OWASP
Open Web Application Security Project

为什么唯品会能够100%使用安全开发流程？

演讲者：黄梦娜

唯品会安全应急响应中心负责人
唯品会内部产品技术团队
高级信息安全工程师
CCIE Security

目录

CONTENTS

一、我们主要面临的威胁?

二、这些威胁从哪里来？

三、软件安全开发

四、安全监控与应急响应

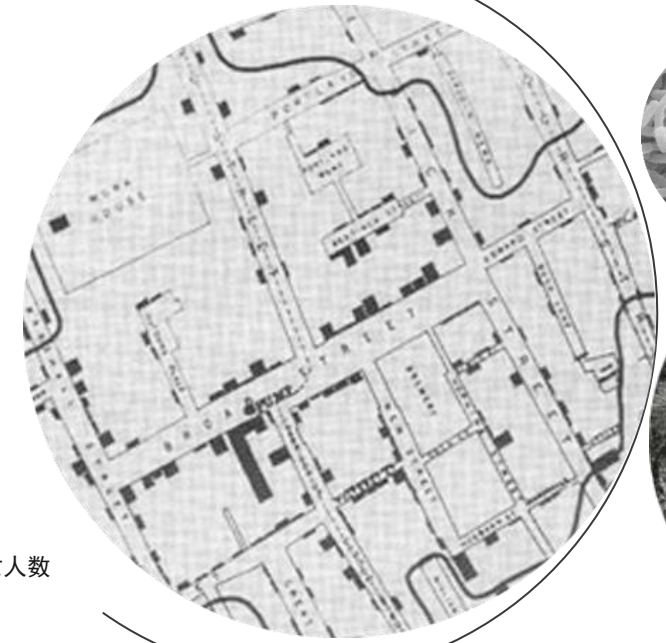
五、安全工作的“实干者”

150年前的一场天灾人祸

伦敦霍乱

150年前 伦敦霍乱 “瘟疫肆虐”

整条河流充斥着一种晦暗不明的淡褐色液体....



黑色=死亡人数

病菌肆虐

- 200万城市人口 垃圾污染严重
- 伦敦的地下就是一个杀人的地狱
- 71508例霍乱病例
- 26101例为死亡人数

恐惧

- 盲目恐惧疾病
- 主要传播途径水源污染

“自下而上”为防霍乱改造排水系统

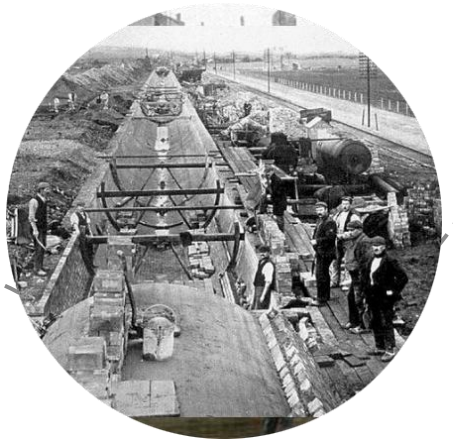
——伦敦排水管道系统 Joseph Bazalgette

“世界七大工程奇迹”

伦敦下水道与金字塔齐名

- 全长160公里 地下3米
- 挖掘土方350万吨 管道直径3米
- 3亿8千万块混凝土砖

《Seven Wonders of the Industrial World》



- 每年3900万吨污水
- 通过这个系统排入泰晤士河

一、我们主要面临的威胁?

威胁泛化

1. 关键漏洞 一览众山小
2. 数据泄露 汇入地下经济
3. 安全事件 商业军火
4. 恶意代码 灯下黑
5. 电信诈骗 泛滥成灾
6. 勒索软件 席卷全球

1.1 关键漏洞 一览众山小

2014/4 Heartbleed
内存越界

OpenSSL服务器内存中64K的数据
用户名、密码、服务器证书、私钥等敏感信息
深思：国内网站的HTTPS使用率底..

2014/9 Bash Shellshock
控制电脑 系统最高权限

Bash语法灵活、解析程序复杂
几次修补，仍旧发现新问题
结局：演化了一系列的漏洞...

信息攻防 强弱能力
被关键漏洞拉平

2015 XcodeGhost
恶意代码

2017/5/12 EternalBlue
80亿美元损失

WannaCry利用MS17010漏洞在全球范围大爆发
通过：445端口、自我复制、自我传播

2016 Dirty Cow CVE-2016-5195
内核级的漏洞 root提权

COW是 Linux 用来减少内存对象重复的技术
竞争条件：低权限用户可以修改只读对象

1.2 数据泄露 汇入地下经济

人的**身份**

几乎是永久的

人与人之间的**关系**

基本是稳定的

12306数据泄露 14多万用户信息

雅虎数据泄露 10亿多账户

某知名邮箱数据泄露 5亿多条

社交网站 成重灾区

此类数据泄露带来的影响 **很难在短时间内被冲淡**

1.3 安全事件 商业军火

2015年 Equation攻击

活跃了近20年的APT攻击组织
早于其他组织发现更多0day漏洞
拥有一套用于植入恶意代码的信息武器库
可对数十种常见品牌硬盘实现固件植入的恶意模块
绕过代码签名限制的特殊方法

