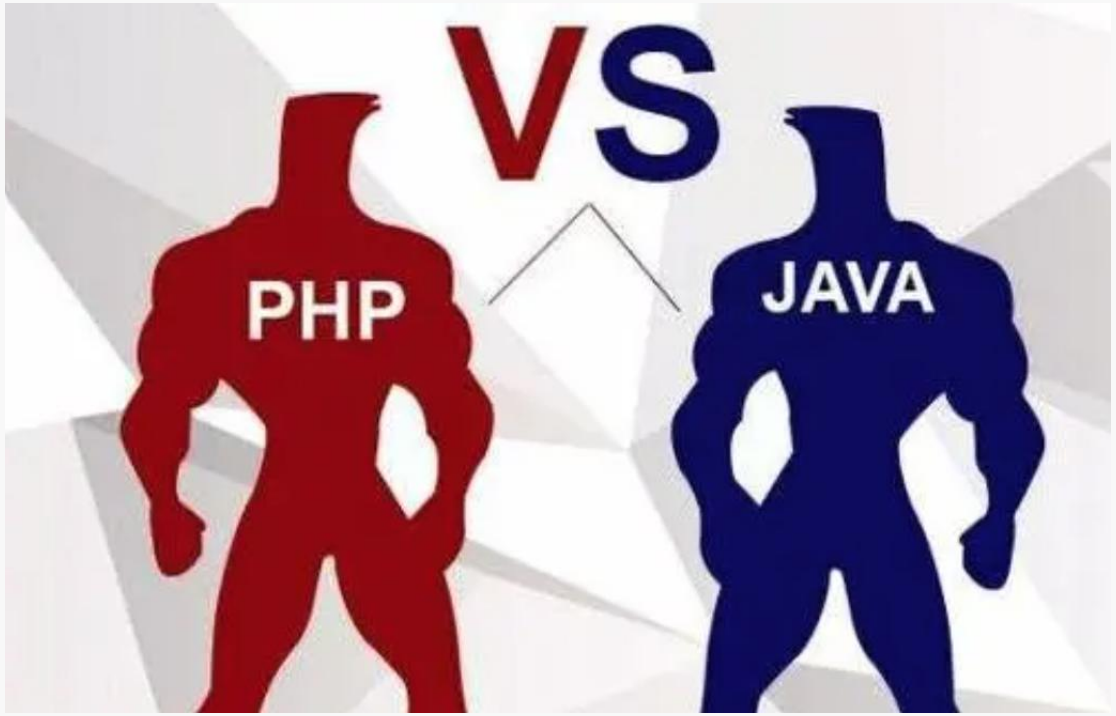
但并不是所有的业务都被要求快速，开发模式逐渐出现差异化。



技术发展带来的多样化

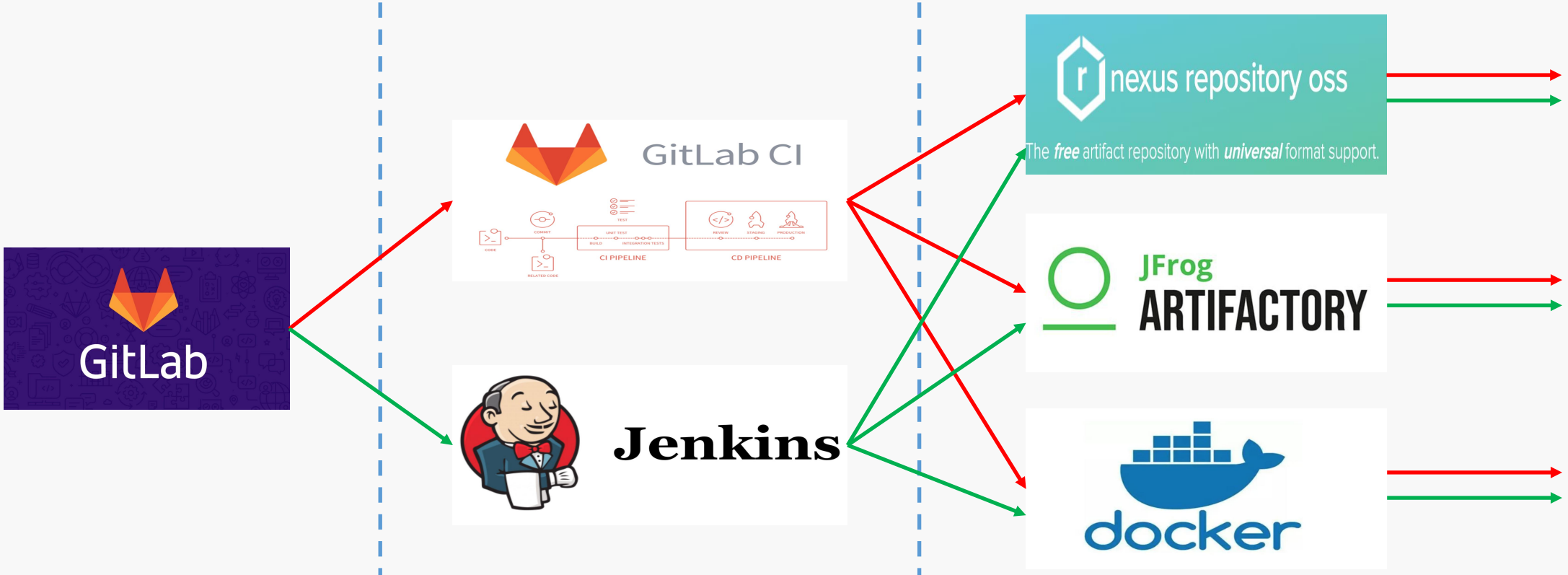
在数字化转型的大背景下，编程技术的发展，出现了新语言代替旧语言的情况。

然而，仍旧会有多种语言共存的局面。



研发基础设施不统一

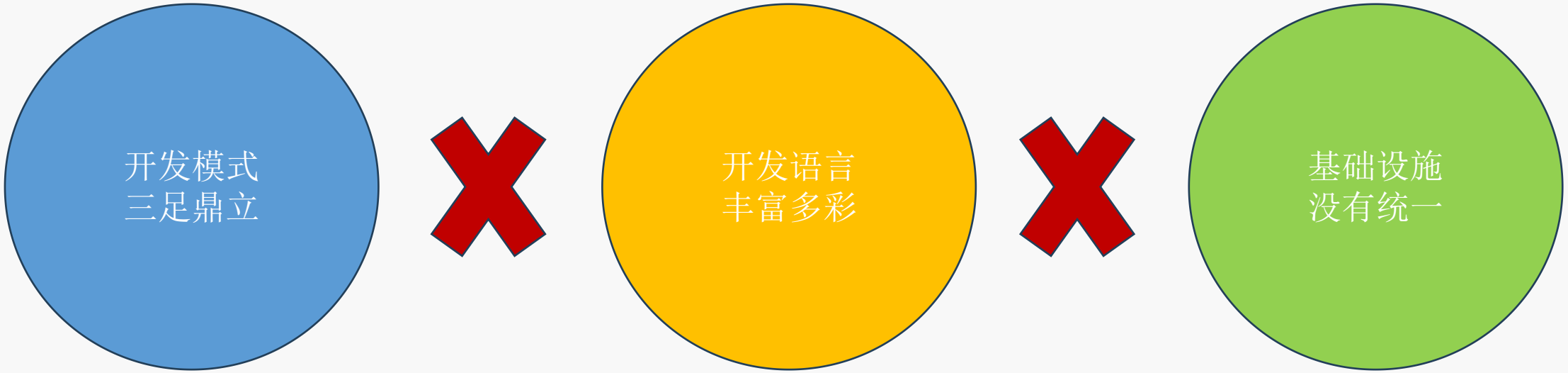
发布流程及平台可能因为业务不同的发展速度，有着不一样的实现方式及存在。



多重混沌带来的巨大挑战

安全工作是建立在现有流程上的，并不应该单独创建新流程，改变原有的研发体系。

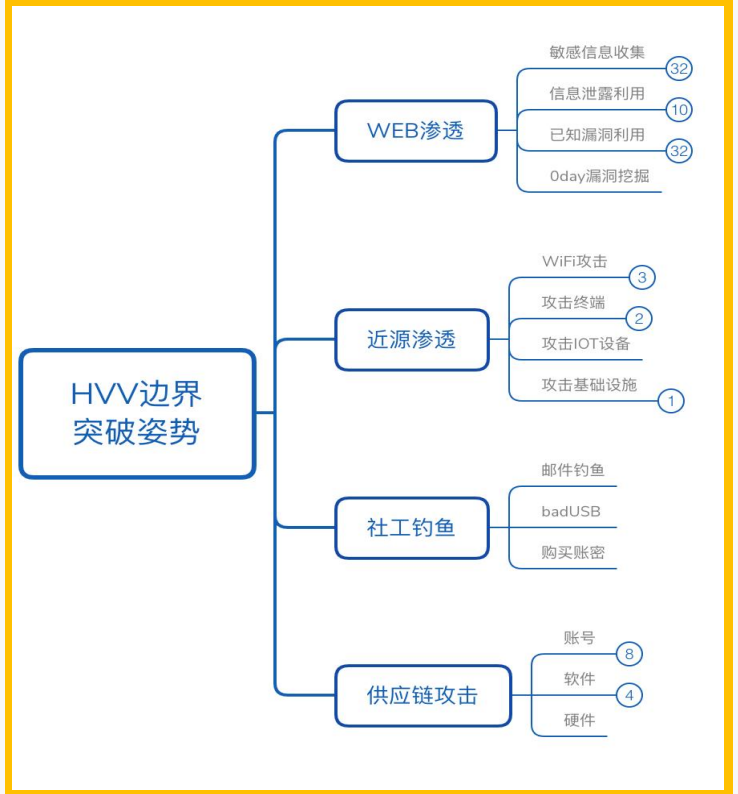
但若是现有流程都没有实现统一，开发安全活动的设计和落地，将找不到抓手，甚至无从下手...



