网络安全创新大会
Cyber Security Innovation Summit

从DevSecOps看安全产品的自身安全

聂君　奇安信集团

演讲大纲

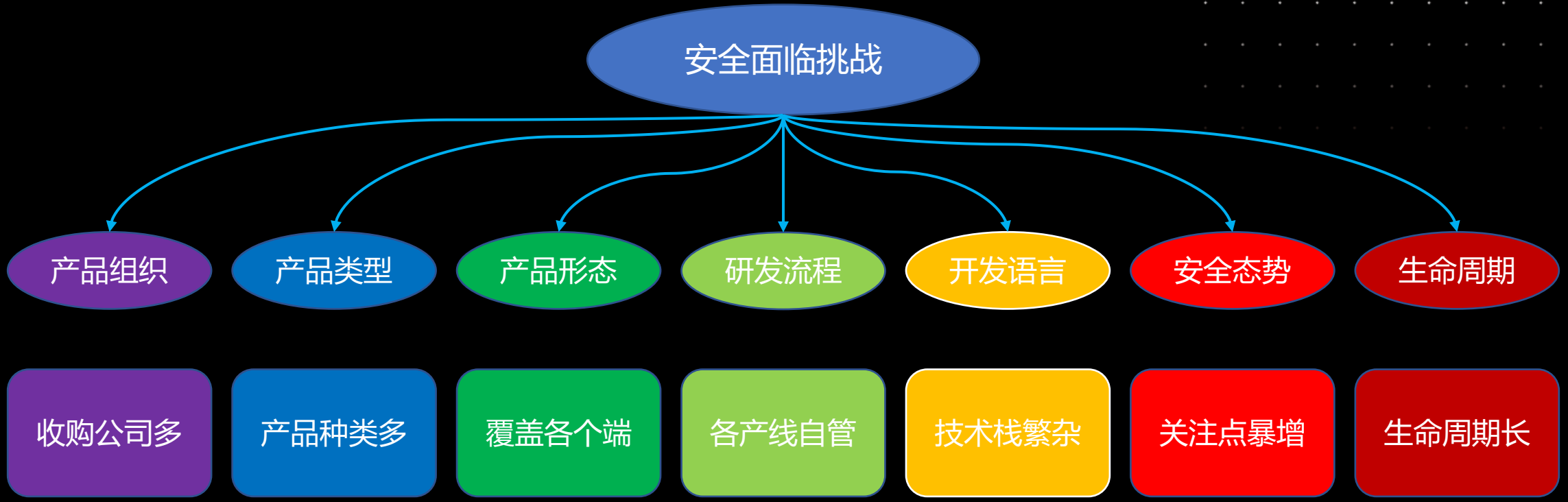
网络安全创新大会
Cyber Security Innovation Summit

1 硬件盒子产品现状

2 产品安全与DevSecOps

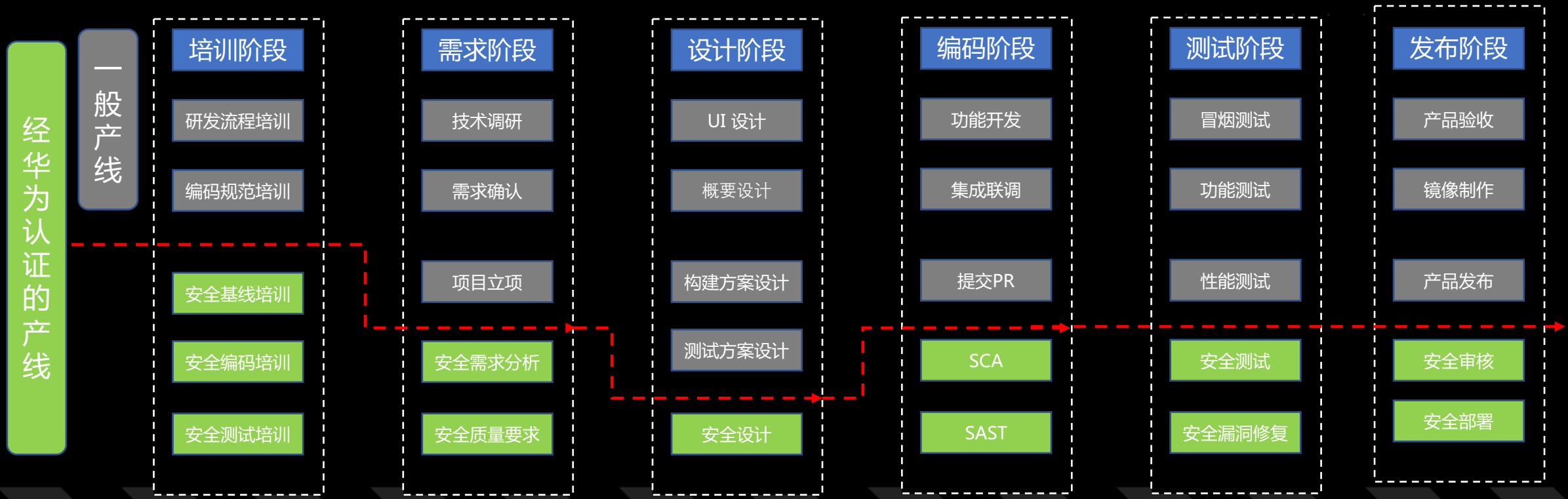
3 产品安全实践建议

硬件盒子产品现状


安全面临挑战
产品组织
产品类型
产品形态
研发流程
开发语言
安全态势
生命周期
收购公司多
产品种类多
覆盖各个端
各产线自管
技术栈繁杂
关注点暴增
生命周期长