42个国家
500次感染
300多个域名
100台服务器托管

模式化攻击

攻击成本降低
缺少鲜明基因特征
难追溯

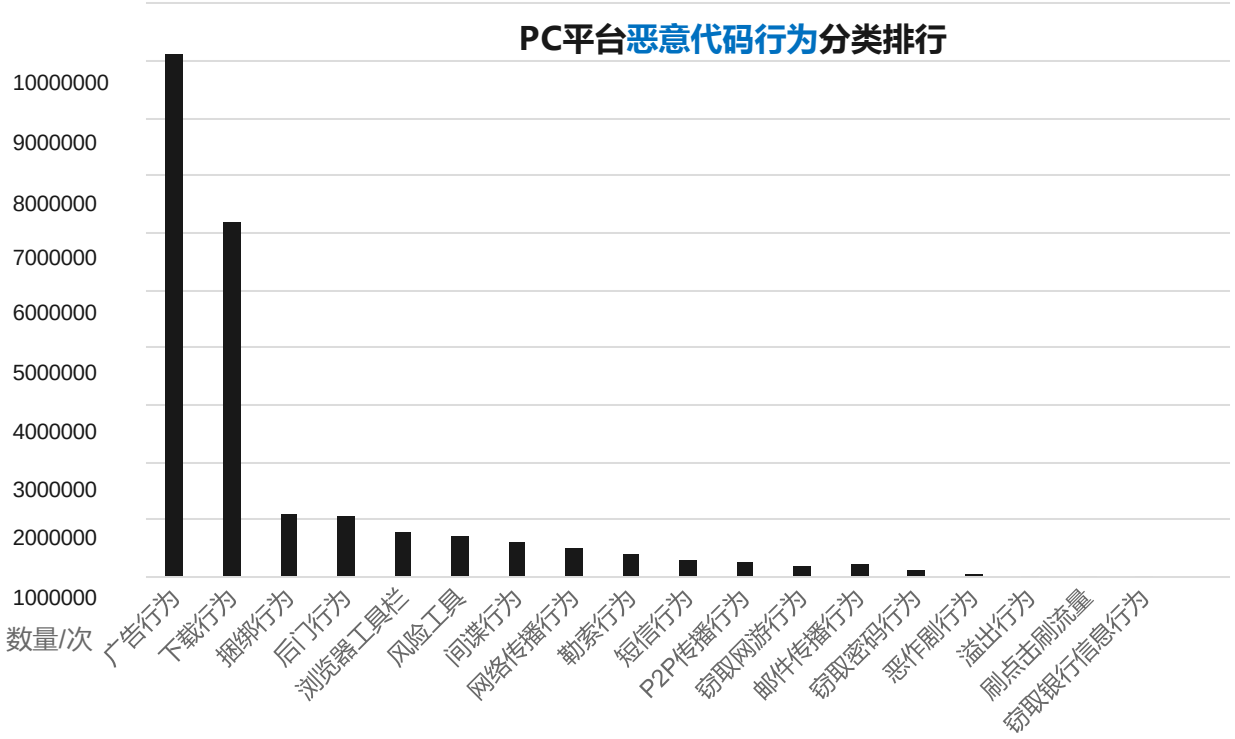
2016 Dyn DDOS

美国最主要DNS服务商Dyn
1.2Tbps流量
“史上最严重DDoS攻击”
规模大：上千万个IP
物联网设备感染Mirai
组成僵尸网络

连带影响：杭州某公司召回四种网络摄像头，大约430万台

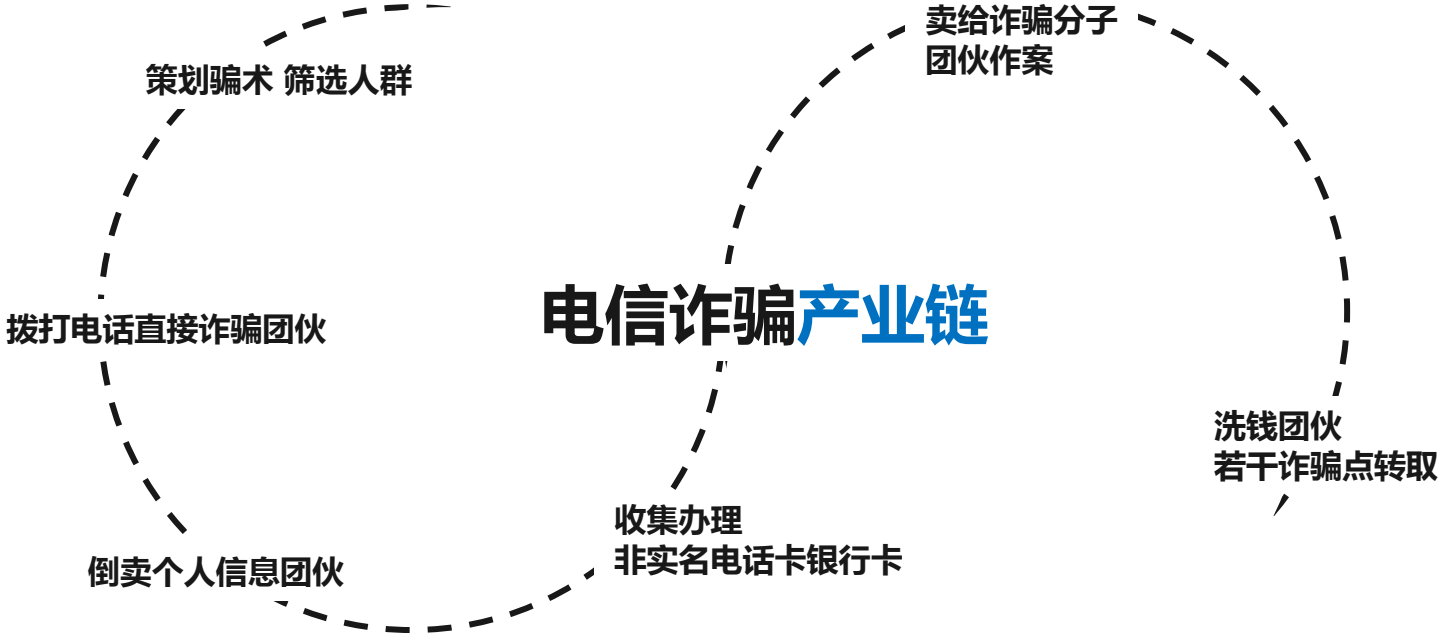
42个国家 | **难溯源** | **1.2Tbps**

1.4 恶意代码 灯下黑



1. 流量模式
2. 个人隐私倒卖
3. 低投入高收益
4. 越发普遍

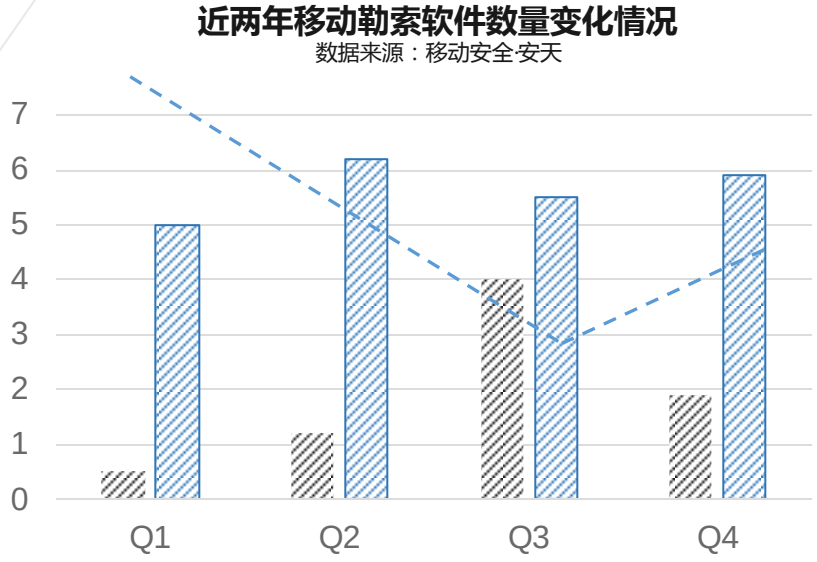
1.5 电信诈骗 泛滥成灾



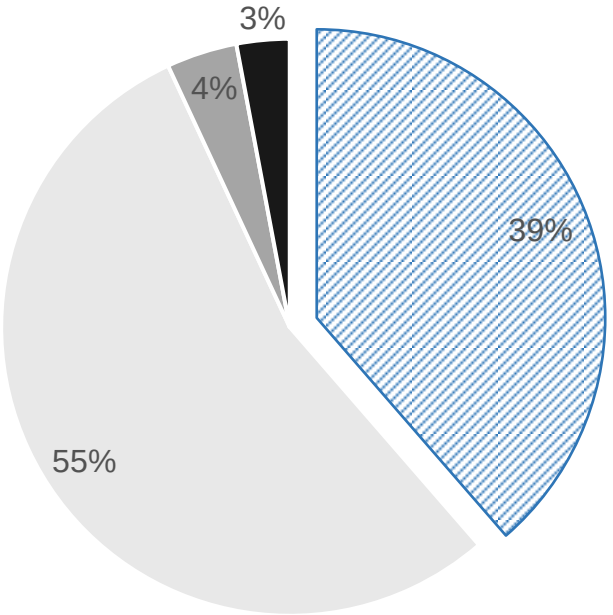
2015年全国公安机关共立电信诈骗案件59万起，同比上升32.5%，共造成经济损失 **222亿**

