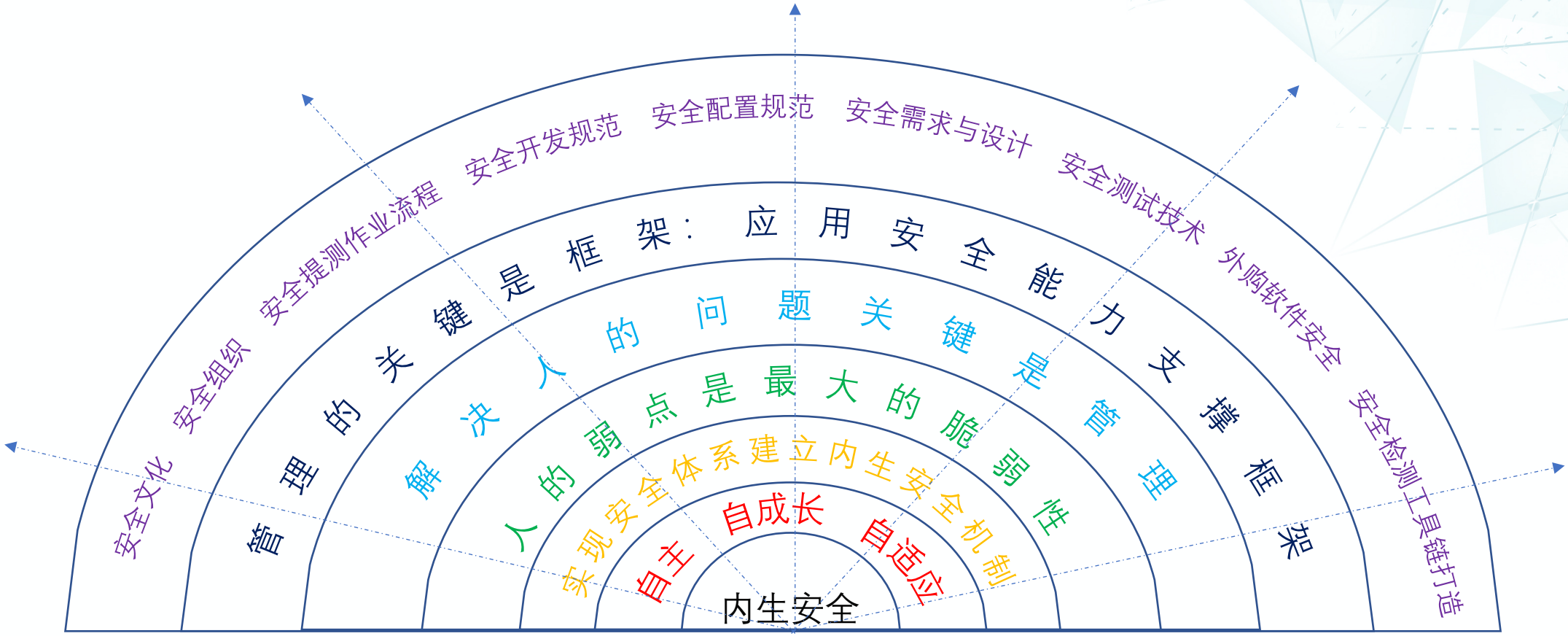
浅谈安全产品的内生安全实践

目　录

内生安全与应用安全


安全文化
安全组织
安全提测作业流程
安全开发规范
安全配置规范
安全需求与设计
安全测试技术
外购软件安全
安全检测工具链打造
管理的关键是框架：应用安全能力支撑框架
解决人的问题关键在管理
人的弱点是最大的脆弱性
实现安全体系建立内生安全机制
自主
自成长
自适应
内生安全