产品组织

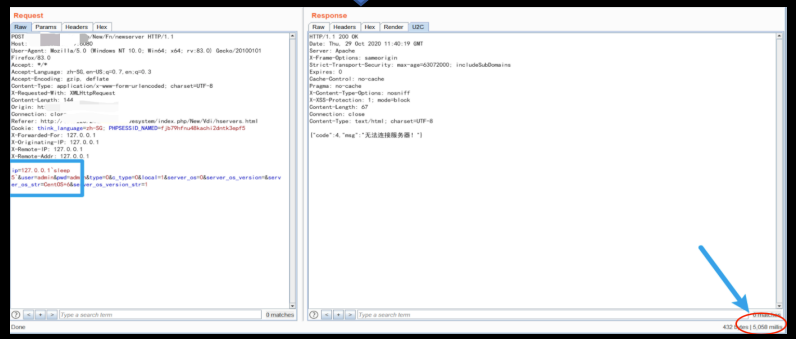
- 不同产品线/子公司，不同的安全水位
- Dev-Ops相关人员的安全意识和安全能力差异较大

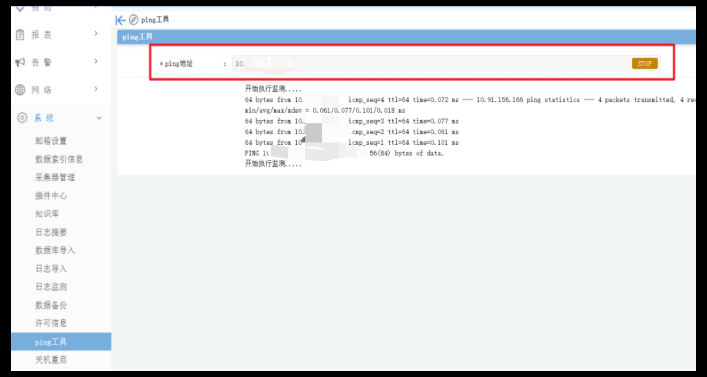


产品类型

- 产品种类多，需要理解的安全场景也多
- 安全需求与正常功能相矛盾，特别是存在命令注入的场景

用户名处存在命令注入，sleep 4s



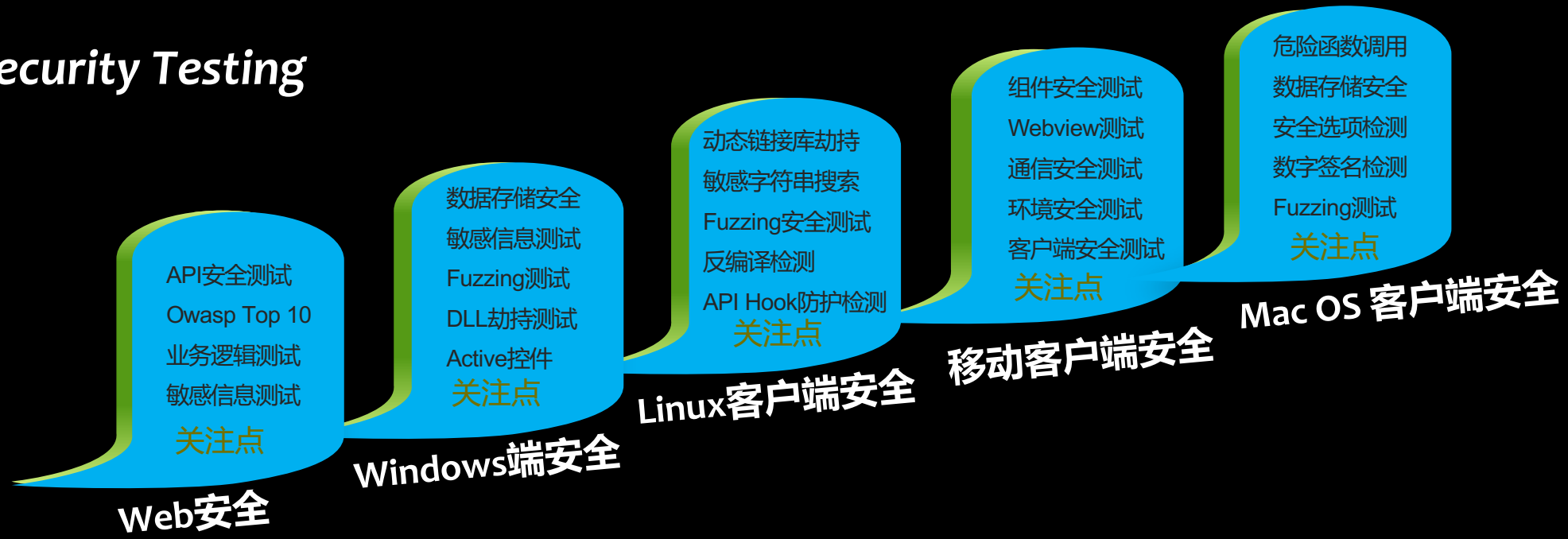


系统- ->ping地址功能处存在命令注入

系统- ->日期与时间功能处存在命令注入

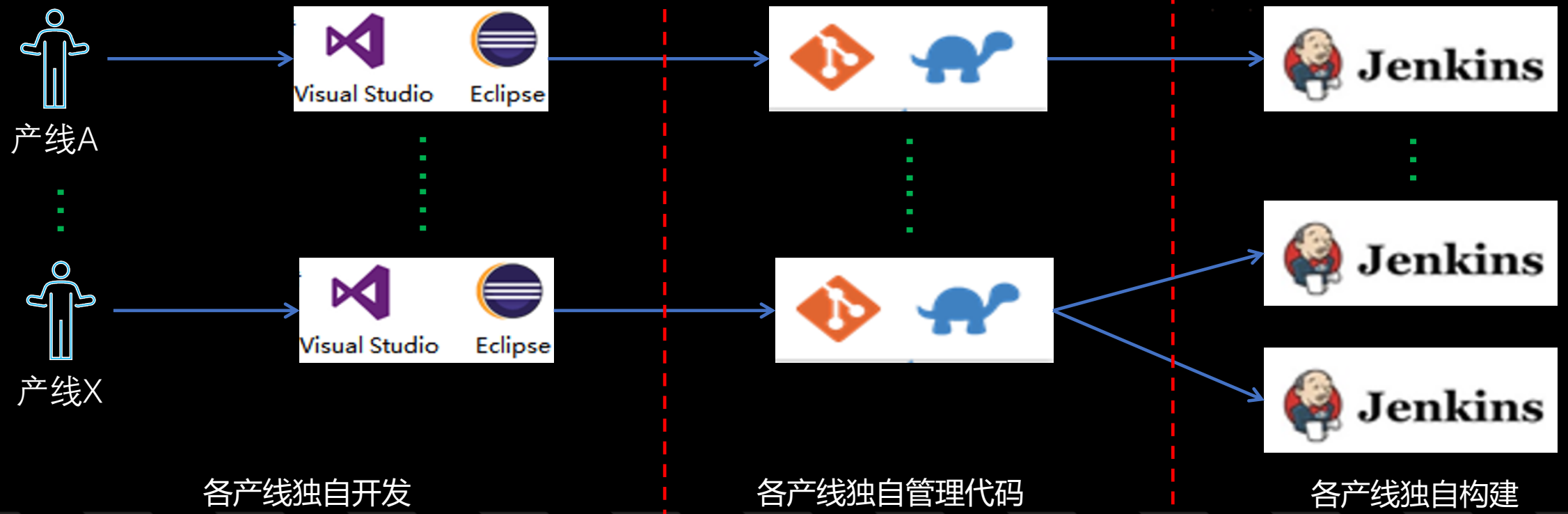
产品形态

- 从客户端到服务端，基本上都有覆盖