02 从安全角度看软件开发

安全漏洞通常是企业的入口

仅从国家信息安全漏洞共享平台统计，近十年发现漏洞逾**17w**个，平均每年有1.7w个漏洞被发现。



在实战攻防演习中，应用系统经常被用于打点，是突破企业边界安全防护的最佳手法之一。

安全漏洞治理早已是行业讨论最多的话题，在国家层面已经对漏洞管理做出明确要求。


ICS 35.040
L 80

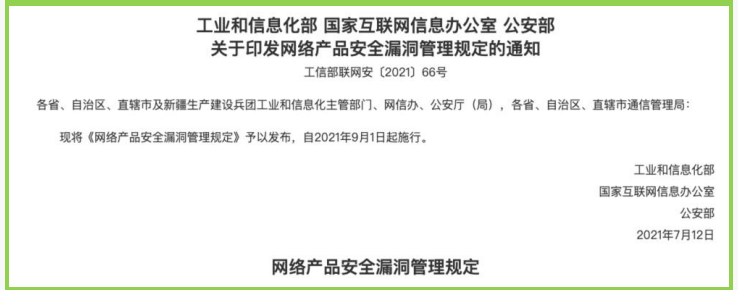
GB

中华人民共和国国家标准

GB/T 30276—2020
代替 GB/T 30276—2013

信息安全技术
网络安全漏洞管理规范

Information security technology—
Specification for cybersecurity vulnerability management