2016年 十大电信诈骗 最高骗走 **1700万**

1.6 勒索软件 席卷全球



2016年 勒索病毒造成损失预估超过 **10亿美元**



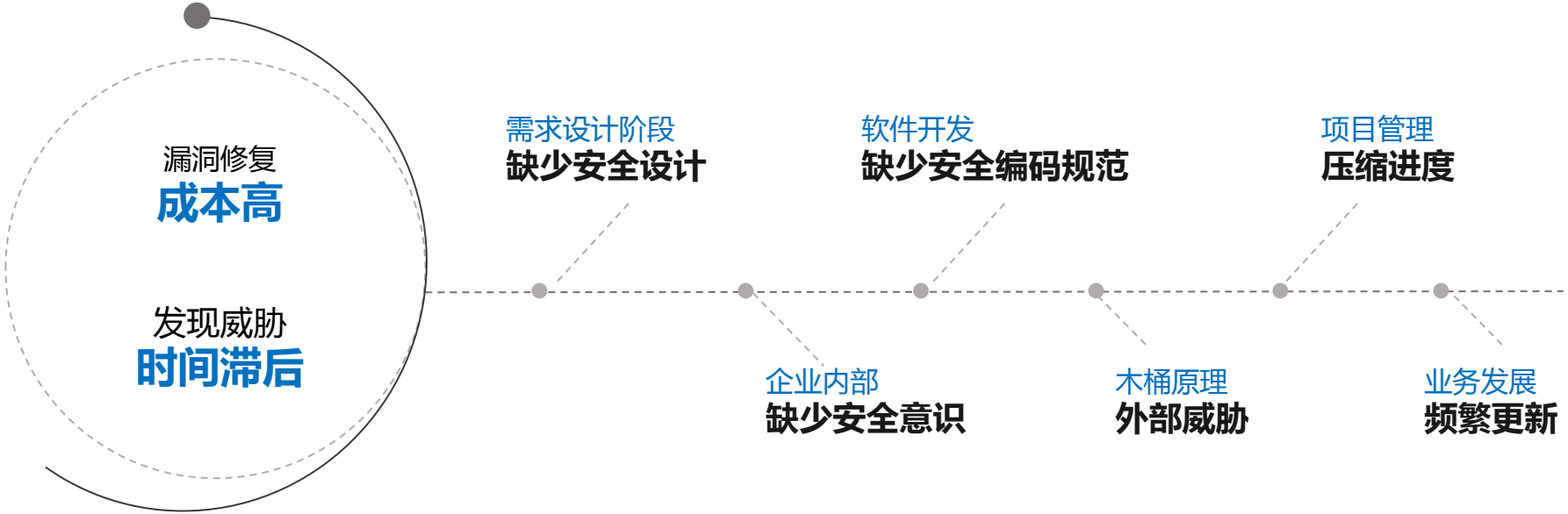
勒索软件在全球范围内分部情况占比
数据来源：移动安全·安天

二、这些威胁从哪里来？

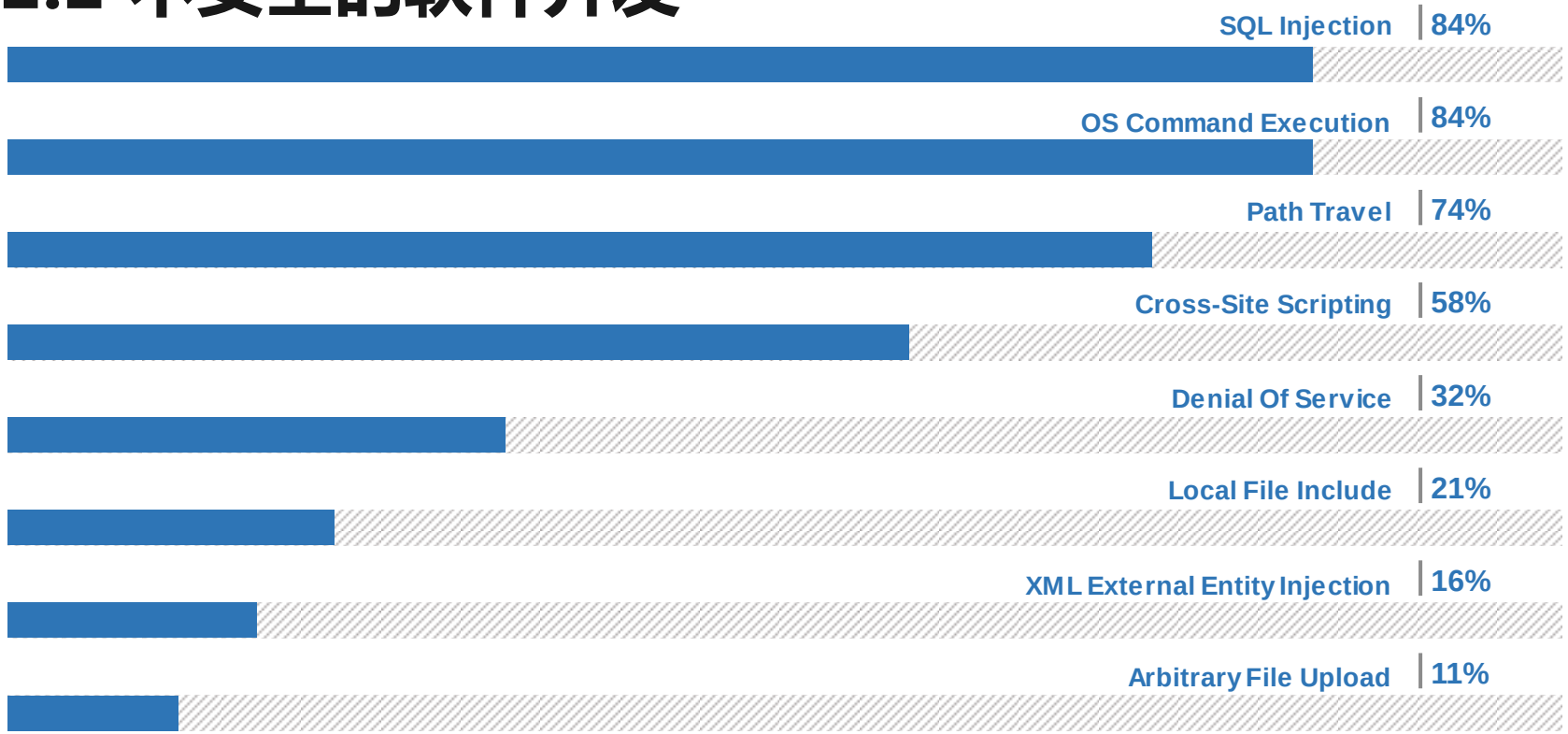
不安全的软件开发？

2.1 业务发展之初 系统脆弱 遭受攻击 “漏洞爆发”