- 从国产arm操作系统到Windows、Linux、Android、iOS、MacOS，安全测试技术面临挑战



研发流程

- 各产品线自主管理代码，打包、发版未统一
- 无统一发布平台，上线前的安全卡点难嵌入

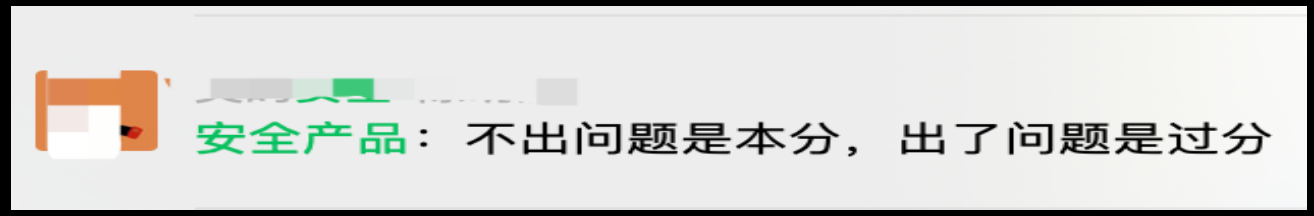


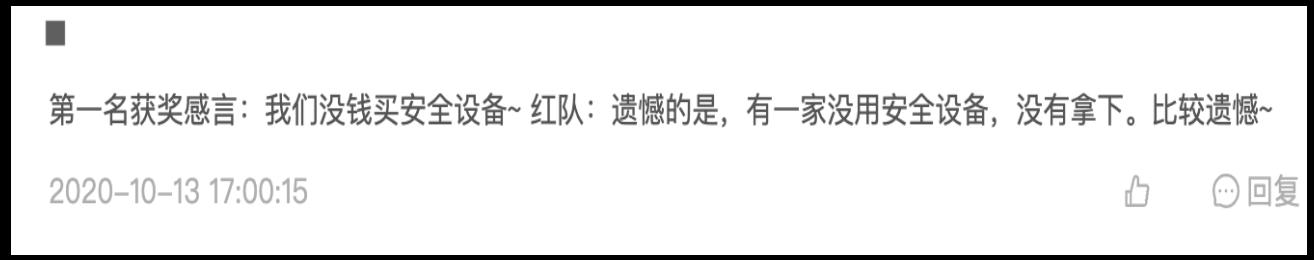
开发语言

- 各类开发语言应有尽有，代码审计难度大
- 各类开发框架均有涉及，难输出安全SDK

安全态势

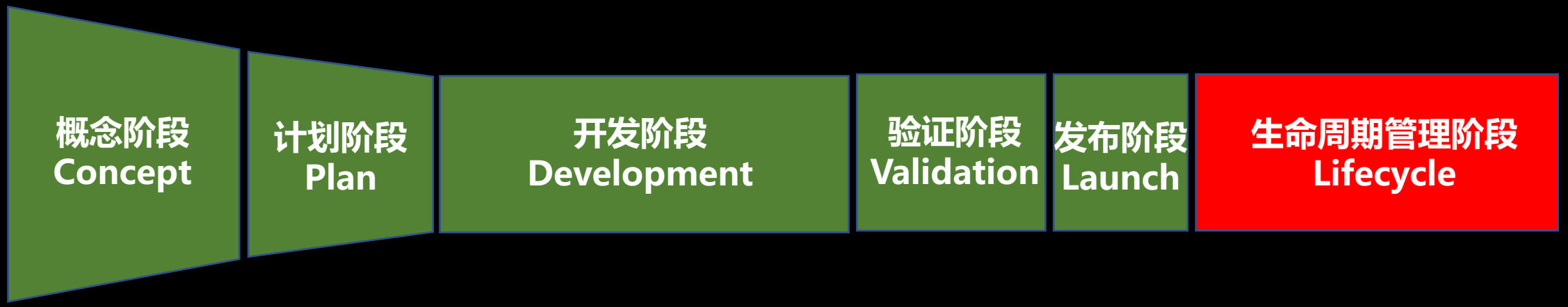
- 本身安全问题也较多，安全起步晚，高危漏洞突出，比如：RCE（SQL Injection、OS Injection）
- 实战攻防重点靶标，漏洞影响被无限放大，关注度高





