唯品会 | 唯品会安全应急响应中心

因唯安全 所以信赖

2017唯品会第二届电商安全峰会

——深度揭秘唯品会信息安全建设实践

苏州
中国·苏州

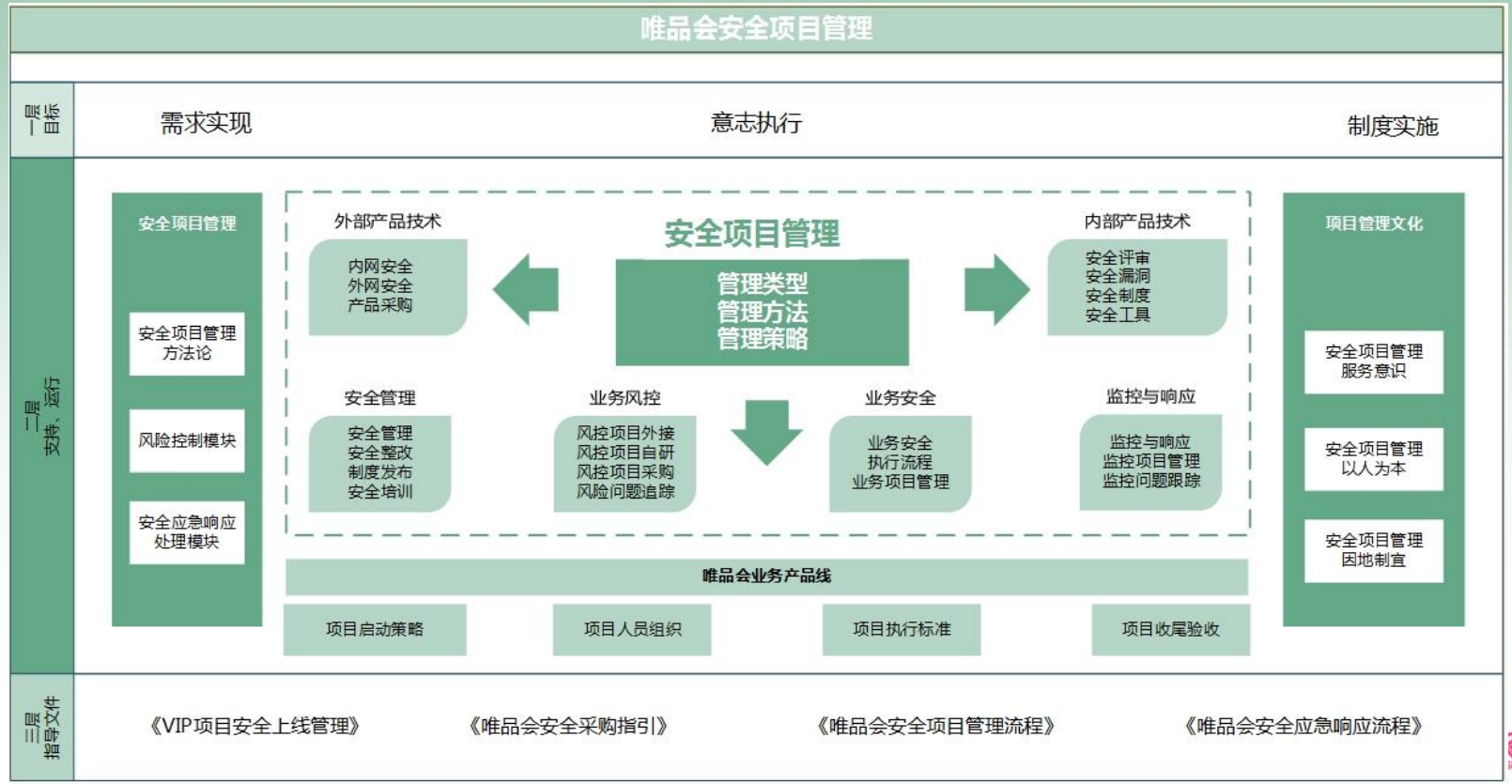
“钢铁意志 优雅着陆”

——项目管理在信息安全工作中的最佳实践

- 安全项目经理的岗位职责
- 没有安全项目经理什么样?
- 安全项目管理实战案例分解说明安全项目经理岗位职责赋予的作用
- 电商模式下安全项目经理的大侄

什么是安全项目管理?

安全项目管理做什么?



没有安全项目经理

口口相传、职责模糊、项目推进困难、资源浪费、监督跟踪滞后、上线验收找谁、知识传递困难

有安全项目经理

流程制度、漏洞跟踪、项目运营

流程制度——内部流程制度，外部执行落地

《VIP项目安全上线管理流程》的诞生？

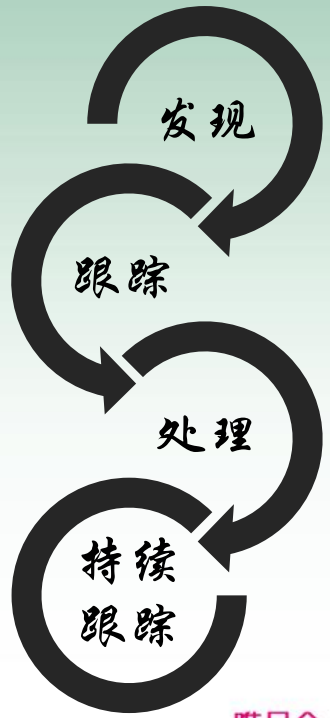
- 邮件往复，Excel记录
- 安排耗费时间，环境沟通复杂
- 质疑排期时间，质疑工作量评估

