RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑

开源代码安全性之梦魇与破魇利器

Gunter Bitz 博士， MBA、CISSP、CPSSE

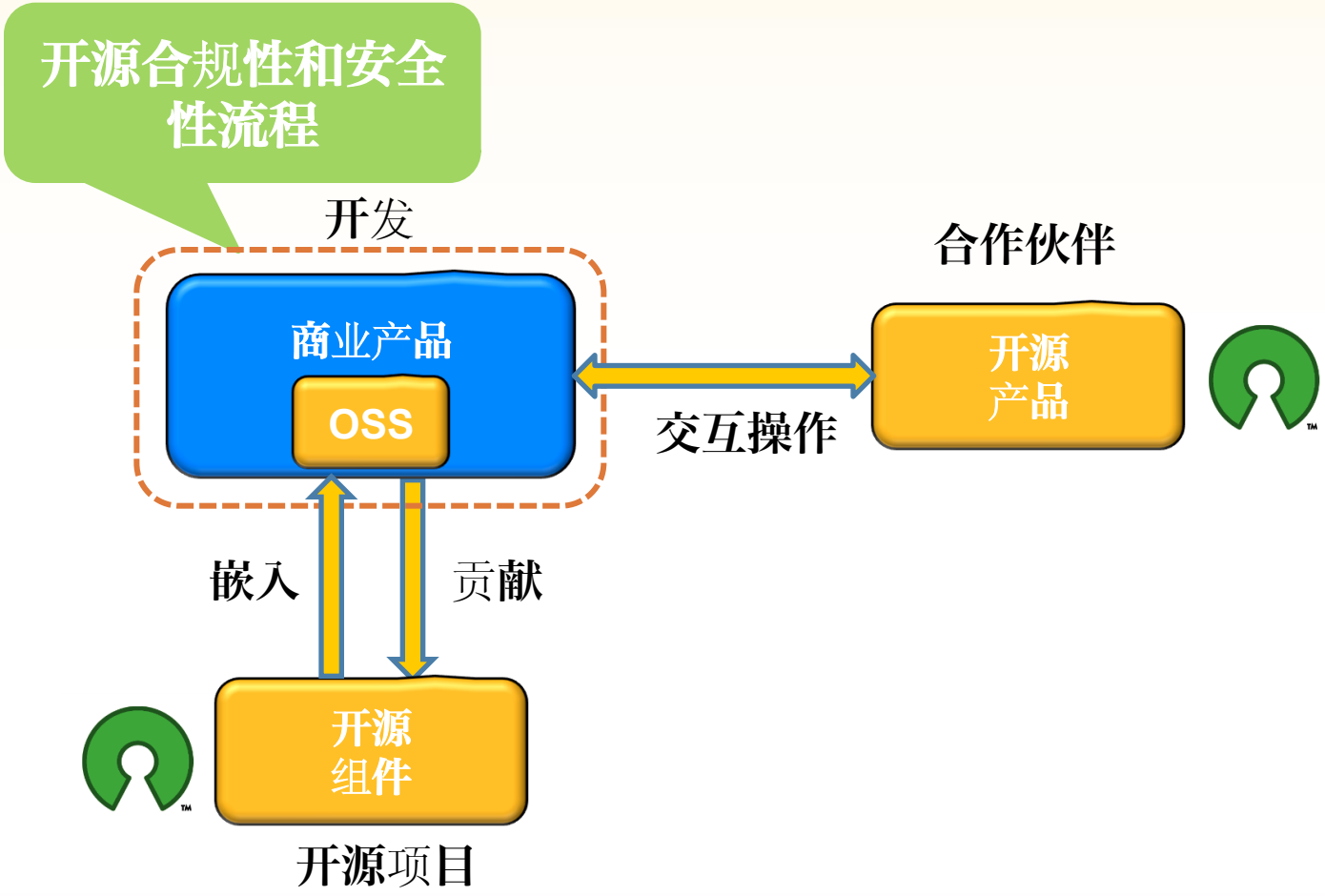
SAP 中国 / 质量监督和产品部门

RSA CONFERENCE CHINA 2012

RSA信息安全大会2012

- 开源代码在商业软件中的使用
- 使用开源代码的法律风险
- 开源软件（OSS）的安全风险
- 利器：
- 屏蔽开源组件
- 软件开发周期中安全性与回归性的集成
- 开源代码审批流程
- 安全性测试方法
- OSS 的安全响应流程