工业和信息化部 国家互联网信息办公室 公安部
关于印发网络产品安全漏洞管理规定的通知

工信部联网安〔2021〕66号

各省、自治区、直辖市及新疆生产建设兵团工业和信息化主管部门、网信办、公安厅（局），各省、自治区、直辖市通信管理局：

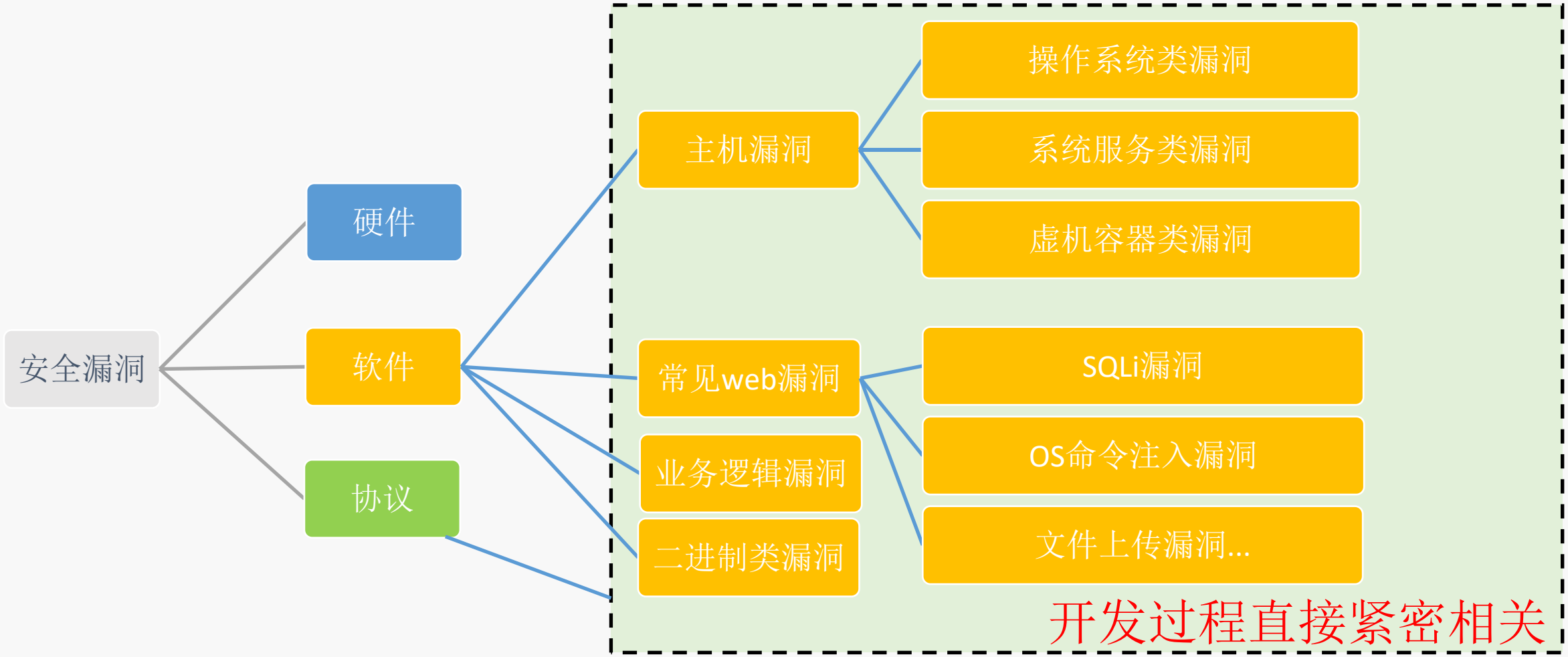
现将《网络产品安全漏洞管理规定》予以发布，自2021年9月1日起施行。

工业和信息化部
国家互联网信息办公室
公安部
2021年7月12日

网络产品安全漏洞管理规定

什么是安全漏洞？

安全漏洞定义：硬件、软件、协议的具体实现或系统安全策略上存在的缺陷。



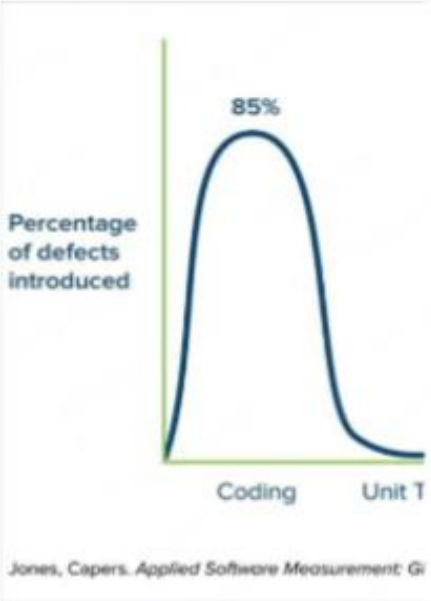
怎么切入做开发安全？

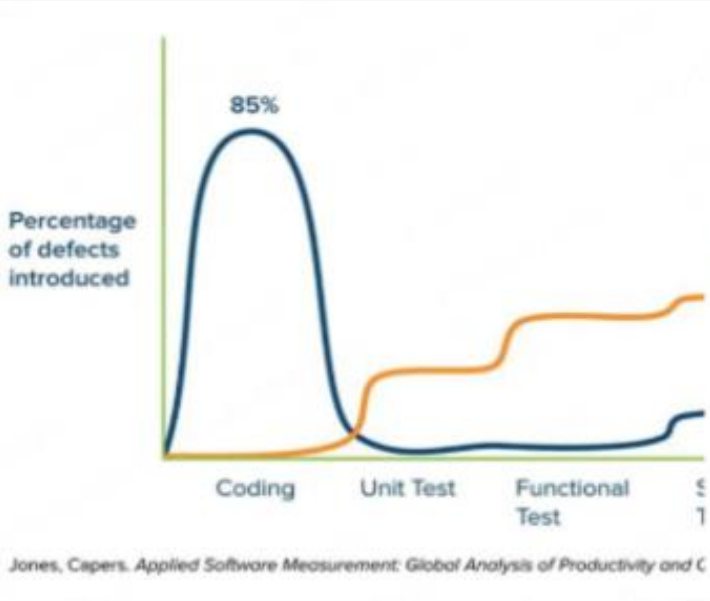
Capers Jones Applied Software Measurement : Global Analysis of Productivity and Quality