生命周期

- 产品生命周期长，从物料到下市，整个环节对外暴露攻击面多
- 多年前的老版本、已下市产品被爆漏洞，管理和维护的难度大



产品生命周期就是产品从进入市场到退出市场所经历的市场生命循环过程，是IPD流程的最后一个阶段。

产品下市后，客户侧或对公网暴露的产品，依旧会遭受攻击。SRC 有时还会收到下市几年的产品漏洞。

演讲大纲

网络安全创新大会
Cyber Security Innovation Summit

1 硬件盒子产品现状

2 产品安全与DevSecOps

3 产品安全实践建议

DevSecOp实施关键要素

三个关键要素

文化

产品、开发、测试、运维、安全、项目经理，安全责任共担
人人都为安全负责

流程

产品安全“左移”，安全提测流程、安全质量门限、安全卡点嵌入开发流程和产品管理流程

技术

打造层层检测的安全测试工具链，联动代码仓库和测试环境数据，自动化或联动功能测试进行安全测试

安全产品与DevSecOps

目前大多数安全产品的开发模式为瀑布式开发，极少数产品的服务端逐步转向DevOps。

经过初步摸索之后，安全文化、安全流程基本在产品开发中落地，安全技术特别是自动化方面做得不够好。

安全文化

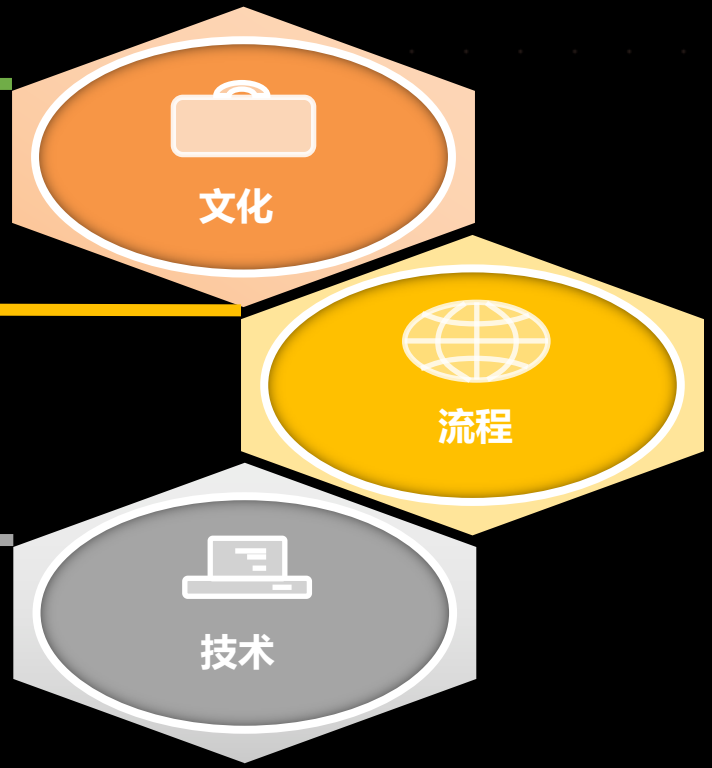
- 安全产品打分
- 安全组织建设
- 发起安全会议

安全流程

- 产品安全提测流程
- TR评审安全检查点
- 外部漏洞处置流程

安全技术

- 黑盒安全测试
- 白盒安全测试
- 人工安全测试



安全文化：安全产品打分

安全得到高层重视，安全元素渗入产品研发，产品技术例会上从安全性、有效性、易用性三方面，对产品进行红黄蓝打分：

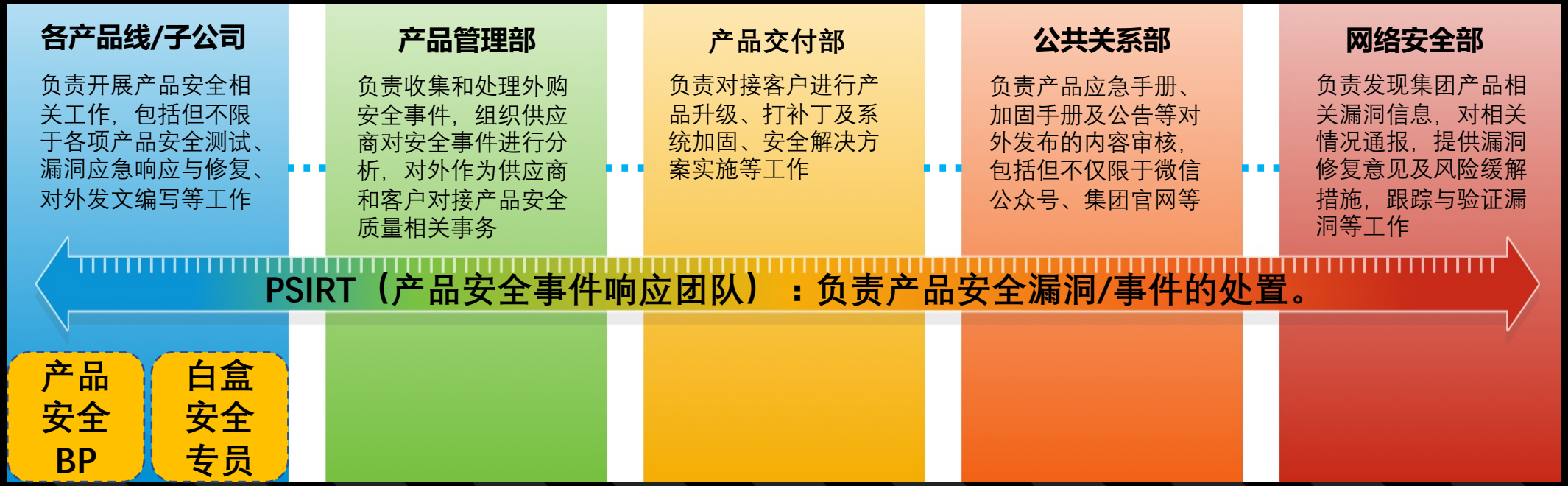
- 红灯：得分区间在【0，60）分
- 黄灯：得分区间在【60，80）分
- 蓝灯：得分区间在【80，100】分

产品评价标准				
评价项	**评价描述**	**评价方式**	**评价分数上限（总分100分）**	**评分细则**
安全性	1.产品使用的应用组件和操作系统是否存在中高危漏洞 2.产品本身是否存在中高危漏洞	产品各项安全测试指标	50分	1.应用组件或者操作系统高危漏洞如果有POC或者EXP，直接扣50分； 2.应用组件或者操作系统高危漏洞如果无POC或者EXP，每个漏洞扣10-20分； 3.应用本身存在高危漏洞，直接扣50分； 4.应用组件或者操作系统或应用本身存在中危漏洞，每个漏洞扣5-10分； 5.同一功能处相同漏洞（高中危）反复出现在不同版本中，每个漏洞扣10-30分。
有效性	1.产品的设计和功能是否满足实际安全建设中的使用需求 2.产品的建设成本 3.产品实际使用中是否存在严重的使用bug，影响产品的落地和推广	企业安全建设产品实验局	30分	1.产品在实际落地过程中符合使用需求的程度 2.产品的部署、推广、配置等建设成本
易用性	1.产品相关文档是否满足日常使用和维护需求 2.产品使用的易用性、是否需要极其专业的人员进行日常的维护	企业安全建设产品实验局	20分	1.文档包括产品使用手册、运维手册、安全配置等
评价要求： 1、产品安全测试过程中，如果发现高危漏洞，则最终评价结果直接为红色；如产品评价期内安全漏洞修复，则不进行扣分处理；				

