奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

BCS2022系列活动-冬奥网络安全“零事故”宣传周

基于三道防线的产品安全自查架构

武鑫　奇安信集团产品安全负责人

奇安信 | BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

产品安全自查的重要性

- 冬奥部署9大类、55款、813台安全设备，遭受**3.8亿**次网络攻击。
- 所有涉奥产品在部署前，均要求通过“三道防线”的 严格检查。

纵深防御体系

边界安全	流量安全	主机安全
防火墙	天眼威胁分析	终端准入
WAF	上网行为管理	天狗
VPN	入侵检测	椒图主机安全
SD-WAN	TIP威胁情报	虚拟化安全

被攻击的目标

1 自身安全性

2 功能兼容性

3 产品完整性

奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

基于三道防线的自查架构

第一道防线
高强度自检

第二道防线
兼容性测试

第三道防线
完整性验证

五大安全能力研究团队
黑白灰盒安全测试方法
产品安全测试矩阵
产品物料清单

关卡1

产品线和PQA联合团队
冬奥1:1环境测试
产品兼容测试流程
审核人员check测试结论

关卡2

现场安全运营团队
产品测试结论同步
产品升级包清单清点
MD5指纹验证

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

第一道防线：安全测试矩阵

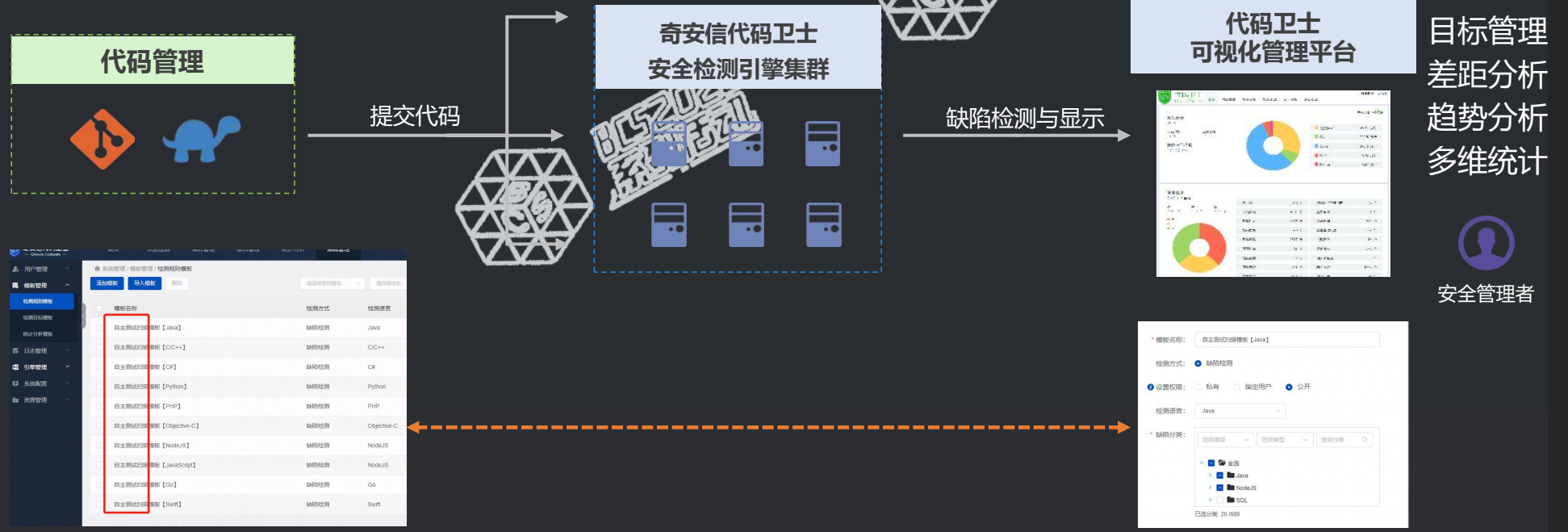
五大安全能力研究团队
300余人进行漏洞挖掘，
以常规安全提测模式
开展13个安全专项，
发现5782个安全漏洞。