应用安全能力支撑框架建设全景

安全文化

- 培训体系
- 考核机制
- 课件开发
- 培训推广
- 培训指标
- 效果考核
- 钓鱼测试
- 运维安全技能
- 开发安全编码
- 安全测试赋能

检查清单

- 应用运行环境规范
- 基础服务配置规范
- 安全需求checklist
- 框架组件黑白名单
- 应用安全配置清单
- 发布审核核查机制

供应链安全

- 采购安全流程
- 外购软件安全管理
- OEM产品质量安全要求
- 提供基础架构组件清单
- 产品交付安全

DevSecOps

- 工具链建设

SDLC

- 组织建设
- 流程检测
- 工具建设
- 安全需求
- 安全设计
- 安全编码
- 安全运营
- 安全组件
- 开源组件安全

应急响应

- SRC
- 应急流程
- 应急SLA
- 应急SOP
- 生态合作
- 活动宣传
- 智能机器人

漏洞运营

- 漏洞管理办法
- 漏洞闭环流程
- 漏洞发现机制
- 漏洞分析能力

复盘机制

知识库沉淀

目　录

应用安全能力支撑框架差距分析

制定应用安全通用需求测试清单	建立SDLC流程与工作机制，扩大试点产品范围，能覆盖公司80%以上的产品线，能100%覆盖各类语言栈的安全评估，减少工具产生的误报，提高人工审核效率，打通与产品线的沟通机制，实现漏洞48小时内闭环
编写安全编码规范，并推广到应用开发过程中	
依托安全编码规范，建立基础安全开发库，并推广使用	
建立包含SAST、DAST、IAST的AST平台	
建立软件组件分析平台，集合漏洞情报和应用清单，快速准确发现漏洞	
开发框架、中间件和通用库黑名单机制	

SDLC安全控制机制

在开发、测试、运维等相关组织中建立良好的安全文化	建立应用安全培训体系，研发实训课程，内容可100%覆盖内部业务领域，一方面对部门内部人员提升专业技能，另一方提升企业员工的安全意识
建立安全需求与设计课程并推广落地	
建立安全开发课程并推广落地	
建立安全测试课程为各业务线测试赋能	

安全文化建立和培训体系

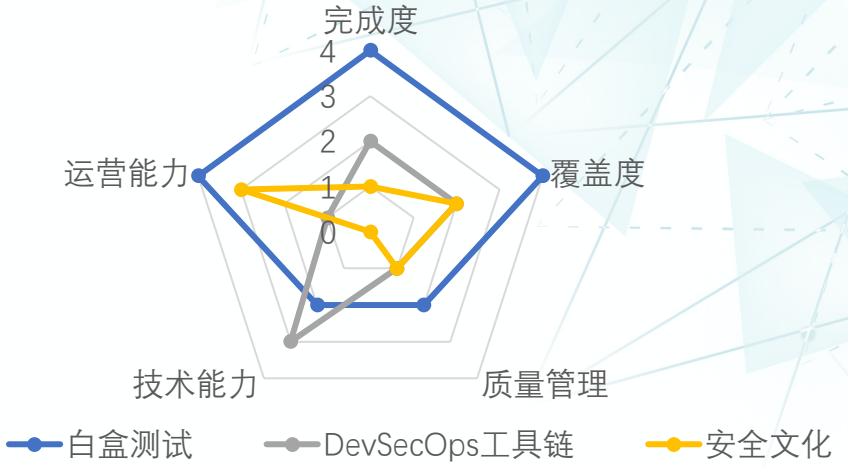
建立内外部漏洞收集渠道	建立web漏洞运营体系，在应用上线前经过安全提测，上线后持续进行安全测试，同时借助白帽子的力量协助漏洞发现，及时将漏洞修复闭环，最终实现线上应用无漏洞
漏洞评级，修复优先级	
漏洞与资产建立关联，实现漏洞匹配到人	
漏洞复测与验证	
建立风险全流程管理体系，黑白名单管理，持续监测	
漏洞知识库建立(有配套的漏洞和配置修复方案)	

内外部漏洞运营体系

应用安全能力支撑框架演进路线

差距分析

- 缺少安全组织，工作推动和漏洞应急闭环能力不足
- 常规漏扫和漏洞情报产生的漏洞修复慢
- 开发人员的安全技能和意识薄弱
- 静态代码扫描漏洞多，白盒代码审计能力需提升
- 安全测试吞吐量不强，推广sdlc阻碍业务上线