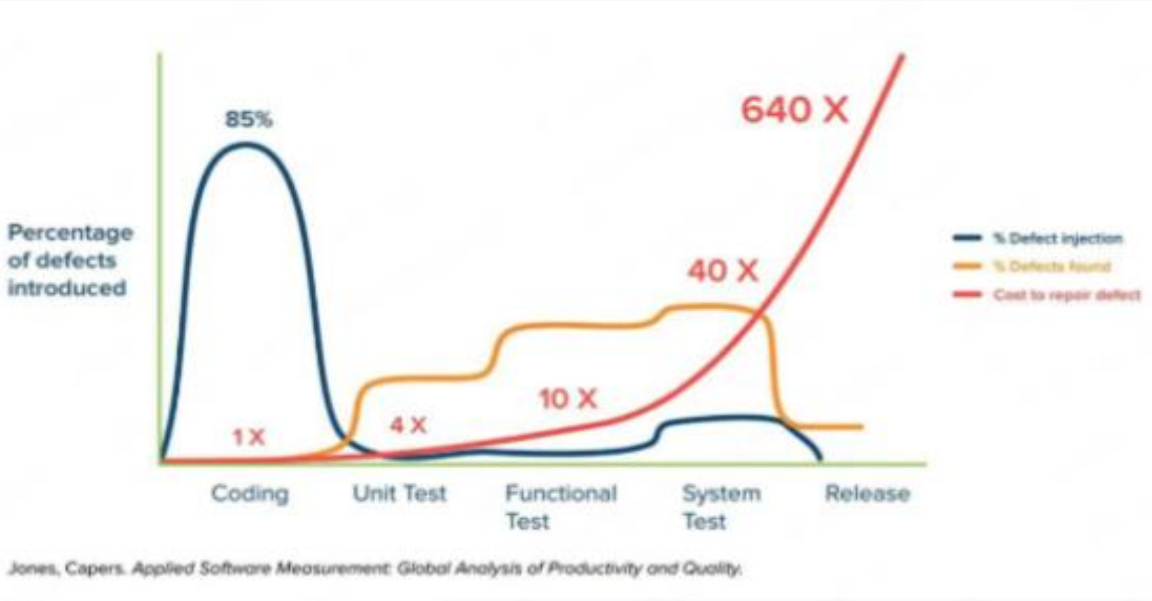
1、85%的缺陷都是在开发人员编码时引入；

2、目前大多缺陷都是在测试阶段发现；

3、缺陷的修复工作越往后成本越大。



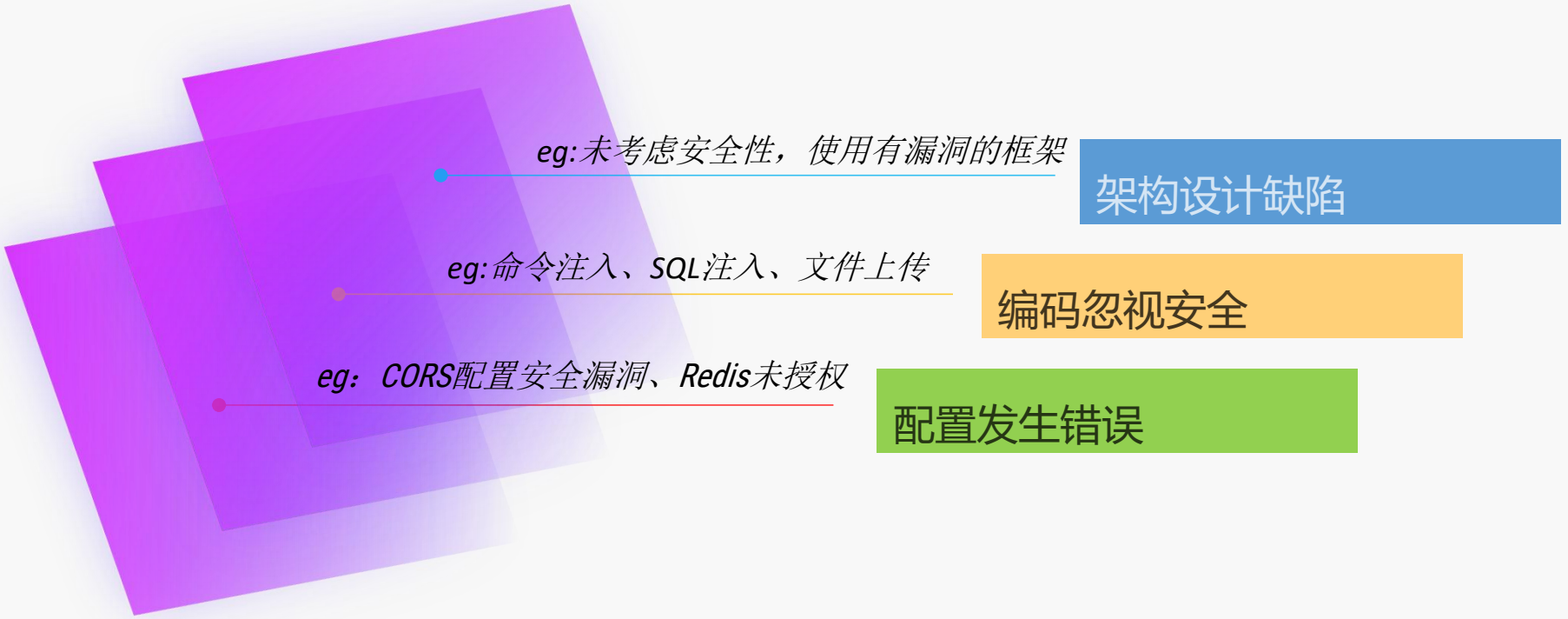




开发过程中，安全漏洞的生产源

有时候，还没开始写代码，就已经引入了漏洞；

有时候，写完提交了代码，还是会有漏洞产生。



开发过程中，安全漏洞的治理

开发安全是一个体系化的工程，包括“发现-验证-修复-复盘”及常态化运营等环节。

03 开发安全的关键要素

谈论开发安全时，应该关注什么？

安全不要新造流程！安全不要新造流程！安全不要新造流程！

安全融入开发流程！安全融入开发流程！安全融入开发流程！So...