概述：开源代码在商业软件中的使用



使用开源代码的法律风险

- 开源软件(OSS)有不同的许可协议
  - 友好的许可协议：Apache、BSD、MIT
  - 著佐权 (Copyleft)/有传染性的许可协议：GPL、LGPL
- 著佐权 (Copyleft) 协议的义务
  - 发布修改部分的源代码和衍生作品的源代码
  - 任何衍生作品需用与原开源代码相同的许可条款
- 修复措施
  - 符合协议条款
  - 移除侵权代码
- 因忽视协议而产生的诉讼：Busy Box

Westinghouse 因违反 GPL 条款而支付 90,000 美元损害赔偿

RSA CONFERENCE CHINA 2012

TECHNOLOGY LAB / INFORMATION TECHNOLOGY

BusyBox takes out bankrupt opponent in GPL lawsuit

A software developer has convinced a court that an electronics manufacturer …

by **John Timmer** - Aug 6 2010, 2:25am -800

23

The person behind a set of GPL-licensed Unix utilities called BusyBox has been engaged in a lawsuit against a dozen consumer electronics companies, accusing them of violating his copyright. The companies allegedly have been distributing hardware (including HDTVs) that includes BusyBox, but then licensing it to consumers under GPL-incompatible terms.

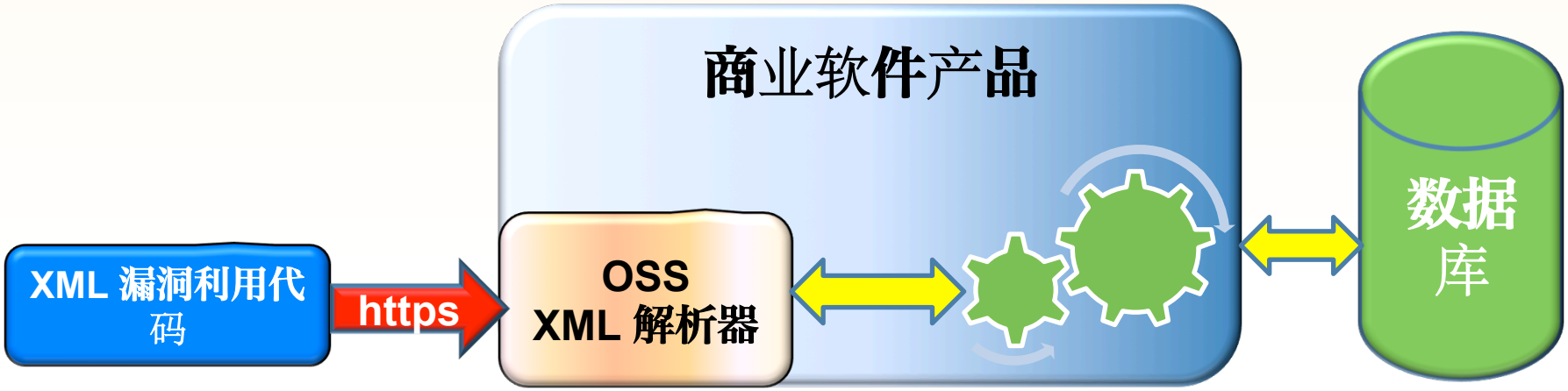
In late July, the judge in the case issued a summary judgement against one of the defendants, Westinghouse Digital Electronics, which stopped participating in the case when it entered bankruptcy protection. The ruling isn't a sweeping victory for the GPL, but it does show that the GPL is compatible with the standards for summary judgement.