演进路线

Part 1

- 建立PSIRT组织，推动漏洞高效闭环
- 从流程上设计并完善安全组织架构

Part 2

- 加强与研发的沟通，渗透安全理念
- 持续推进人员培养，提升白盒挖掘能力

Part 3

- 打造SAST、DAST、IAST平台能力
- 建立工具链并完善，打通DevSecOps

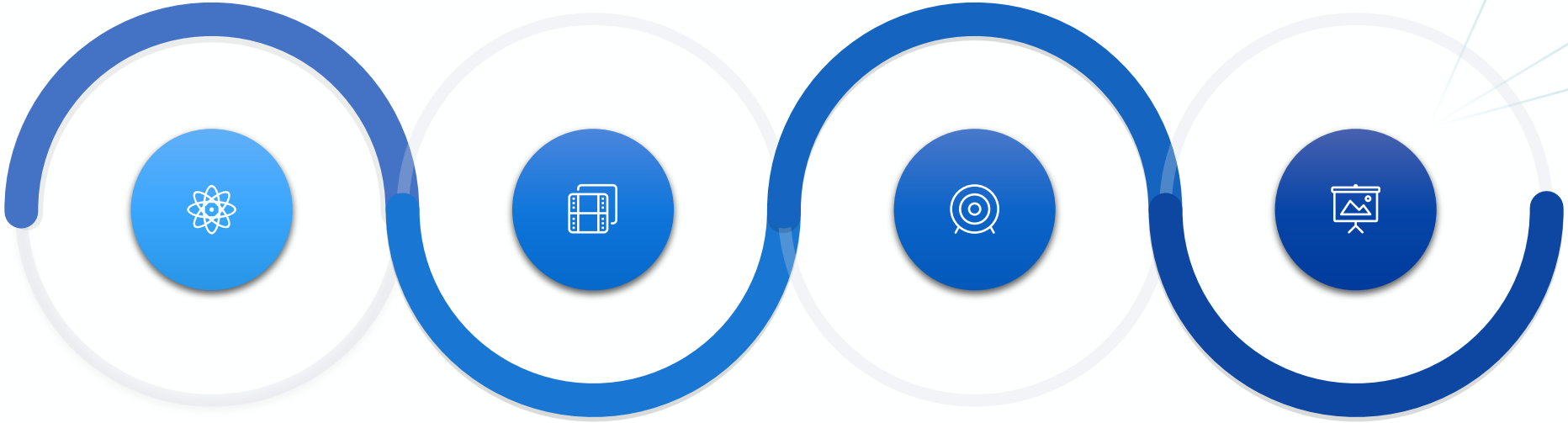
内生安全落地实践模型V1.0

安全培训

安全设计 (TR3)	安全编码	安全测试	发布审核 (TR5)	线上运营
1、根据安全设计checklist完成安全设计自查 2、受攻击面分析（选做） 3、STRIDE威胁建模（选做）	1、根据安全开发规范进行安全编码 2、**编码结束后**自主安全扫描： 1）静态代码扫描 2）第三方开源组件扫描 3）Web应用漏洞扫描 4）扫描报告解读分析 5）解决高中危扫描漏洞	1、**冒烟测试通过后**提交安全测试工单 2、安全测试 1）验收各项安全扫描报告 2）自主安全扫描结果复测 3）人工安全测试 3、安全漏洞修复 4、安全漏洞复测	1、无高中危漏洞后申请上线发布/项目交付 2、验收总体安全评估情况，并确定安全是否pass 3、遗留高中危漏洞，须申请特批流程*	1、线上业务系统发现新漏洞，由网络安全部通知产品线研发进行修复 2、各产品线研发响应： 12小时完成严重漏洞修复 24小时完成高危漏洞修复 3个工作日完成中危漏洞修复