——安全漏洞如同灾害一般爆发



2.2 不安全的软件开发

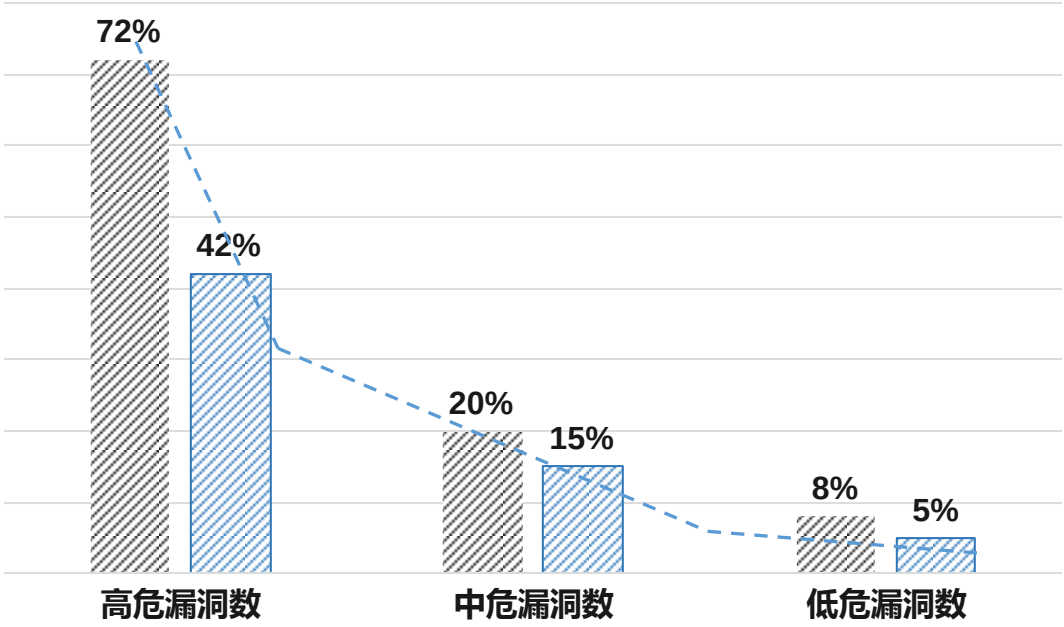


Reference: Google 《Most popular attacks》

三、软件安全开发

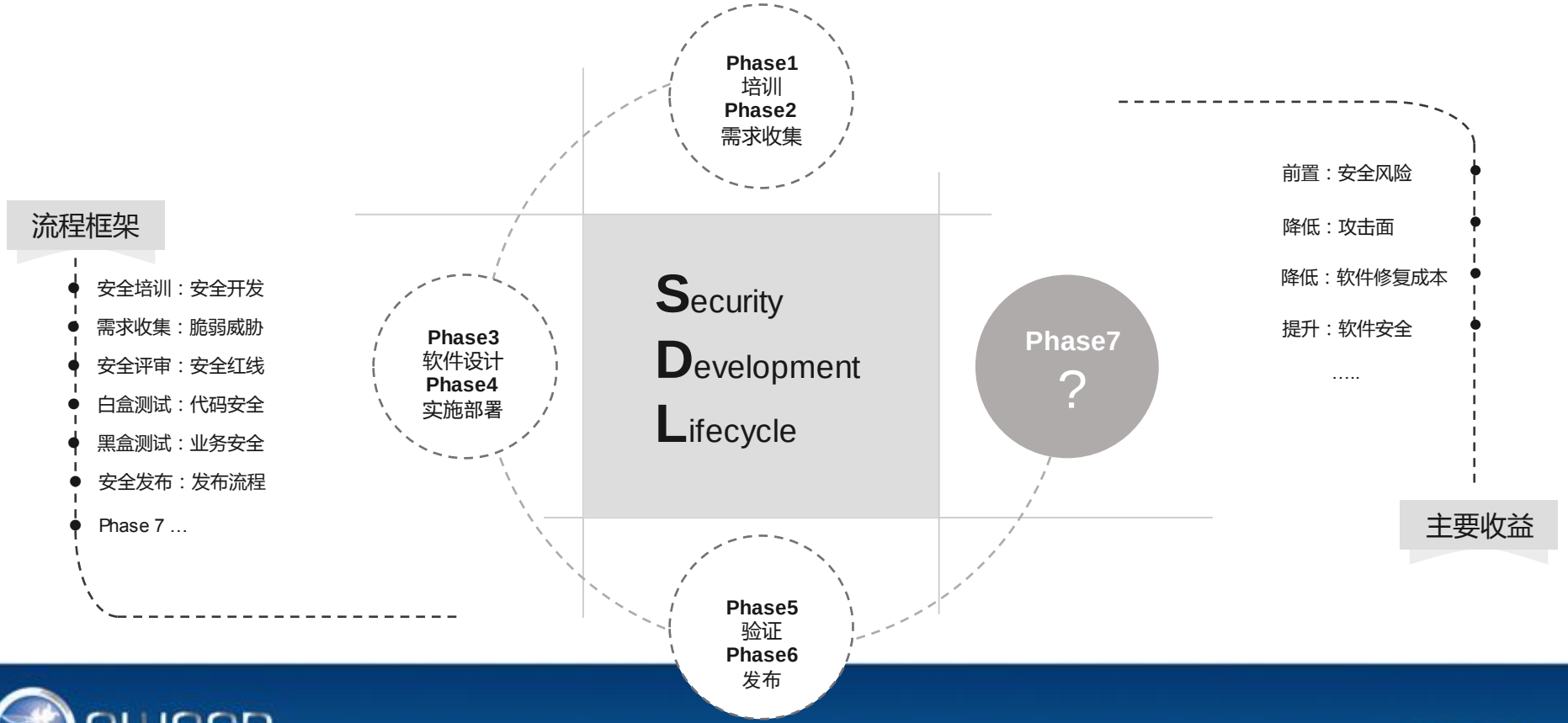
电商安全之软件安全开发

3.1 改进效果

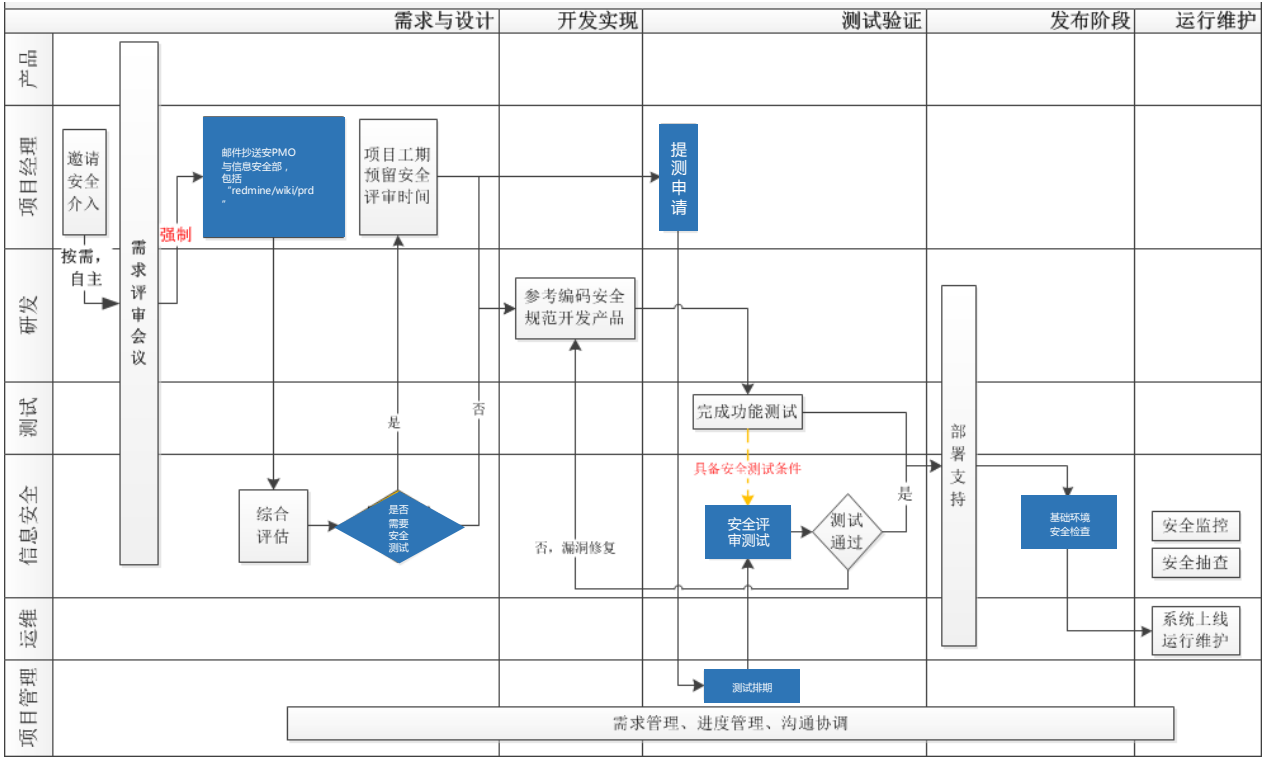


高危及严重漏洞数量整体 **降低30%**

3.2 “自下而上”软件安全开发流程SDL



3.3 唯品会项目安全上线管理流程



3.3.1 安全培训

参考文章：**《唯品会信息安全培训体系》**
2017-01-09 **唯品会安全应急响应中心**官网微信号
https://mp.weixin.qq.com/s/btFpm7kjPnvl7Wp02StarA

安全开发培训

信息安全培训

安全意识培训

3.3.2 需求与设计


需求评审原则：CIA
风险评估
业务场景梳理
业务之间的关联性
安全需求
C.I.A
威胁建模
攻击面最小化
基本隐私
权限最小化
默认安全
纵深防御
S.T.R.I.D.E. 威胁分析
信息模型
功能模型
行为模型
安全设计

3.3.3 威胁建模与安全评审

S	T	R	I	D	E
Spoofing 仿冒	**T**ampering 篡改	**R**epudiation 抵赖	**I**nformation Disclosure 信息泄露	**D**.o.S 拒绝服务	**E**levation of Privilege 权限提升