信息来源：http://arstechnica.com/information-technology/2010/08/court-rules-gpl-part-of-a-well-pleaded-case/

开源软件的安全风险

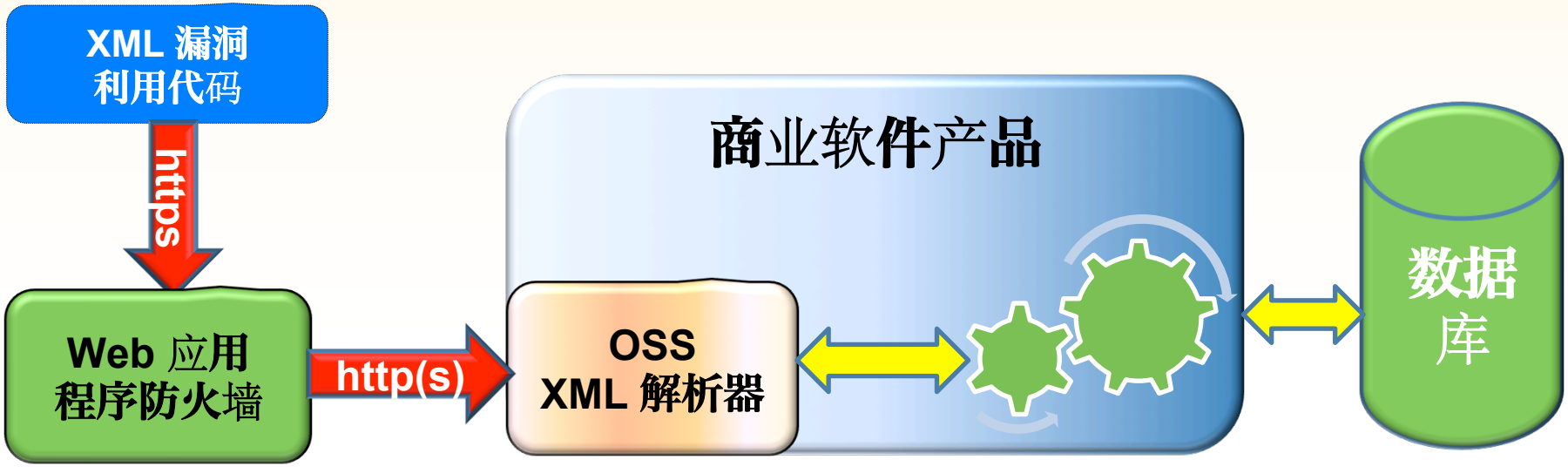
- 使用开源软件与商业软件相比是否更安全？
- 取决于诸多因素：
  - 代码更改的监督力度够不够？
  - 项目团队是否积极测试安全性？
  - 第 3 方黑盒和白盒测试工具的使用程度
  - 是否建立了安全响应流程？
  - 活跃的开发人员社区的规模
  - 项目团队仍然活跃// 很长时间未发布任何更新
  - 用户社区（可报告bug的群体）的规模