产品安全测试矩阵								
安全测试大类	执行团队 / 安全动作	产品线	安服观星实验室	技术研究院	代码安全实验室	A-TEAM实验室	网络安全部	安全能力
安全提测流程	安全测试工单	√					√	提测流程
	静态代码扫描	√					√	代码卫士
	开源组件扫描	√					√	开源卫士
	IAST安全测试	√					√	IAST工具
	实战渗透测试		√			√	√	专家经验
	人工代码审计		√		√		√	专家经验
	二进制漏洞挖掘			√	√		√	漏挖平台
产品安全部署	部署手册安全审计	√					√	专家经验
	加固手册安全审计	√					√	专家经验
产品安全运营	产品安全众测	√					√	补天众测
	开源漏洞预警	√					√	QAX Cert
	产品物料清单			√			√	天问系统
第三方安全管控	提供安全测试报告	√					√	安全实践
	签署应急响应承诺	√					√	安全实践

第一道防线：SAST安全测试能力

- 静态代码扫描
- 开源组件扫描
- IAST安全测试
- 人工代码审计
- 实战渗透测试
- 二进制漏洞挖掘
- 产品安全众测

每一款涉奥产品，在出厂前均需要通过代码卫士进行静态代码扫描，产品线修复高危漏洞后才允许上线。



- 静态扫描误报高的问题，通过结合业务场景运营规则解决
- 业务方加白的安全函数，有必要进行针对性绕过

奇安信 | BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

第一道防线：SCA安全测试能力

静态代码扫描 → 开源组件扫描 → IAST安全测试 → 人工代码审计 → 实战渗透测试 → 二进制漏洞挖掘 → 产品安全众测

开源卫士查验组件安全性 → GitLab → Jenkins → 部署平台

开源卫士检测组件漏洞

开源卫士检测组件漏洞

开源卫士检测组件漏洞

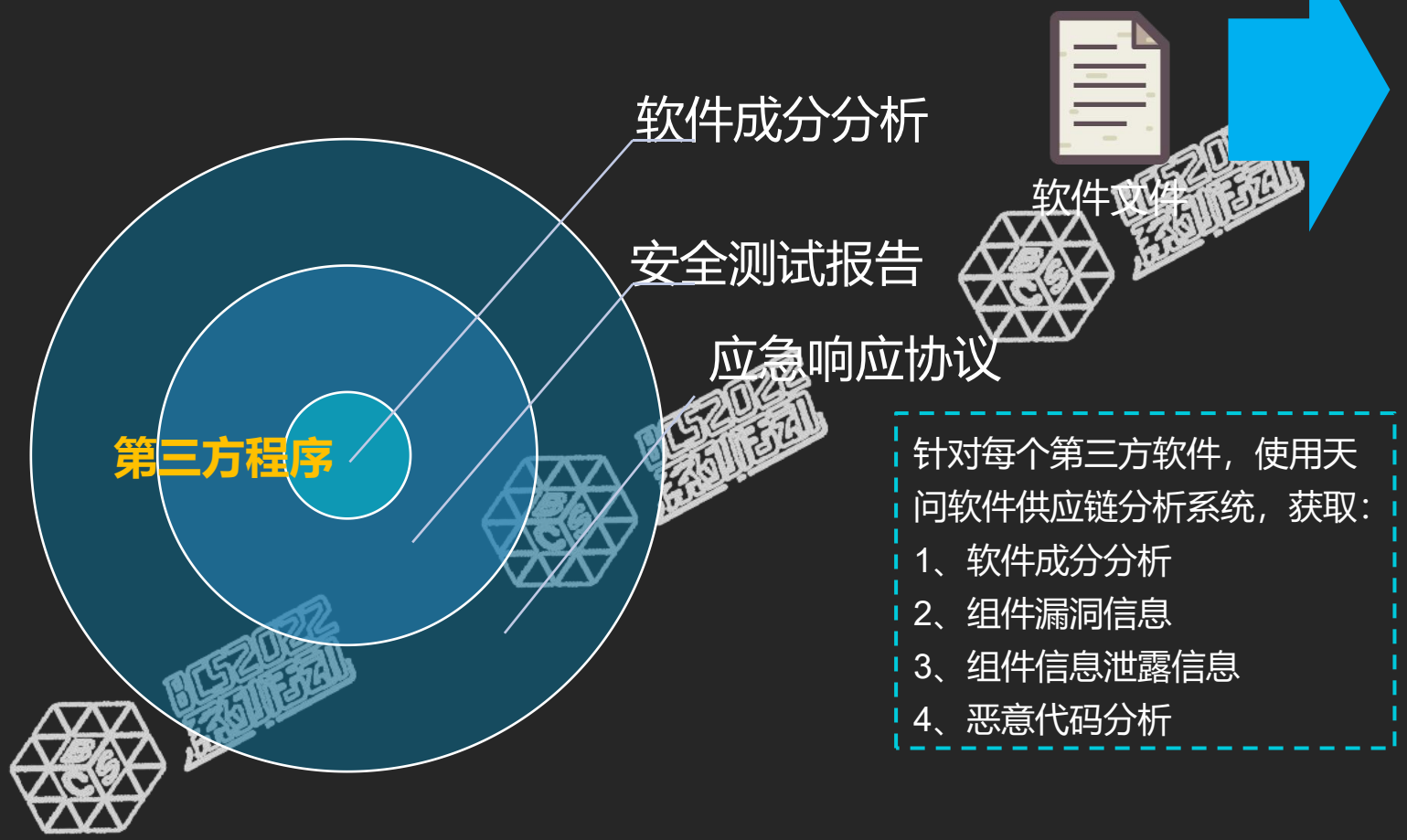
每一款涉奥产品，在出厂前均需要通过开源卫士进行第三方组件扫描，产品线修复风险级别为：超危、高危；利用难度为：简单、一般的开源组件漏洞，才允许上线。