内生安全落地实践：文化

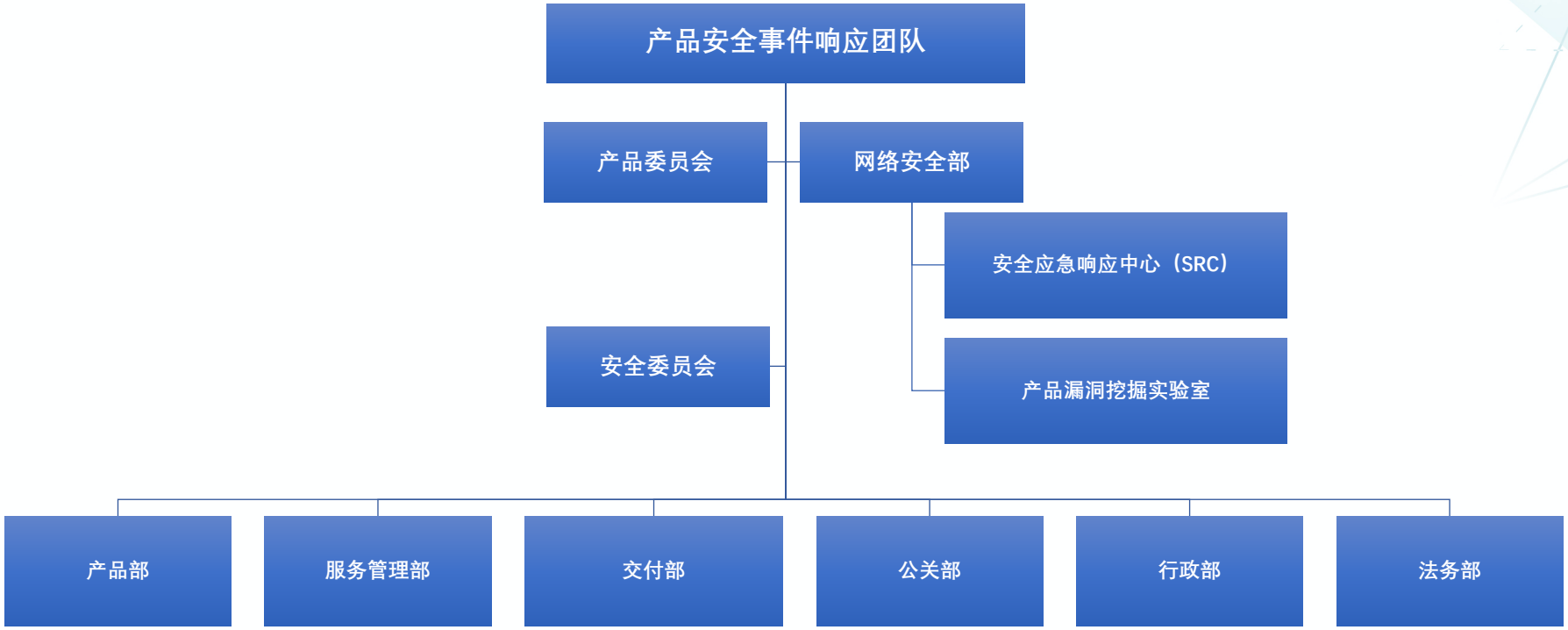
- 产品自身的安全与研发运维流程中的各个环节、每个人都息息相关，筑建产品的安全是每个人的责任。
- 通过内部宣贯、培训、建立部门BP、Hack Sec Day等方式，从组织、职责、重要性、必要性等方面来营造安全氛围。