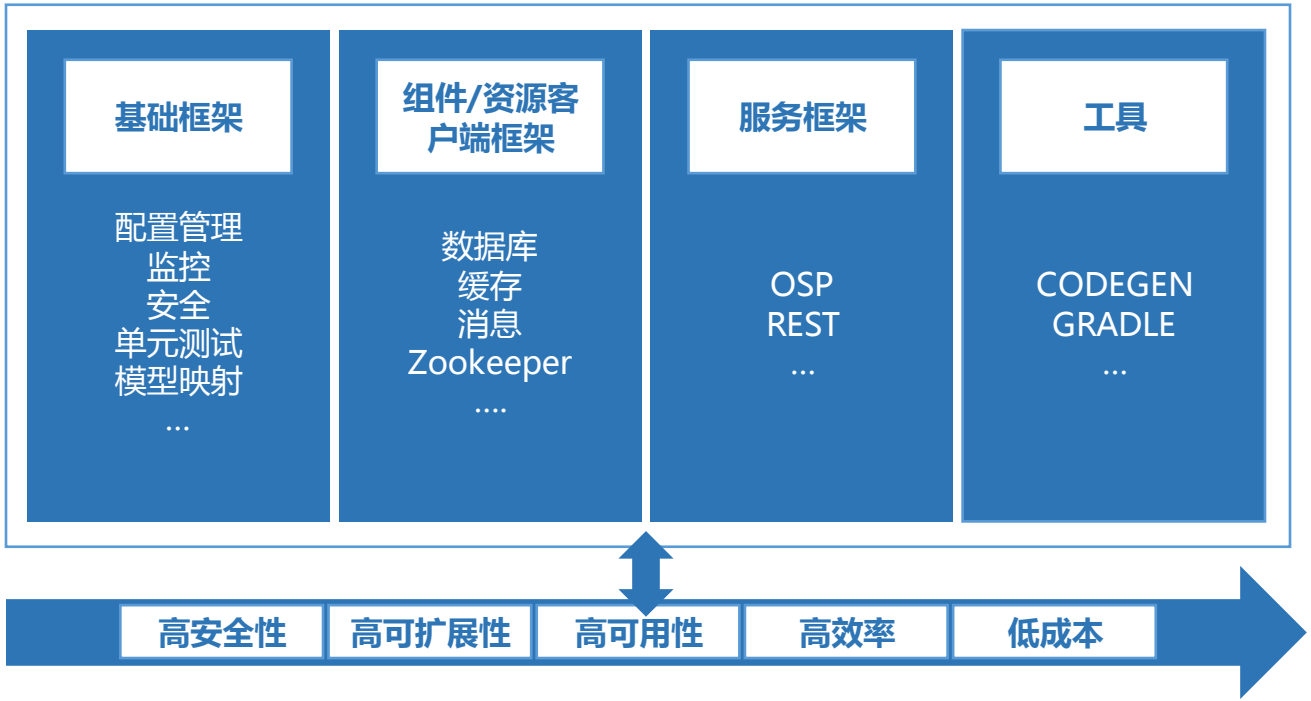
3.3.4 开发实现

唯品会安全开发红线

编号	类别	概述	细则	备注
L01	认证与鉴权	帐号锁定	除公司会员系统之外提供外网访问功能的系统，必须启用帐号登录失败锁定策略（如：3分钟20次登录失败，锁定30分钟）	
L02		错误提示	用户名或密码错误时，返回的提示信息必须一致（如："错误的用户名或密码"）	
L03		登录与注销	有登录功能的系统必须同时有注销功能	
L04		后台页面	后台页面必须对用户身份和访问权限进行检查	
L05	验证码	管理界面	管理后台的登录界面必须设置验证码	
L06		有效期	验证码必须设置有效期（有效时间和错误次数）	
L07		发送频率	使用短信/邮件验证时，必须限制同一ID或接收者的验证码发送频率	
L08	会话安全	会话超时	会话token/session必须设有超时机制	
L09		会话更新	用户登录成功后，必须更新会话ID；用户注销后，必须强制session/token过期	
L10	Cookie	HTTP Only	cookie参数中Session Id等认证相关的字段必须设置HTTP Only	
L11	上传下载	文件判断	对上传文件后缀进行白名单限制，严格判断文件内容与类型是否匹配	
L12		目录跳转	禁止客户端自定义文件下载路径（如：使用../../../../../进行跳转）	
L13		目录权限	存储上传文件的目录必须禁止脚本执行权限	
L14	传输安全	参数提交	禁止通过HTTP GET方式提交**不安全算法**[1]处理过的用户密码	
L15		明文传输	禁止在未加密的HTTP协议中明文传输用户登录密码、支付密码、银行卡卡号、有效期、持卡人姓名、身份证号码、CVV等交易敏感数据。会员系统、支付系统还应在此基础上进一步**增强安全措施**[2]。	
L16		支付安全	禁止在支付密码的传输过程中使用**不安全算法**[1]	
L17	存储安全	敏感数据存储	禁止数据库、日志文件中明文存储用户支付密码、银行卡卡号、有效期、持卡人姓名、身份证号码等交易敏感数据。禁止存储信用卡CVV信息。禁止使用**不安全算法**[1]存储用户身份校验凭据，如：密码。会员系统、支付系统还应在此基础上进一步**增强安全措施**[2]。	
L18	接口滥用	关键接口防刷	提供"查询用户名或手机号是否注册或绑定"功能的接口须调用具备调用频次控制	
			短信下发界面必须提供防刷机制，如加入FDS图形验证码	
L19	日志审计	审计内容	自建用户系统，必须记录：时间/用户ID/界面(Web或APP)/结果（成功或失败）/ IP等信息	
L20		日志清除	除审计用户外，其他人员不应具备日志修改、删除或清空的权限。必须记录清空日志的行为	
L21		日志存储	禁止将日志直接保存在可被浏览器访问到的WEB目录中	
L22	其它	后门	禁止在代码中留置后门	