安全文化：安全组织建立

建立横线与纵向的安全组织，横向打通产品从需求、交付到售后各环节，纵向根据突出问题针对各个产品线建立沟通渠道，实现产品线和安全部门的无缝对接。

- 横向：PSIRT
- 纵向：产品安全BP、白盒安全测试专员



安全文化：发起安全会议

安全文化的落地，不仅从制度、职责、宣传等方面进行落地，更应该加强和安全相关方的沟通，切实关注和解决安全问题。

Dev与Sec之间的Hacking Sec Day

定期或即时沟通安全问题及解决方案

- 产线每月进行安全问题总结
- 本产线新增的安全问题回顾
- 本产线新增的安全需求汇总
- 产线历史问题趋势优化方案

OPS与Sec之间的OPS+Sec联席会

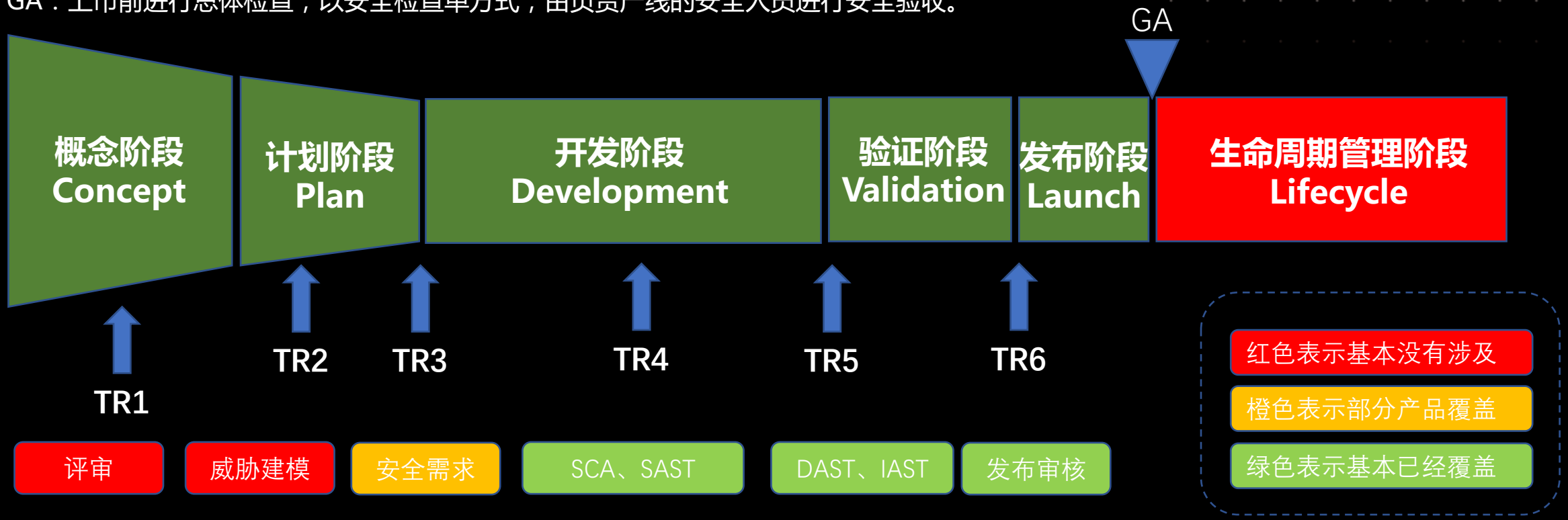
定期或即时沟通安全问题及解决方案

- 每两周进行安全相关工作同步
- 安全事件与安全加固事项沟通
- 系统基础环境安全与配置基线
- 当前基础环境存在的安全隐患

安全流程：安全卡点设置

安全卡点嵌入IPD产品研发管理流程，安全活动主要在TR3-TR6，安全检查主要在：

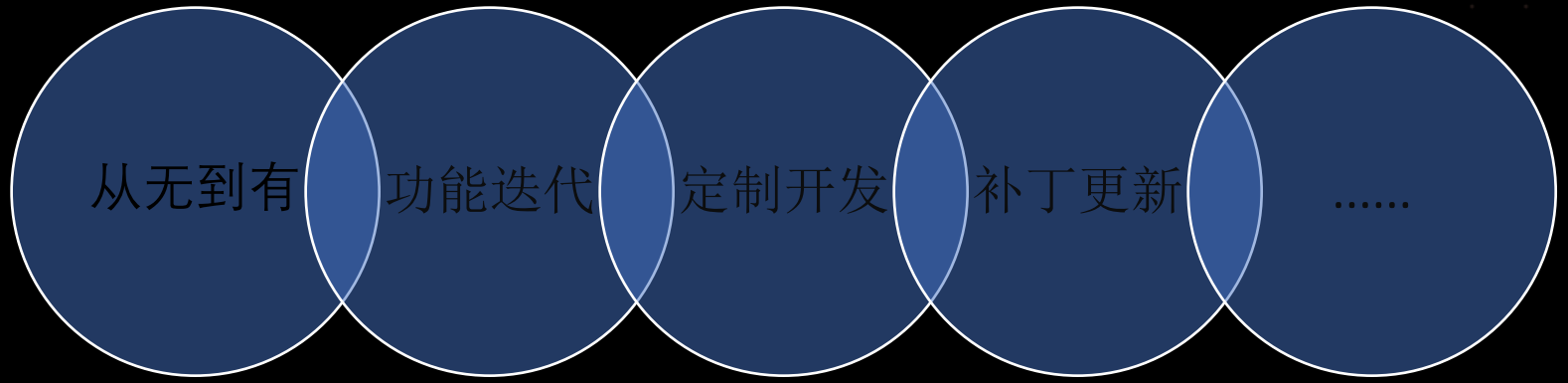
- ✓ TR5：检查各项安全测试情况，部分重点产线涉及到安全需求评审和少量威胁建模场景；
- ✓ GA：上市前进行总体检查，以安全检查单方式，由负责产线的安全人员进行安全验收。