安全制度宣贯　安全意识培训　部门BP制度　Hack Sec Day

内生安全落地实践：组织

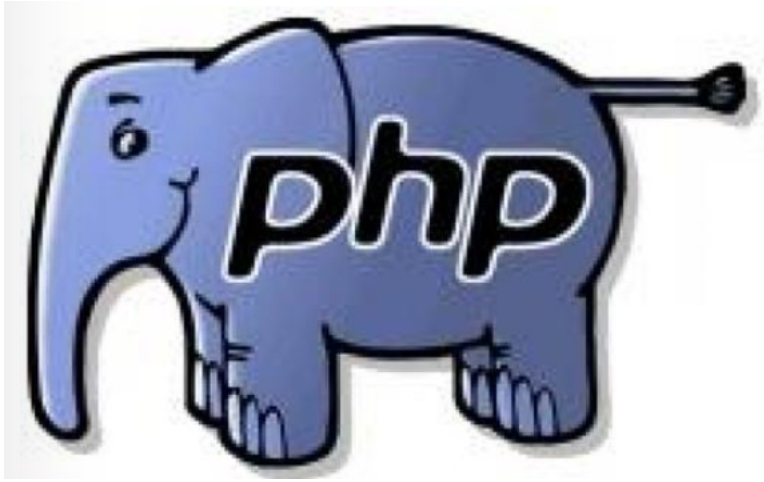
- 建立产品安全事件响应团队，负责产品安全漏洞/事件的处置。

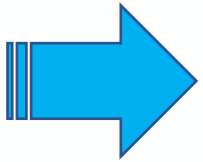


内生安全落地实践：流程

内生安全落地实践：技术

- 从框架安全开始治理



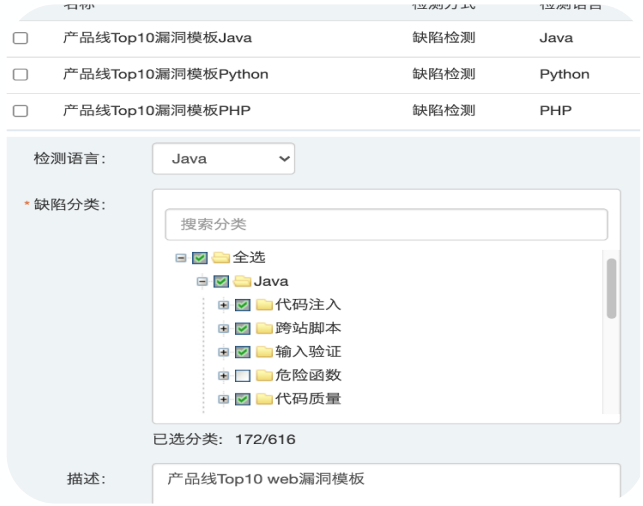


- 防抓包：grpc接口通信
- TLS证书两层CA体系设计
- CSRF天生免疫
- SQLi在中间层做处理
- ……

内生安全落地实践：技术

- 优化/安全检测工具 - - SAST规则精简

默认规则
除去非安全相关为524条



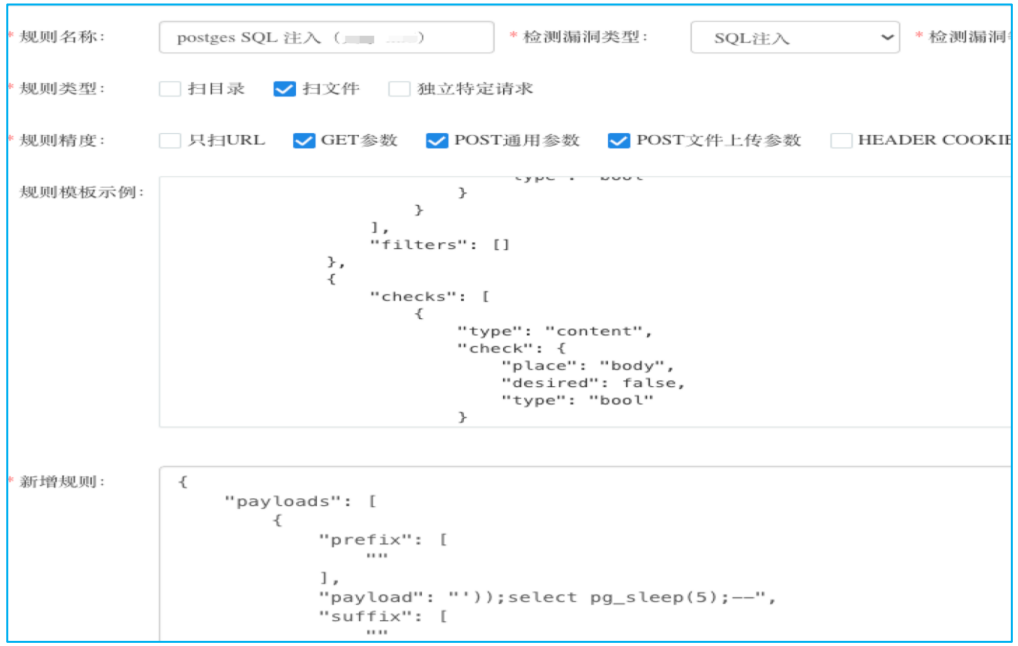
Top 10
检测规则为172条

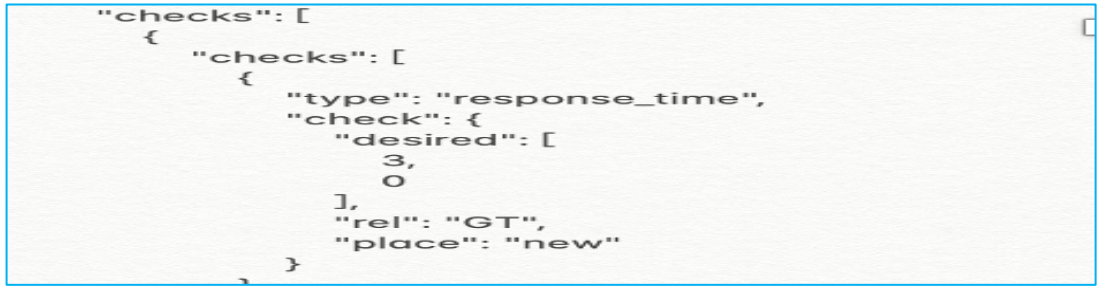
安全要求
仅关注并修复高危漏洞 23

内生安全落地实践：技术

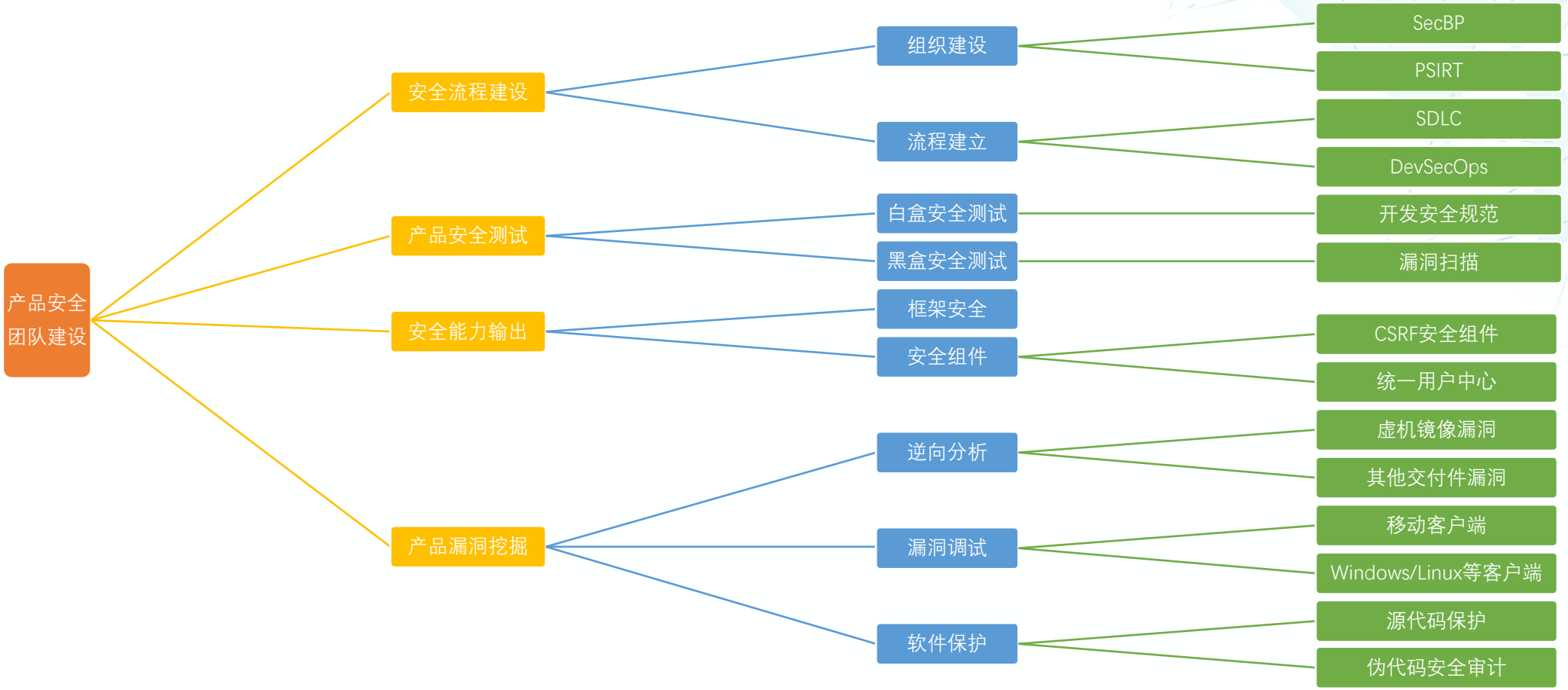
- 优化/安全检测工具 - - IAST规则丰富