序号	开发模式	模式特点	安全模型	安全需求特点	安全责任	治理原则
1	瀑布模式	1、开发周期长 2、每个阶段目的明确，参与人员仅需专注个人部分	SDLC	1、重视过程文档，重人力投入执行缓慢	安全团队	1、设计原则一样 2、部分方法一样 3、融入流程不同
2	敏捷模式	1、开发周期短 2、以客户需求为导向，强调团队之间的高度协作	DevSec	1、强调快速迭代，**自动化**为最基本需求	安全团队、研发团队	
3	DevOps模式	1、同上 2、在敏捷的基础上，强调运维团队应该纳入协作范围	DevSecOps	1、与敏捷模式需求一致 2、结合云原生特点，出现弹性安全需求	安全团队、研发团队、运维团队（“**人人责任共担**”）	

DevSecOps实施的关键要素

开发安全的落地需要组织、流程、规范和安全检测工具的支撑。

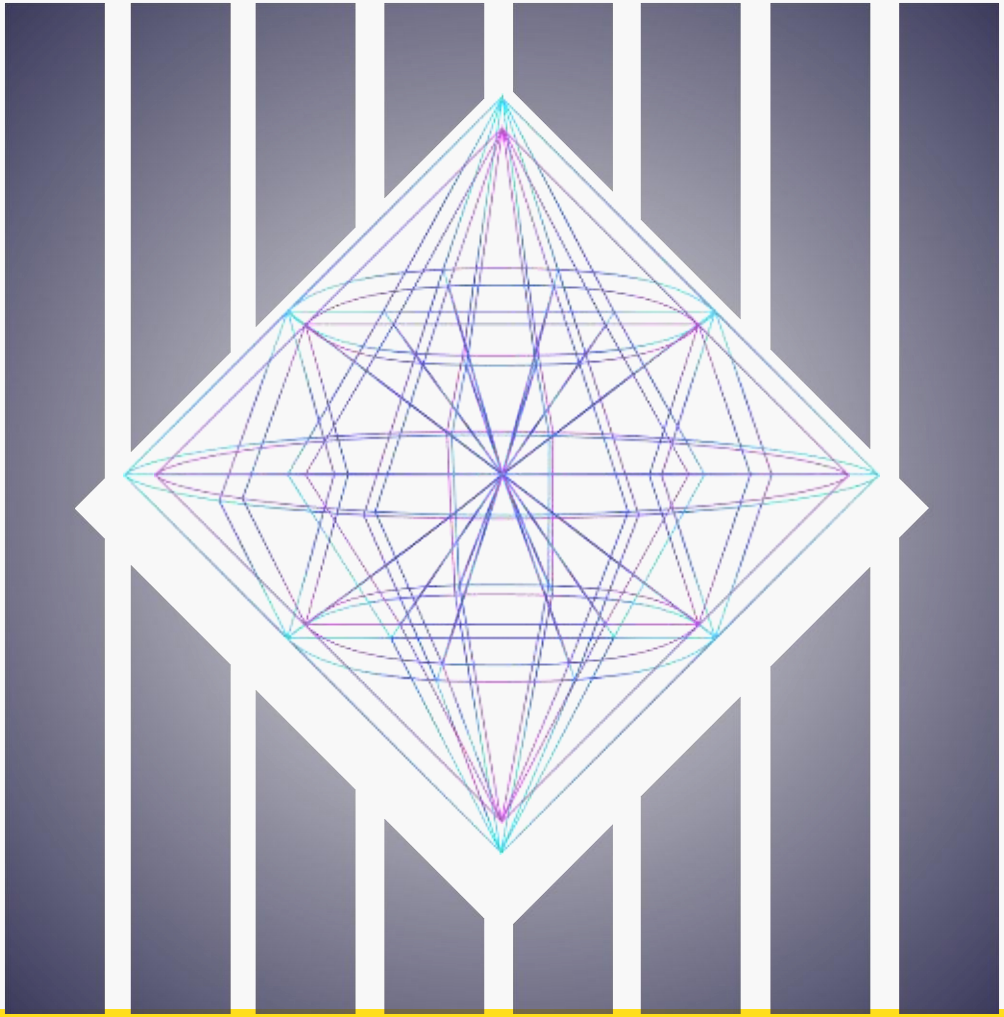
组织架构

安全管理委员会

产品安全团队

产品安全专员

产品安全应急响应小组



安全流程

产品安全提测作业流程