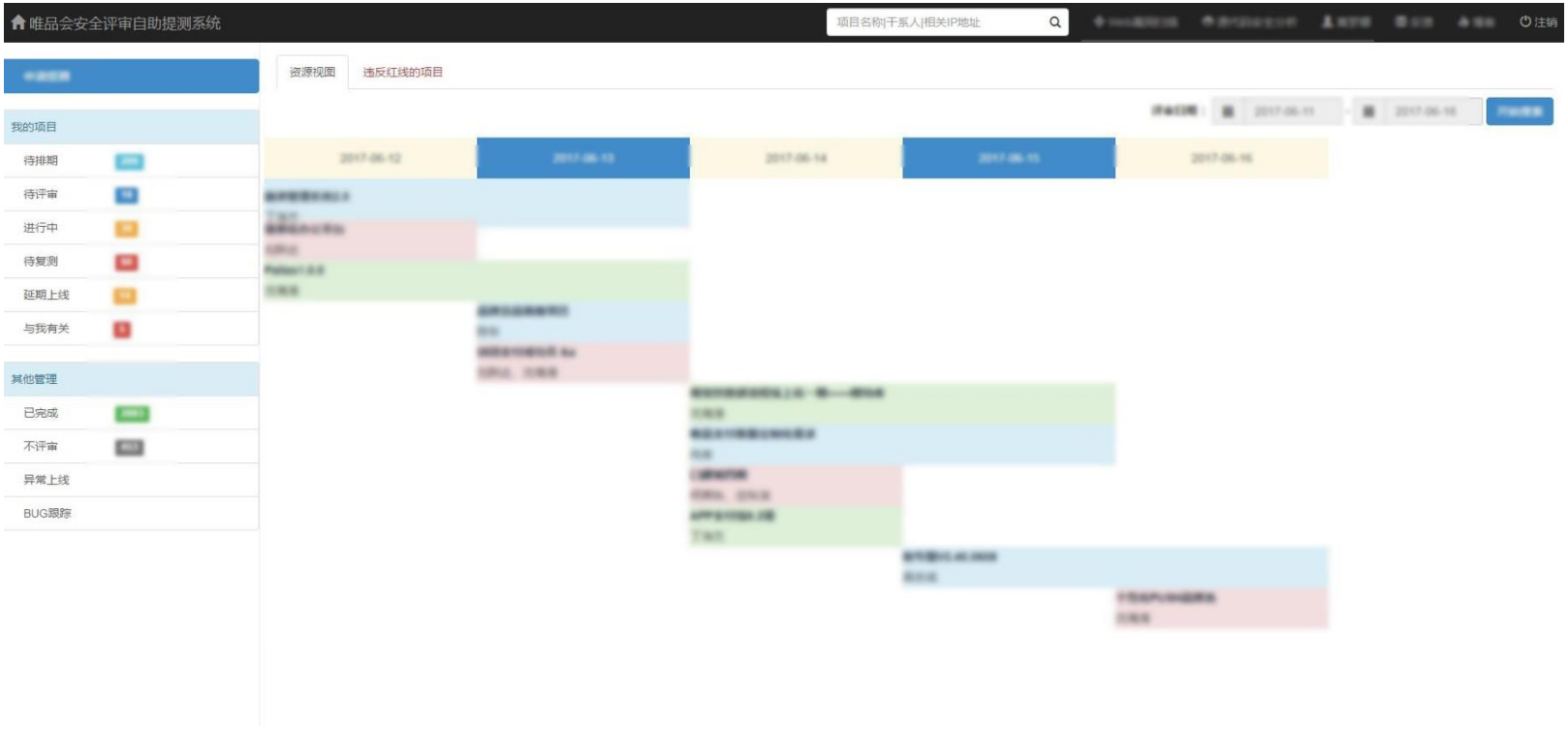
3.3.5 统一框架 开发实现

唯品会Venus统一开发框架

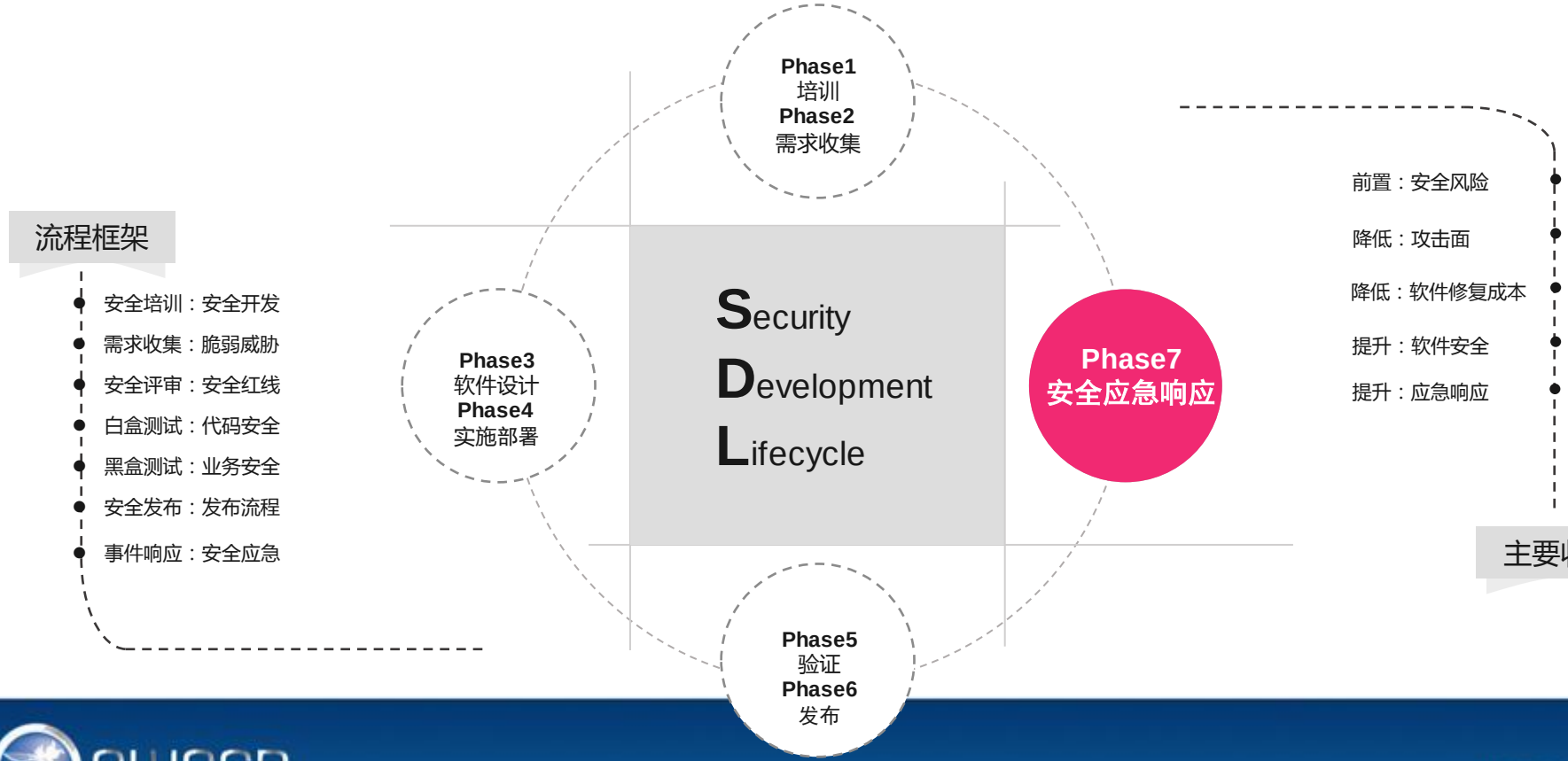


3.3.6 验证与发布

唯品会安全评审自助提测系统



3.4 “安全闭环”唯品会安全应急响应中心



3.4.1 应急与响应

https://sec.vip.com/

四、安全监控与应急响应

VSRC

[1/4] 为什么需要安全应急？

1 › 2 › 3 › 4

- **传播速度快**：整个周末都被勒索软件刷屏
- **覆盖面广**：全球范围爆发
- **案例**：2017年5月13日，全球近一百家遭勒索软件攻击约7.5万台计算机被感染，WannaCry迅速袭击全球各地成千上万个系统。

1

网络威胁形式的多样化和复杂化

新旧挑战

[2/4] 为什么需要安全应急？

1 › 2 › 3 › 4

- 2014年 Heart Bleed/Bash Shellshock
- 2015年 GHOST
- 2016年 Dirty Cow
- 2017年 WannaCry
- 缺乏完善的应急预案

2

业内对严重漏洞的预判能力正在下降

漏洞预判能力降低

[3/4] 为什么需要安全应急？

1 › 2 › 3 › 4

- 上游厂商遭受更多的攻击
- 导致整个供应链工具脆弱性增加
- 行业资质门槛的问题
- 防护能力稍弱的第三方供应商 → 攻击者以其受信任的身份为跳板 → 攻击防护能力较强的企业

3

供应链工具链脆弱性增加

威胁泛化