- 在设计阶段，进行架构设计时使用开源卫士进行查验（安全左移）
- 在编码阶段，提交代码触发开源卫士进行扫描，存在不满足红线的漏洞，推送开发（安全左移）
- 冬奥部署前，使用开源卫士重新进行一轮安全检查，存在不满足红线漏洞须全部进行修复。

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

第一道防线：软件供应链分析能力

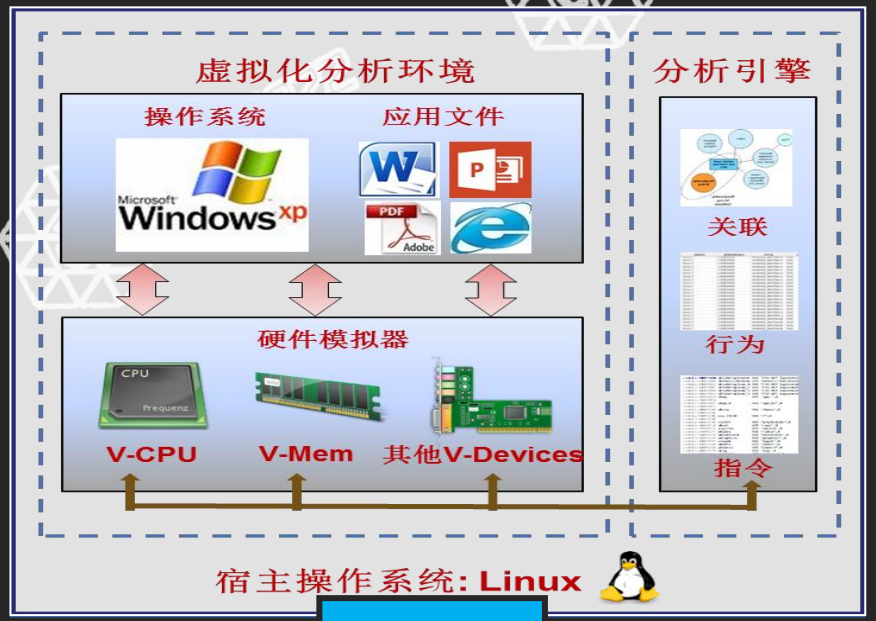
面对供应链攻击，特别是方案中引入的第三方软件，在没有源代码的情况下如何保障安全性?



软件文件

针对每个第三方软件，使用天问软件供应链分析系统，获取：

1、软件成分分析
2、组件漏洞信息
3、组件信息泄露信息
4、恶意代码分析



奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

BCS2022系列活动-冬奥网络安全“零事故”宣传周