产品安全应急响应流程

产品带病上线绿色流程

产品紧急安全提测流程

安全工具

产品安全管理平台

静态代码扫描工具

开源组件扫描工具

其他安全测试工具

安全规范

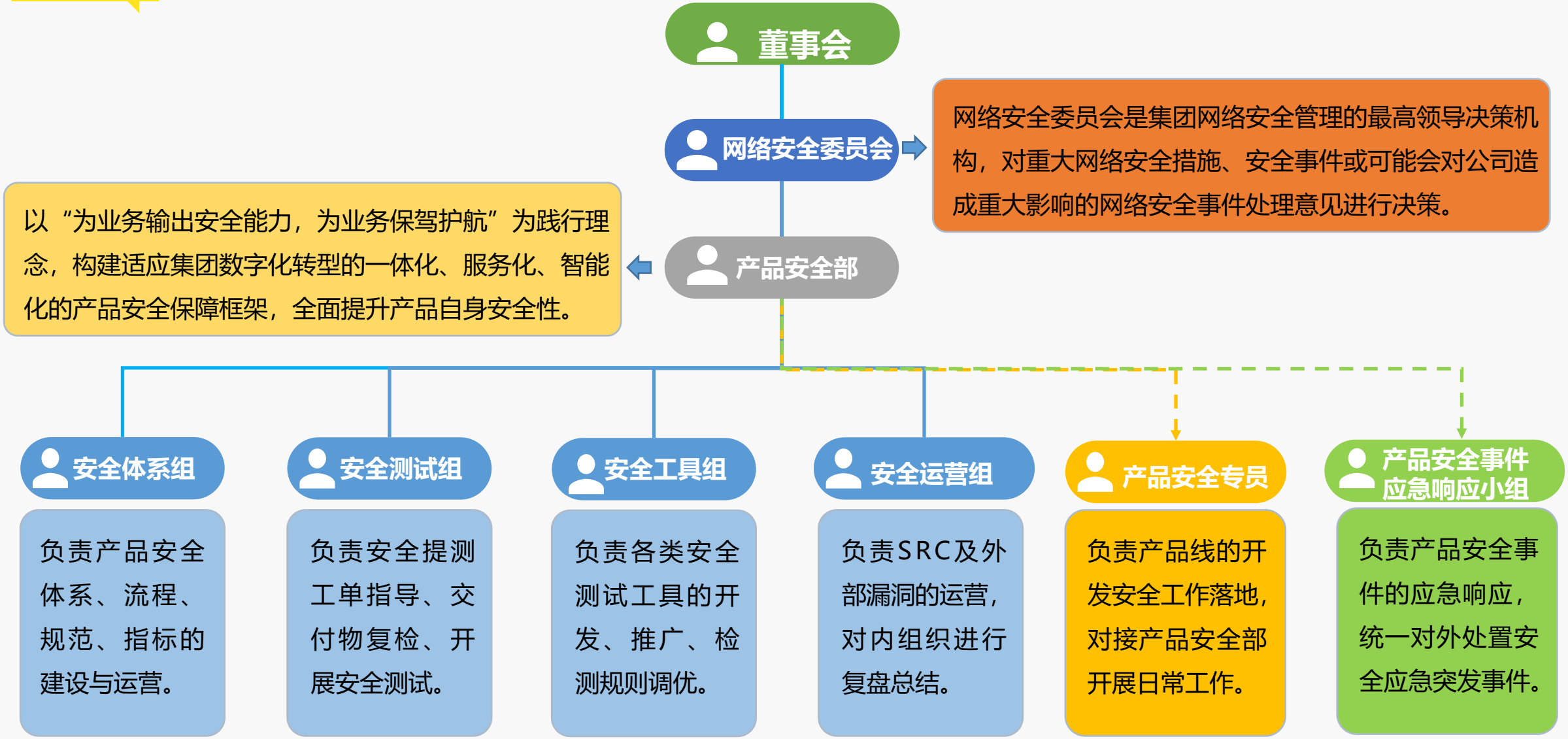
产品安全提测作业规范

安全设计规范

编码安全规范

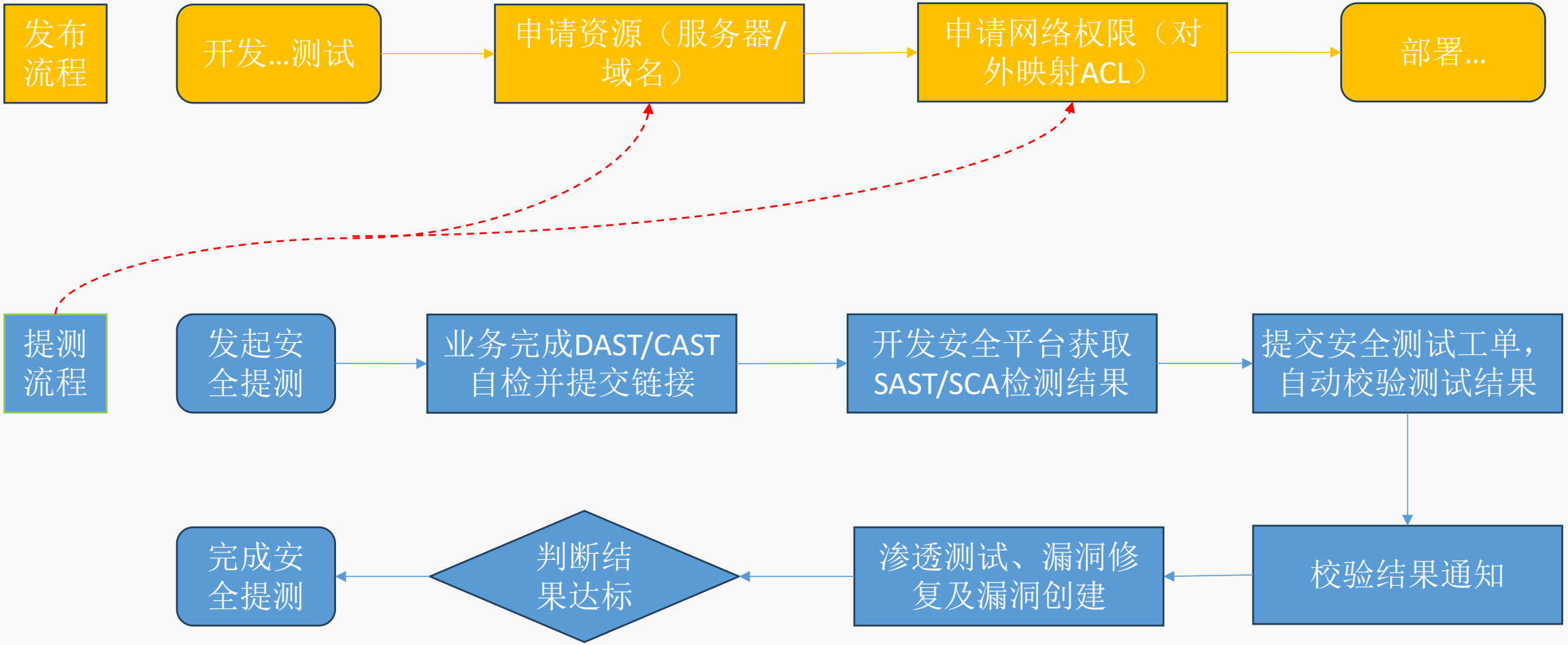
网络安全事件管理办法

组织架构


董事会
网络安全委员会
网络安全委员会是集团网络安全管理的最高领导决策机构，对重大网络安全措施、安全事件或可能会对公司造成重大影响的网络安全事件处理意见进行决策。
产品安全部
以“为业务输出安全能力，为业务保驾护航”为践行理念，构建适应集团数字化转型的一体化、服务化、智能化的产品安全保障框架，全面提升产品自身安全性。
安全体系组
负责产品安全体系、流程、规范、指标的建设与运营。
安全测试组
负责安全提测工单指导、交付物复检、开展安全测试。
安全工具组
负责各类安全测试工具的开发、推广、检测规则调优。