问题在哪？



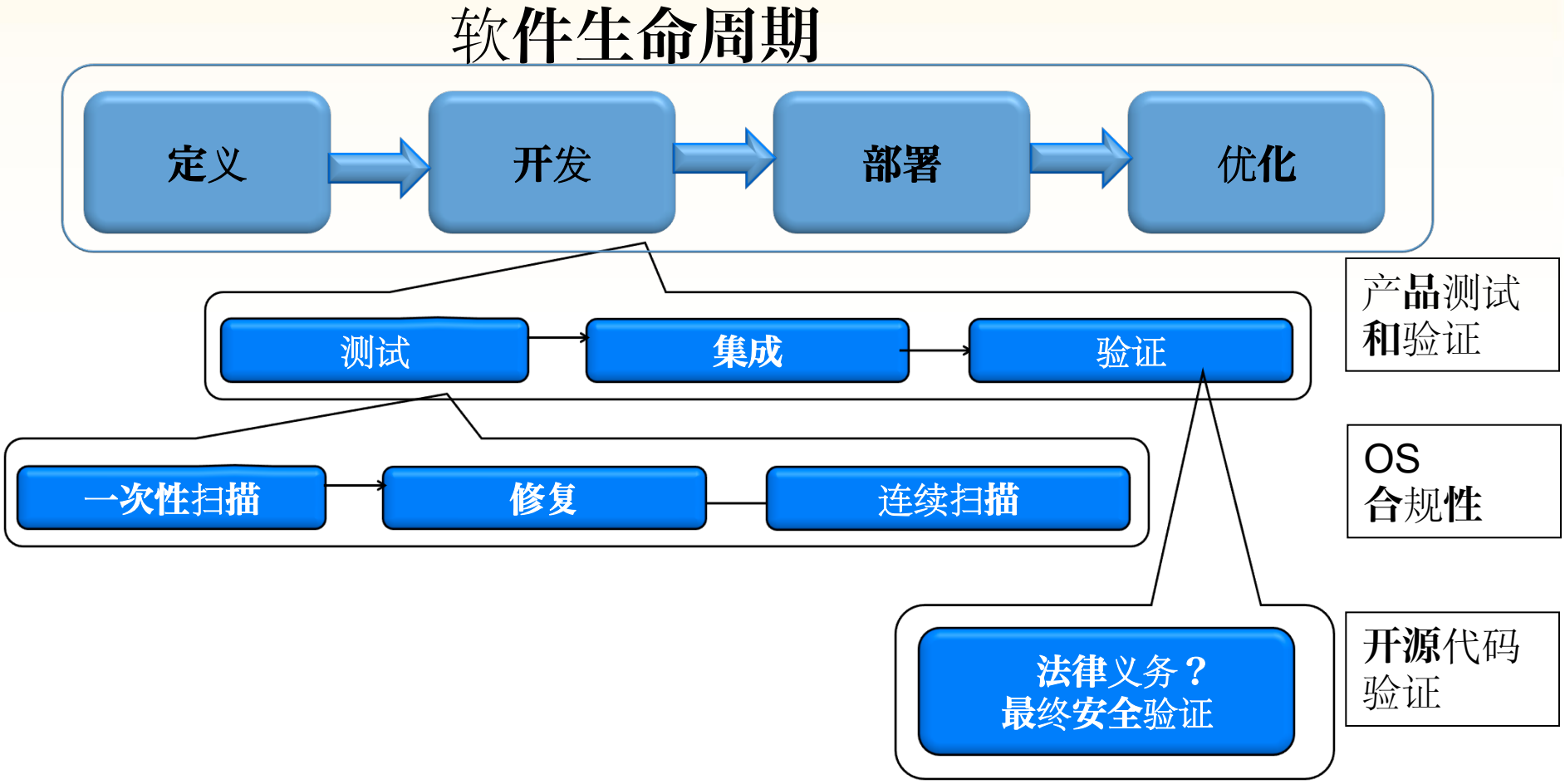
- 开源代码软件开发人员不承担安全责任
- “问题”和商业软件产品供应商紧密相关