[4/4] 为什么需要安全应急？

1 › 2 › 3 › 4

- E.g. 2015年初 CVE-2015-0002 Google的安全小组发现了一个Windows8.1的漏洞，在微软尚未对漏洞做出修补的情况下，Google严格按照自身的标准，在第90天公布了漏洞详情。
- **保护用户安全？** 还是 **保障用户的知情权？**
- 一些漏洞披露方采用了更灵活的漏洞披露方式

4

不正当的漏洞纰漏

漏洞修复未完成

4.1

唯品会安全应急响应中心

——VIP Security Response Center（VSRC）

https://sec.vip.com/

唯品会
vipshop.com

基础组件 固有风险

a. 基础系统本身也是程序
b. 缺少安全设计 软件风险无法预估
c. 安全的“木桶原理”
...

线上电商 特卖模式

a. 业务广泛 线上系统多
b. 互联网在线业务
c. 暴露大量入口
d. 攻击者触手可及
e. 暴露攻击面广泛
...

人为因素 木桶原理

a. 小步快跑敏捷迭代
b. 匆忙上线未经过安全评审
c. 快速迭代未经过安全评审
d. 项目进度缩短未经过安全评审
e. 违反安全开发红线
f. 内部人员的违规操作
....

唯品会
安全应急响应中心
VSRC

无法避免 漏洞被外部发现...

$ 黑灰产业

巨大利益
分工有序
肆意泛滥
...

$ 黑客攻击

恶意竞争
技术抗衡
...

$ 信息泄露

恶意舆论
负面影响
资产受损
...

外部威胁

唯品会安全应急响应中心 重要职责

——VIP Security Response Center (VSRC)