=》解决之路：流程+制度+培训+定制化+惩处

漏洞跟踪——内部整改下发，外部监督跟踪

- 漏洞责任方的认定
- 产品线对接负责人短期内不予修复

漏洞跟踪也是SDL里重要的一个环节！



项目运营——内部资源联动，外部资源协调

不理解安全项目价值
按照版本规划排期
不掌握产品线的资源
跨团队项目管理

唯品会VPMM管理体系
安全项目管理流程

业务上的安全项目
安全采购的项目
安全基础建设

联动机制—oauth项目

- 淘汰基于PHPSession的会话管理机制
- PC所有相关域对接Oauth使用Passport_Token

=》导致的直接结果就是大量恶意请求不能直接踢下线

项目1—oauth

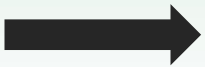
安全项目开展：

- 你抢了我的资源
- 你的项目不是我的kpi
- 依托于别人
- 顾前顾后，没人顾中间
- 业务和安全的冲突

项目1—oauth

安全项目执行：

- 人员更换
- 移动端不能受到影响
- 容错与降级
- 新旧会话兼容
- 跨部门沟通、测试与联调
- 20+域的大调整
- 10+域一次性同步调整
- 12个第三方联登业务不能丢



迎难而上

全局把控

果断决策

强制执行

项目1—oauth

12个第三方
联登业务不能丢弃

高流量 → 梳理业务、谁梳理？

低流量 → 下线？谁拍板？

项目1—oauth

安全项目收尾：

上线后效果的持续监控

同步结果给各个业务部门

安全项目不截止在当前

业务负责

价值科普

多策略

安全项目管理

启动：解决冲突，掌握资源

规划：全局管理，紧急程度

执行：果断决策，迎难而上

收尾：持续跟踪，业务负责

多么痛的领悟，安全得有自己的项目管理团队

安全项目经理需要的素质？

安全项目管理练兵
-特卖模式下的电商大促

安全项目经理的VIP大促

业务目标——62小时 200亿!!

系统稳定支持62小时 500亿!!

到点开始，到点结束；短时间对业务高并发，对安全的考验

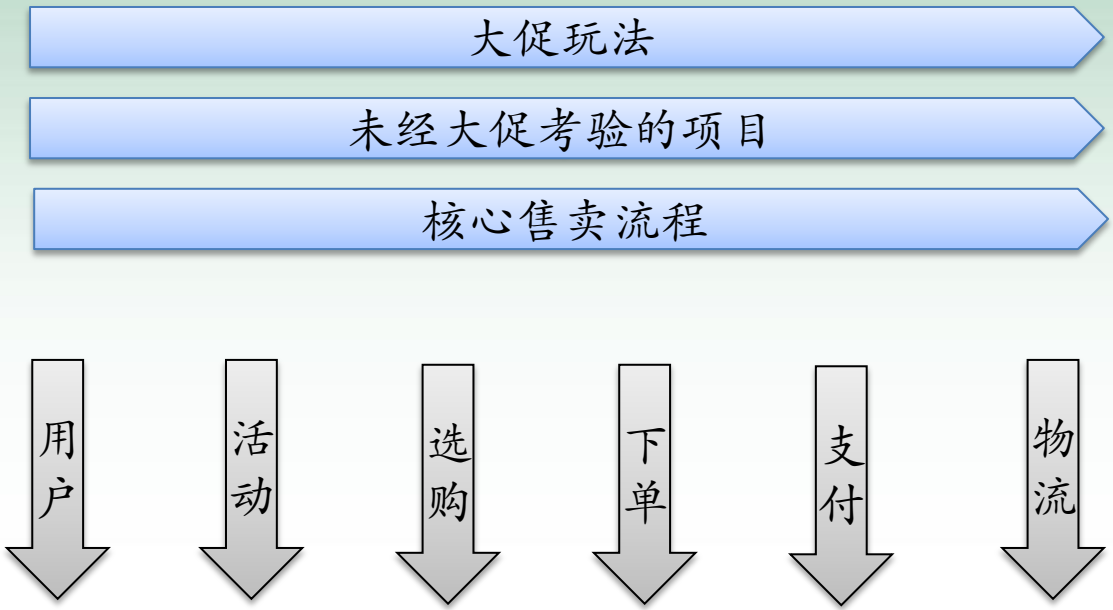
唯品会 | 唯品会安全应急响应中心

安全项目经理的VIP大促

- 安全挑战：
- 日常项目可以回滚
- 工作重合、冲突
- 人员多、乱
- 安全的考验

安全项目经理的VIP大促

战前情报收集



安全项目经理的VIP大促

1 启动

明确职责
同步玩法
输出项目

2 执行

活动评审
大促项目

3 监控

活动+监控

4 开始前

项目关闭
所有既定的执行动作完成

5 开始

主战场

6 收尾

复盘

怎么把安全项目管理做的更好？

谢谢您的倾听！

唯品会 | 唯品会安全应急响应中心

VIP Security Response Center

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