利器之一：
屏蔽开源组件

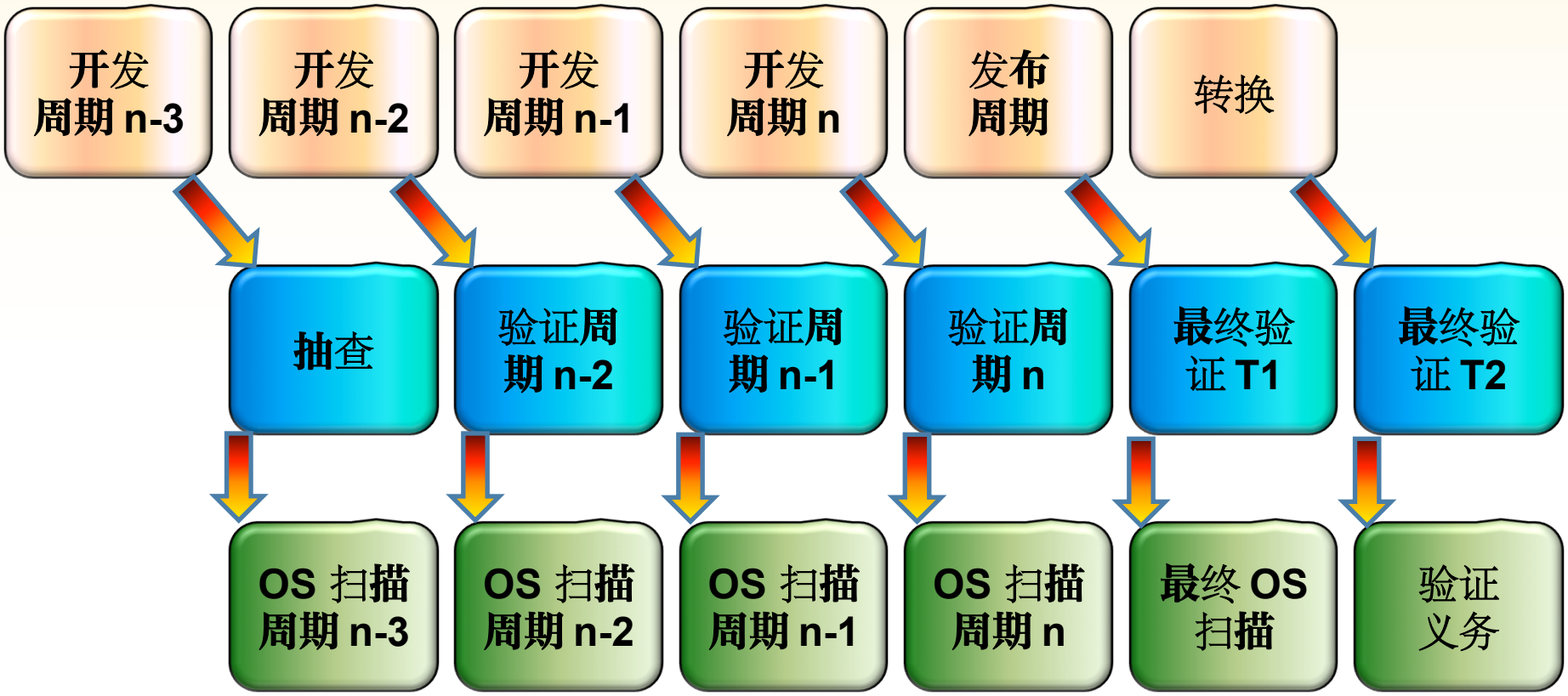


- 使用附加 Web 应用程序防火墙来阻止恶意请求
- 防火墙能否监控所有可能的攻击渠道？

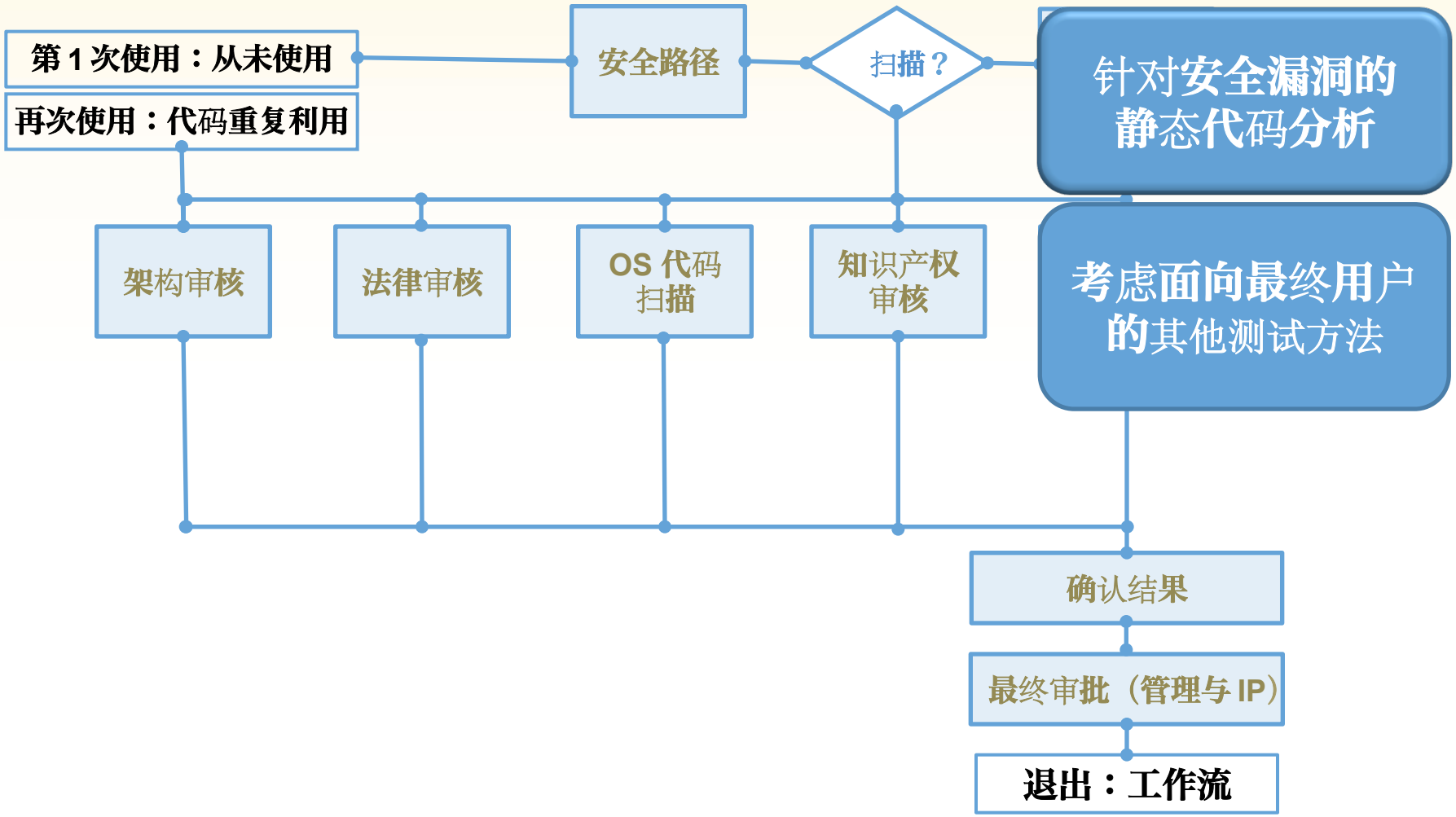
利器之二：
开发周期中集成安全性和合规性流程



敏捷开发情况下的集成


开发
周期 n-3
开发
周期 n-2
开发
周期 n-1
开发
周期 n
发布
周期
转换
抽查
验证周
期 n-2
验证周
期 n-1
验证周
期 n
最终验
证 T1
最终验
证 T2
OS 扫描
周期 n-3
OS 扫描
周期 n-2
OS 扫描
周期 n-1
OS 扫描
周期 n
最终 OS
扫描
验证
义务