Payload：'));select pg_sleep(5);--





内生安全落地实践：人员


产品安全团队建设
安全流程建设
产品安全测试
安全能力输出
产品漏洞挖掘
组织建设
流程建立
白盒安全测试
黑盒安全测试
框架安全
安全组件
逆向分析
漏洞调试
软件保护
SecBP
PSIRT
SDLC
DevSecOps
开发安全规范
漏洞扫描
CSRF安全组件
统一用户中心
虚机镜像漏洞
其他交付件漏洞
移动客户端
Windows/Linux等客户端
源代码保护
伪代码安全审计

目　录

展望

- 打破公司墙，延续安全开发带来的自身安全能力到运营阶段，做好基础安全防护一定程度上能对抗0day。

边界类设备

集权类设备

■**杜绝弱口令**：修改默认账号密码，包括部署时的操作系统账号密码、控制后台管理员等角色的密码

■**严格管控ACL**：管理控制台不开放到，仅管理员内网IP才能访问，系统级别的注意重启后生效

■**拆分部署应用和控制台**：通常控制台和应用可以拆分部署，对IP:PORT进行严格管控

■**及时更新打补丁**：获取厂商关于设备更新的信息升级打补丁或采用厂商提供的加固方案

■**开启应用层面日志**：部分安全产品默认未开启web日志，故应保证日志有效并统一处理