2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

内生安全 从安全框架开始

ENDOGENOUS SECURITY:
STARTING FROM A CYBERSECURITY FRAMEWORK

金融机构开源软件安全治理思考与实践

梁鹏

清华大学电子工程学硕士
中国农业银行研发中心信息安全与风险管理部副处长
长期从事金融领域应用系统研发和应用安全管理工作

背景与挑战

治理策略与实践

思考与体会

背景

云计算

移动互联网

AI

大数据

开源软件快速发展

监管要求

内部管理要求

安全问题不容小觑

国家信息安全形势

挑战

数量众多

- 开源软件种类和数量规模巨大
- 存在安全漏洞众多

关系复杂

- 广泛的直接引用
- 错综复杂的间接引用

成本较高

- 大量应用系统升级改造
- 大量的回归测试

情况多变

- 版本不断升级
- 漏洞不断发现

背景与挑战

治理策略与实践

思考与体会

总体思路

兼顾安全与发展

治理策略

摸清家底


不知道有哪些？
不知道谁在用？
不知道安全吗？
搭建自动化的漏洞排查工具
构建引用关系自动化分析能力
搭建统一管理的开源软件仓库

制定标准

接受什么？

拒绝什么？

关注什么？

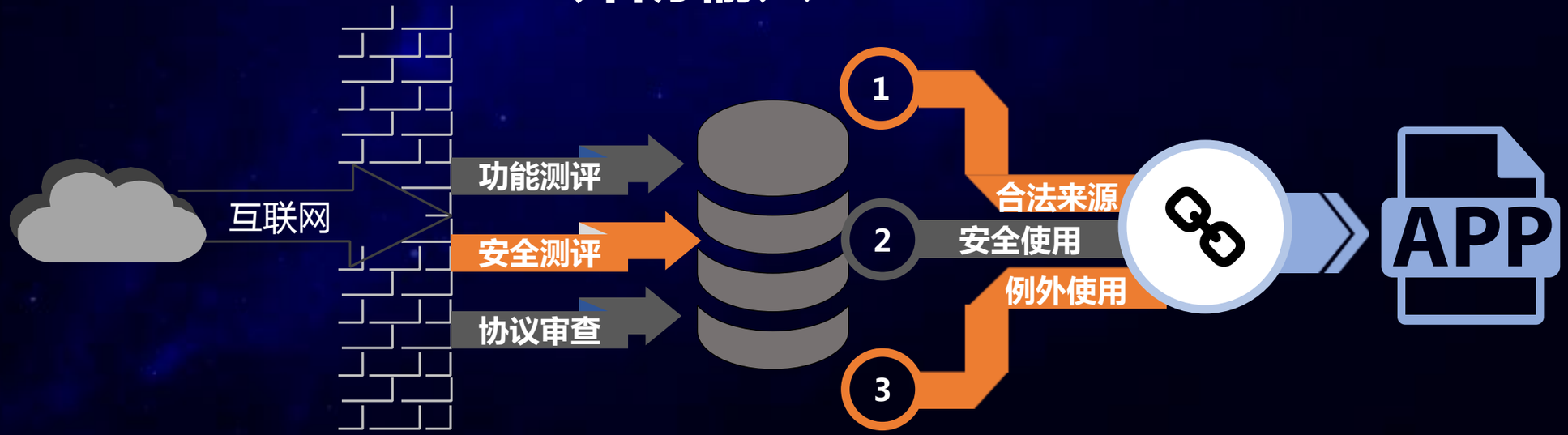
风险偏好

差异化管理

外防输入

不知道从哪里来？

不知道能不能用？



引入环节严格把关

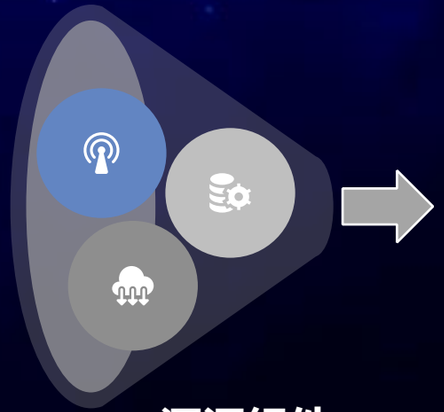
构建环节阻断风险

内防扩散

不安全组件的使用范围扩大了吗？

安全的组件新发现了漏洞怎么办？

- 建立漏洞组件的灰名单
- 建立应用系统的白名单
- 及时更新灰名单白名单



漏洞组件

存量的不安全组件

新发现漏洞的组件

例外引入的组件

限制使用白名单

持续监测

昨天安全今天还安全吗？

漏洞信息从哪里来？

- 对接多个漏洞库
- 多环节持续检测，及时更新白名单

存量处置

不知道从哪里入手？

不知道代价有多大？

修复方案谁牵头？

- 明确处置支持方
- 试点开路
- 分批推进
- 稳步实施

专项治理
重点突破

自主治理
整体压降

即时处置
落实要求

度量与评价

治理任务完成了吗？

治理成效怎么样？

过程性指标

为漏洞治理方案符合性的指标，评估工作完成度，如任务完成率。

结果性指标

作为漏洞治理有效性的指标，评估体系及处置方案的合理性，如治理期漏洞减少比例、治理期漏洞减少比例、风险处置方式占比等。

背景与挑战

治理策略与实践

思考与体会


管理例外
完善工具
没有银弹
打持久战

感谢聆听！