利器之三：
开源代码的审批流程



利器之四：
安全性测试方法

RSA CONFERENCE CHINA 2012

- 静态源代码分析--“代码扫描”
  - 大量误报
  - 服务器代码（例如 Web 服务器、应用程序服务器）解读困难
- 代码审核 – 适合小型组件
- 模糊测试
  - 专家指导下的测试工作
  - 代码覆盖率并非总是最佳方案
- 手工渗透测试
  - 非常精确的测试结果
  - 代码覆盖率取决于可用预算
- 自动化渗透测试
  - 精确的测试结果
  - 代码覆盖率并非总是最佳方案

独立或集成

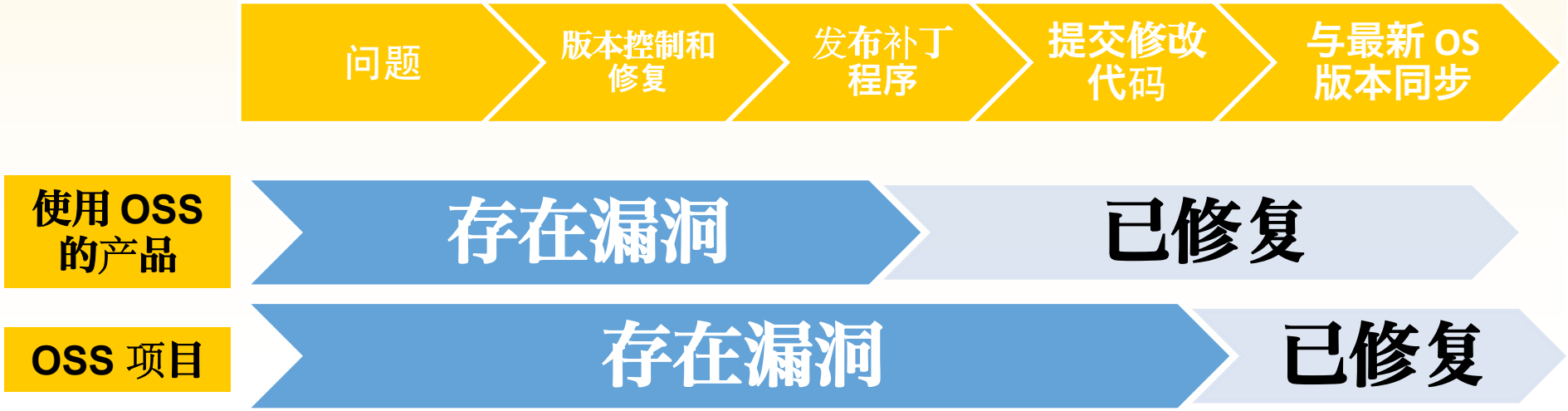
独立

集成

利器之五：
OSS 的安全响应流程

- 为每个开源组件分配专门的内部所有者
  - 为使用同一 OSS 组件的多个产品组分配一个所有者
  - 所有者负责维护 OSS 组件
  - 所有者接收所有漏洞修复请求
- 监测公共信息源
  - 此处发现的所有内容都会创建一个错误修复请求
  - CVE/MITRE
  - SANS
  - CERT/CC
  - 安全重心 (Bug Traq)
  - NVD –（美国国家漏洞数据库）
  - 项目网站及更多

开源软件的安全响应流程



- 在商业产品代码中首先解决安全问题
  - 预防与客户有关的责任问题
- 将代码提交至开源社区作为资源共享
- 回交修补后的开源组件
  - 减少 OSS 组件日后需要升级时的工作量

总结

- 在使用开源软件之前应先考虑法律风险
- 开源软件的安全性很大程度上取决于 OS 项目团队的成熟度
  - 不能保证它与内部开发的软件孰优孰劣
- 需要本地开源监督流程来控制开源代码的纳入
- 将安全性测试集成到开发生命周期中至关重要
  - 同样适用于敏捷开发流程
- 安全响应流程同样必须覆盖开源软件

谢谢！

Gunter Bitz， SAP
gunter.bitz@sap.com

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012