安全流程：安全提测流程

安全提测范围：由集团或下属分公司、子公司研发或者OEM的所有对外发布、销售、提供服务的软件、硬件、云服务、APP、接口等。

安全提测场景：

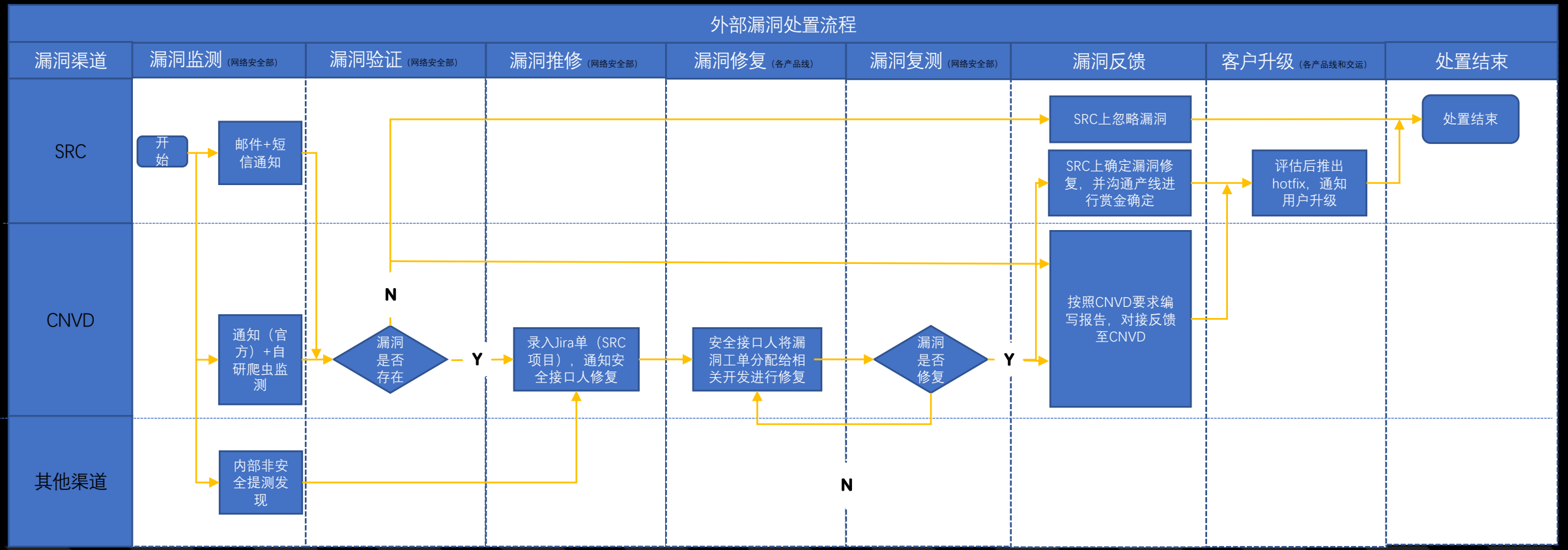


配套安全流程：

- 安全提测插队流程：针对产品提测排队情况，遇到紧急情况可进行安全自测后，找领导请求插队进行安全测试
- 安全提测绿色通道：安全提测后存在高、中危漏洞但仍需要立即上线，走流程申请绿色通道并制定修复时间、责任人、上安全防护措施

安全流程：外部漏洞处置流程

外部漏洞：主要是指非自主发现的漏洞，来源包括SRC、CNVD等渠道接收到的产品漏洞。



安全技术：安全测试工具链

安全技术方面，在安全产品研发运维流程中，常见的一些新技术的应用受到限制，比如RASP不适合装在盒子中。

总体而言，侧重点偏向于白盒安全测试、黑盒安全测试和人工安全测试三方面（以下打钩相关均有涉及，但不深或自动化程度不高）

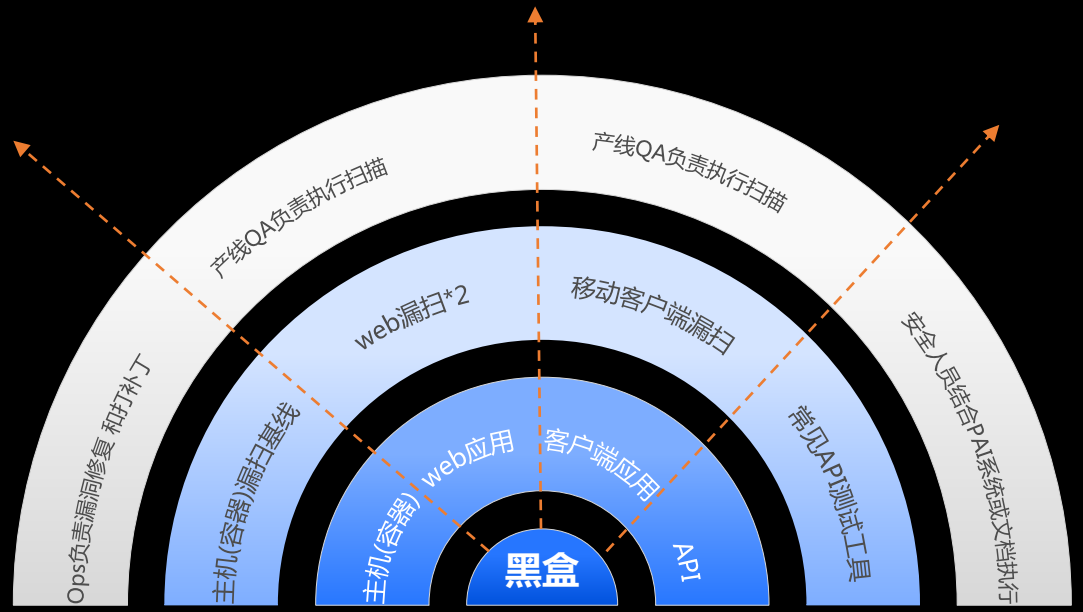
安全技术：白盒安全测试

- 白盒安全测试专员机制：由产线安全专员负责扫描或自动触发扫描，并组织培训对结果进行处理
- 内部安全漏洞Top10规则：梳理内部常见漏洞类型Top10，编写开发安全规范并用工具扫描进行技术check
- 重点产品人工代码审计：在自动化工具覆盖的基础上，周期性的进行人工代码审计

安全技术：黑盒安全测试