唯品会
安全应急响应中心
VSRC

1、漏洞及威胁情报安全应急响应

a. 安全漏洞处理
b. 安全事件溯源
c. 脆弱性分析及系统整改
d. 其他相关事件及处理

2、黑客入侵事件处理

a. 黑客入侵事件响应
b. 相关后续工作事宜

3、信息安全窗口

a. 协助企业信息安全危机公关
b. 传递企业对信息安全的态度

4、连接内外枢纽

a. 对外开放的交流平台
b. 反馈唯品会安全风险的途径
c. 加强与业界同仁间的合作交流

凝聚内外部安全力量的枢纽！

唯品会安全应急响应中心 提升重大威胁检测效率

4.4

唯品会安全应急响应中心 提升安全应急效率

安全应急

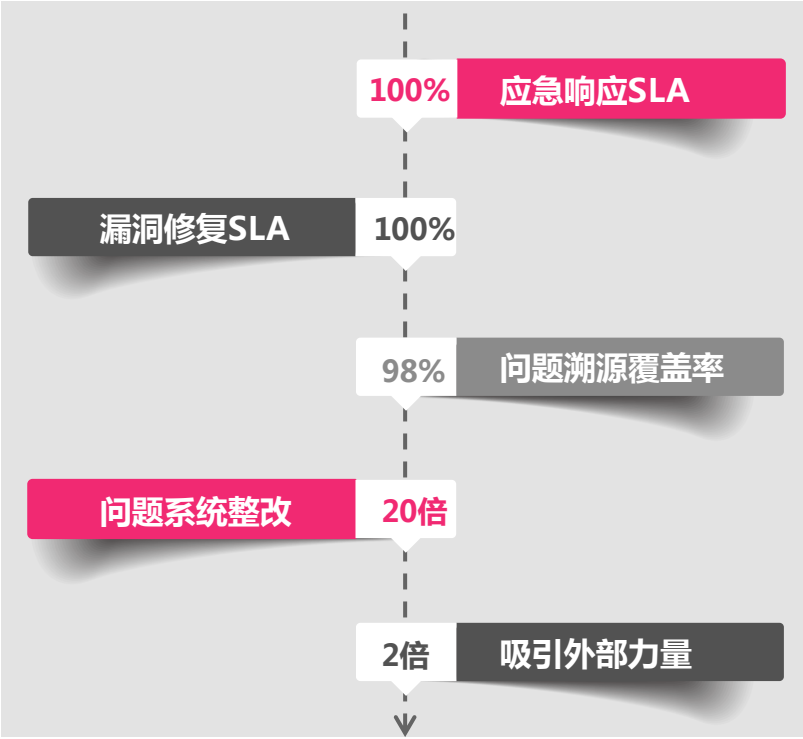
- 应急响应SLA 100%：
- 做到**7*24小时应急SLA**的安全应急响应

- 漏洞修复SLA 100%：
- 跟进开发**100%漏洞修复SLA** 完成漏洞修复上线

- 及早抑制发现内部风险：
- 基本达到**98%问题溯源**

- 整改下线域名 4个月时间
- 问题子域**近180个**下线 提升近20倍

- 企业内部安全系统试金石
- 有效传递**100%唯品会信息安全的态度**



4.5

唯品会安全应急响应应中心

安全感

- 吸引外部白帽子数量 新增127名 上升2倍
  达500人
- 唯品会安全应急响应应中心微信公众号关注人数
  增加数千人
- 公众号技术分享文章阅读量
  16万上升到了20余万人次
- 外部反馈 技术分享 内容质量优异

提升：
唯品会会员对唯品会的安全感

提升：
唯品会会员对唯品会的信任度

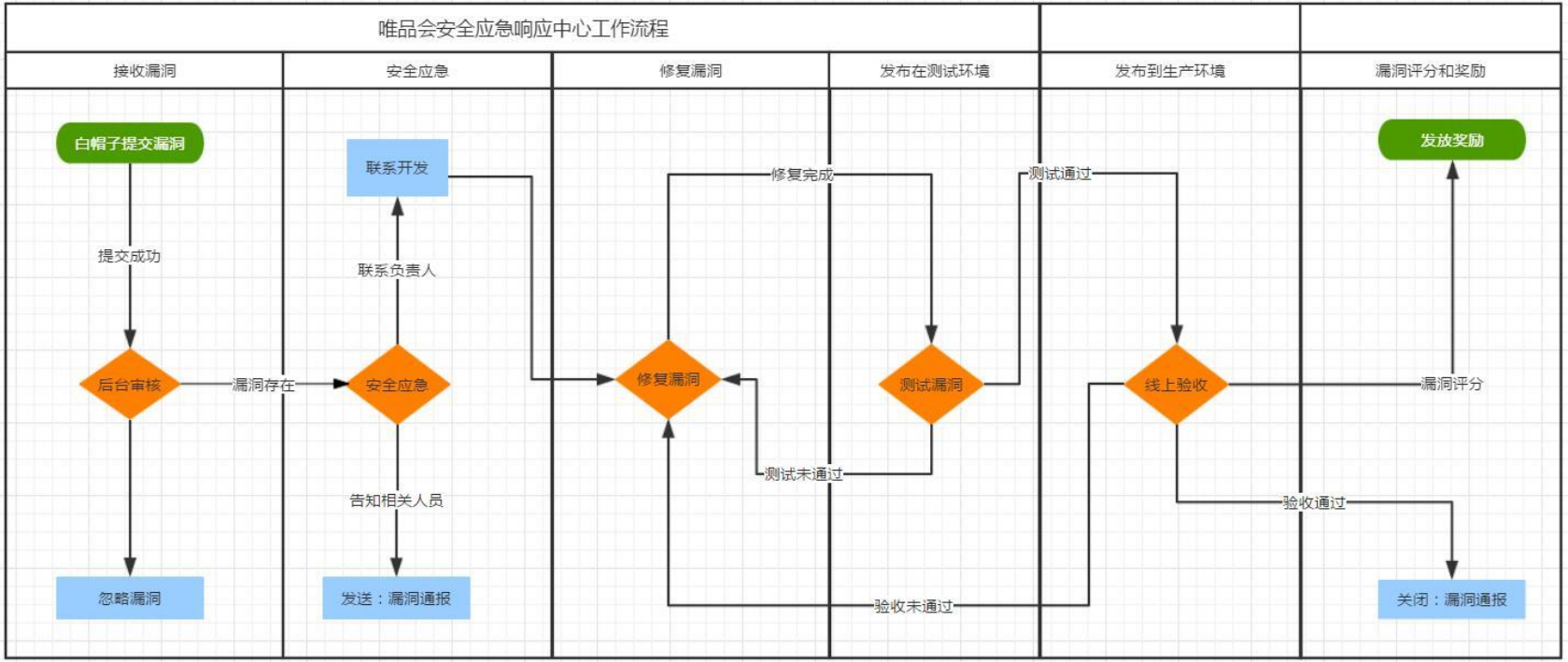
提升：
唯品会信息安全工作在行业内影响力

提升：
唯品会安全应急响应中心行业内知名度

4.6

VSRC安全应急闭环流程

——Responsible Vulnerability Disclosure Process



案例1：VSRC史上最高奖励记录：5万元

30分钟应急完毕全部机器

浅析：
Java RMI远程
反序列化任意类及
远程代码执行解析

原因：
1、业务上线前未经安全评审
2、端口的巡检策略有待调整
3、其余关联性安全问题

2/4 11:40 发现风险

2/4 11:42 验证漏洞
2/4 11:44 联系业务方
2/4 11:50 确定缓解措施
2/4 11:55 通知相关人员

2/4 12:15 处理受影响服务器

2/4 13:00 排查受影响范围
2/4 13:20 处理全部受影响服务器
2/4 15:00 全部服务器处理完毕
2/5 追根溯源 讨论最终解决方案

2/4 15:30 完整事件处理报告

案例2：第三方平台系统泄露大量敏感文件

除夕前一天的下午

第三方平台

安全开发红线

安全意识薄弱

违反上线流程

多处违反安全编码

除夕前天下午....

15:20 发现风险并确认危害

15:30 关闭外网服务

一周时间 软件整改

五、安全工作的“实干者”

“沧海横流”的时代 不做”预言家”

TIPS:

风险前置

资产清单

提前预知

…

尽管面对种种恐惧，但是自身的进步和发展，才是最大的“安全”

感谢您的聆听!

唯品会安全应急响应中心

专业

我们致力于保护用户信息安全
我们积极营造更加安全的
线上电商购物平台

微信号：VIP_SRC
官方网站：http://sec.vip.com
微信公众号：唯品会安全应急响应中心
漏洞接收邮箱：sec@vipshop.com