安全运营组
负责SRC及外部漏洞的运营，对内组织进行复盘总结。
产品安全专员
负责产品线的开发安全工作落地，对接产品安全部开展日常工作。
产品安全事件应急响应小组
负责产品安全事件的应急响应，统一对外处置安全应急突发事件。

安全流程

产品安全测试结果，嵌入业务发布流程，业务上线前必须完成安全测试并且达标。典型流程示例如下：

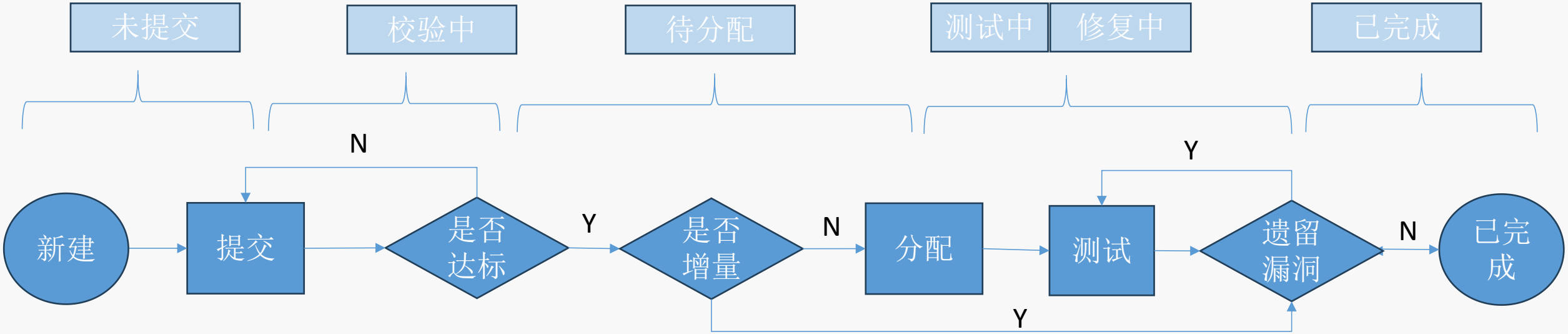


安全工具

需求	设计	开发	测试	运营
1，安全需求checklist（法律/法规、行规及客户相关安全要求，可集成到安全平台中做成业务场景问卷）；	2，安全设计checklist（可集成到安全平台中做成交互式问卷）； 3、威胁建模工具；	4，静态代码扫描（SAST）； 5、开源组件扫描（SCA）；	6，主机安全扫描（DAST）； 7、web漏洞扫描（IAST/DAST）； 8、客户端安全扫描（CAST）； 9、容器镜像扫描；	10，SRC平台； 11，PSIRT平台； 12，开源软件运营平台。