黑盒安全测试的落地实践，主要是由单一扫描变为多重纵深扫描，针对API接口专门制定未授权&敏感信息泄露扫描。

- DAST在安全产品中的应用：针对主机-应用-客户端进行安全扫描，web层面交叉进行安全扫描；
- IAST在安全产品中的应用：非严格意义上的交互式安全测试，当前仅为从QA浏览器上导出流量进行测试；
- API未授权和敏感信息测试：需要QA提供接口文档或直接录入API系统，直接或加上参数拼接URI进行访问，查看和过滤response判断。



安全技术：人工安全测试

针对重要产品大版本迭代进行人工安全测试，主要关注：

- 历史漏洞排查；
- 历史漏洞总结，同类漏洞测试；
- 历史漏洞之外漏洞的人工安全测试：
  1、前端加密绕过进行暴力破解尝试
  2、重点关注业务逻辑类漏洞
  3、授权后敏感信息泄漏API
  4、场景化深层次难发现的web漏洞

序号	漏洞类型	漏洞对应场景
1	命令执行	跟IP，时间，文件名，应用服务、协议、网络接口等相关的功能处
2	SQL注入	所有输入的功能点
3	越权漏洞	涉及权限的功能，多级角色、业务逻辑长的功能
4	跨站脚本攻击(XSS)	所有输入的功能点
5	安全配置错误	默认配置，临时配置等功能点
6	跨站请求伪造(CSRF)	涉及添加，删除，修改等功能
7	文件上传	所有涉及文件上传的功能
8	暴力破解攻击	登录，绑定，认证等功能点
9	服务端请求伪造(SSRF)	跟第三方服务器交互的功能点
10	组件版本漏洞	结合SCA结果，再次验证产品中可利用的组件漏洞情况

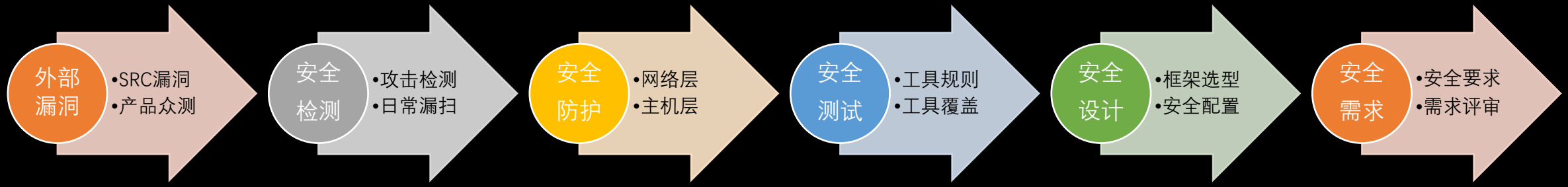
其他产品安全：安全风险收敛

目前通过在IPD流程中嵌入各类安全活动，发动各产品线和OPS承担一定的安全责任，可以在一定程度上将安全风险进行收敛。但面对安全挑战日益严峻的今天，仍旧出现较多的安全问题。从风险控制的角度考虑，典型风险都应该成立专项进行治理，比如：

其他产品安全：安全运营反馈

安全运营反馈：接收到SRC或产品众测的漏洞，逐层向左反馈并检查安全活动的落实情况与盲区。比如：

- 安全检测，白帽子挖漏洞时是否触发告警规则？
- 安全防护，主机安全基线，各类ACL是否失效？
- 安全测试，是否覆盖？安全检测工具为什么没有检测出来？
- 安全设计，安全设计用例是否覆盖，是否执行到位？
- 安全需求，安全需求中是否提及漏洞相关的组件或服务？



从源头开始治理，层层检测，实时监测

演讲大纲

网络安全创新大会
Cyber Security Innovation Summit

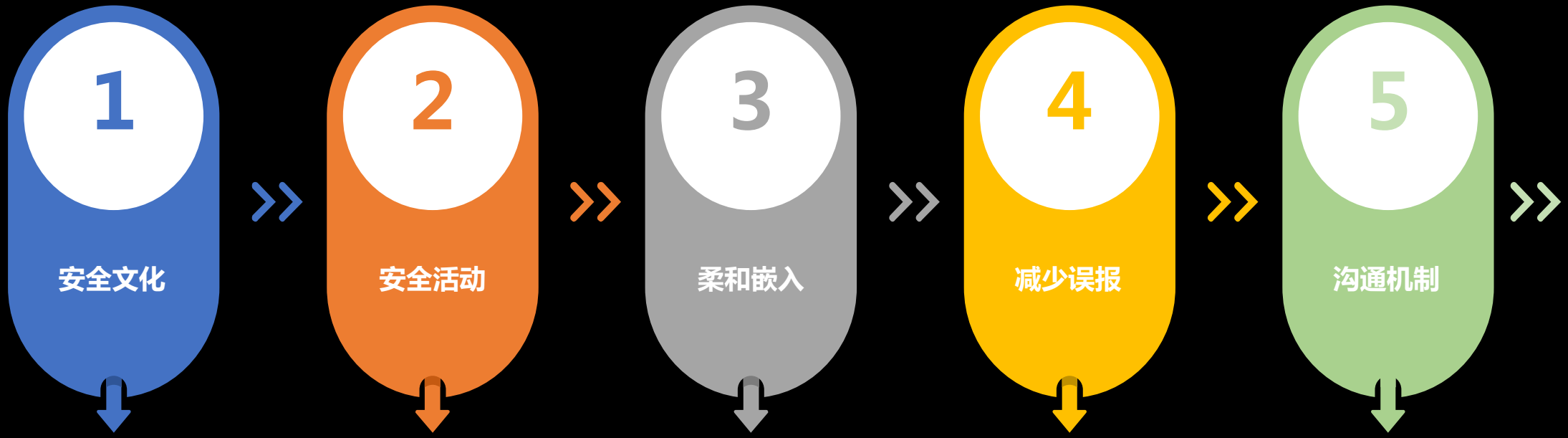
1 硬件盒子产品现状

2 产品安全与DevSecOps

3 产品安全实践建议

产品安全实践建议

没有一家DevSecOps的实践可以原封不动的照搬来拿使用，但是其中的一些安全活动嵌入、安全运营思路、技术难点攻克方法可以借鉴。以下十条实践建议，仅供参考（1至5）：安全文化+安全活动+柔和嵌入+减少误报+沟通机制



产品安全实践建议

十条实践建议（5至10）：

安全工具+供应链安全+基线安全+漏洞闭环+运营反馈

6 安全工具

选择合适的安全工具融入到CI/CD流程，做到自动化和可定制化

7 供应链安全

关注供应链安全问题，包括第三方库与SDK、外购软件及开源组件

8 基线安全

加强应用部署的基线安全，尤其是基础组件的未授权和弱口令等问题

9 漏洞闭环

对漏洞进行分级，抓大放小切勿一次想完成所有已知漏洞的修复

10 运营反馈

持续不断地进行运营反馈，优化现有的流程、安全工具检测规则

网络安全创新大会
Cyber Security Innovation Summit

THANKS