04 混沌模式下的开发安全解决之道

一个安全提测工单的生命周期



业务方
- 填写项目信息
- 填写自检信息

PSM平台
- 检查信息规范

PSM平台
- 检查测试结果
- 通知检查结果

业务方
- 根据通知整改
- 再次提交工单

PSM平台
- 创建漏洞工单（允许SCA和CAST存在延期修复的漏洞工单）

安全人员
- 分配全量工单
- 抽查自检结果
- 开展人工测试

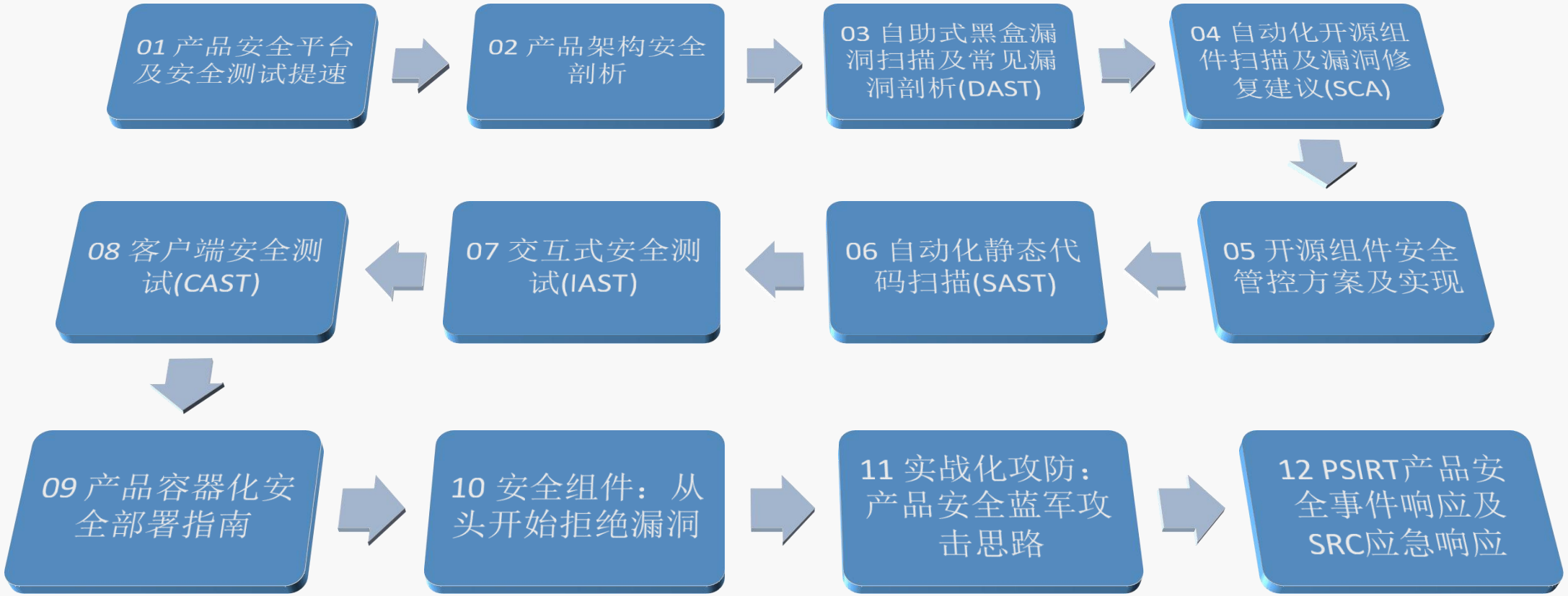
业务方
- 修复已知漏洞
- 申请绿色通道

安全人员
- 评估潜在风险
- 审核特批申请

安全培训赋能

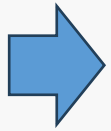
产品安全专员必参加，带动产线其他人参加

联合研发学院做分享，全公司内部进行普及



开发安全运营

一切围绕软件安全质量提升的工作，都属于开发安全运营。包括但不仅限于：



安全指标	安全测试覆盖率　安全漏洞检出率 次均安全漏洞数　非自主高危漏洞数
安全事件	启动应急响应　检出情况分析 防护方面验证　安全测试回顾
复盘总结	定位问题　剖析原因 改进计划　跟进落地

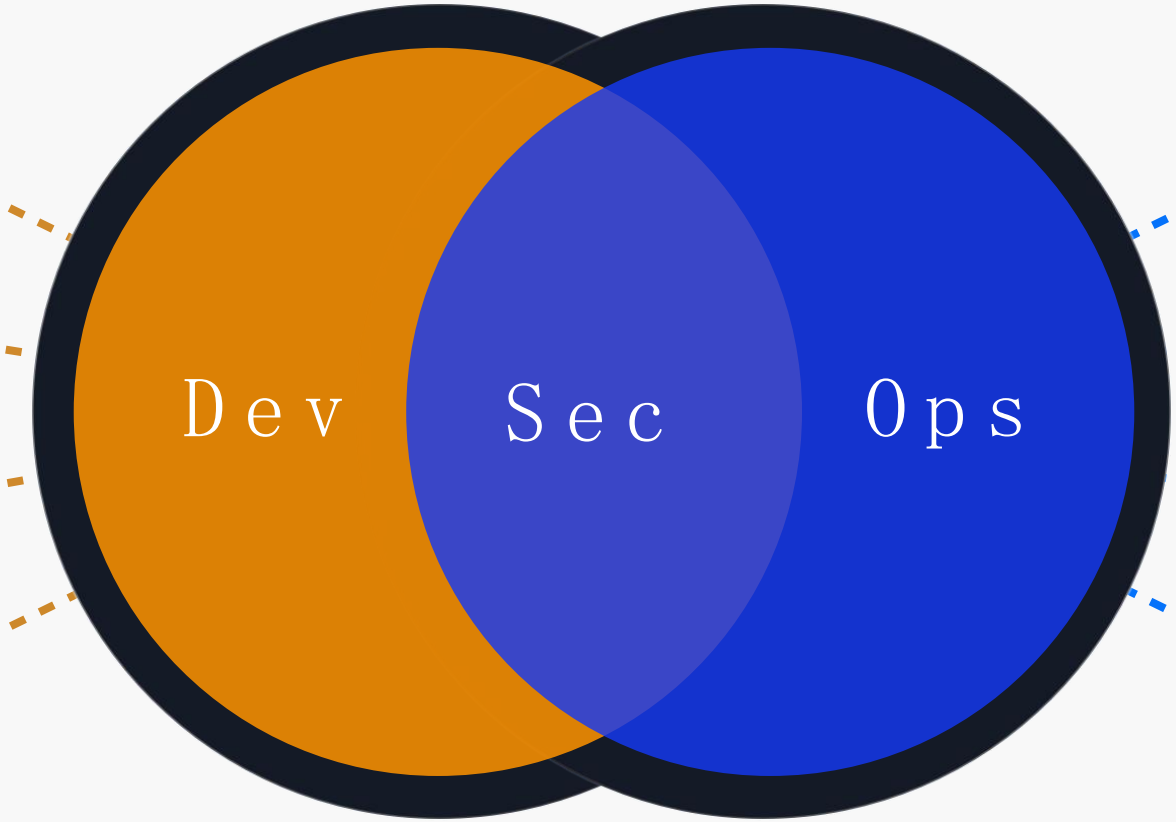
从SDL到DevSecOps的一些建议

SDL和DevSecOps在本质是一样的，离不开组织、流程、规范和工具的支撑

从开发模式转向DevOps的过程可能比较漫长，安全需要做好持久战的准备

建立开发-安全-运维责任共担的有效方式包括培训、技术分享和定期开会

安全团队需要提供安全能力和方法给有能力的业务方，比如安全工具的API



安全工具融入开发流程是多种模式并存的，最佳是同步测试，次之为异步

安全流程与规范的设计，可以参考行业做法、标准规范，但一定结合实际

在建设完开发安全体系后，重点要转向运营并持续向左、流程、规则反馈

CI/CD研发基础设施涉及大量敏感信息，已经成为攻击队的首选目标之一

Thank you!