企业安全建设点滴分享

Baidu 百度

2016.07

罗启汉

内容要点

安全建设中的典型现象与“坑”

如何应对其中的问题

甲方安全人才主要构成

安全建设大致历程

孵化新安全产品、安全服务 → 增强对抗能力

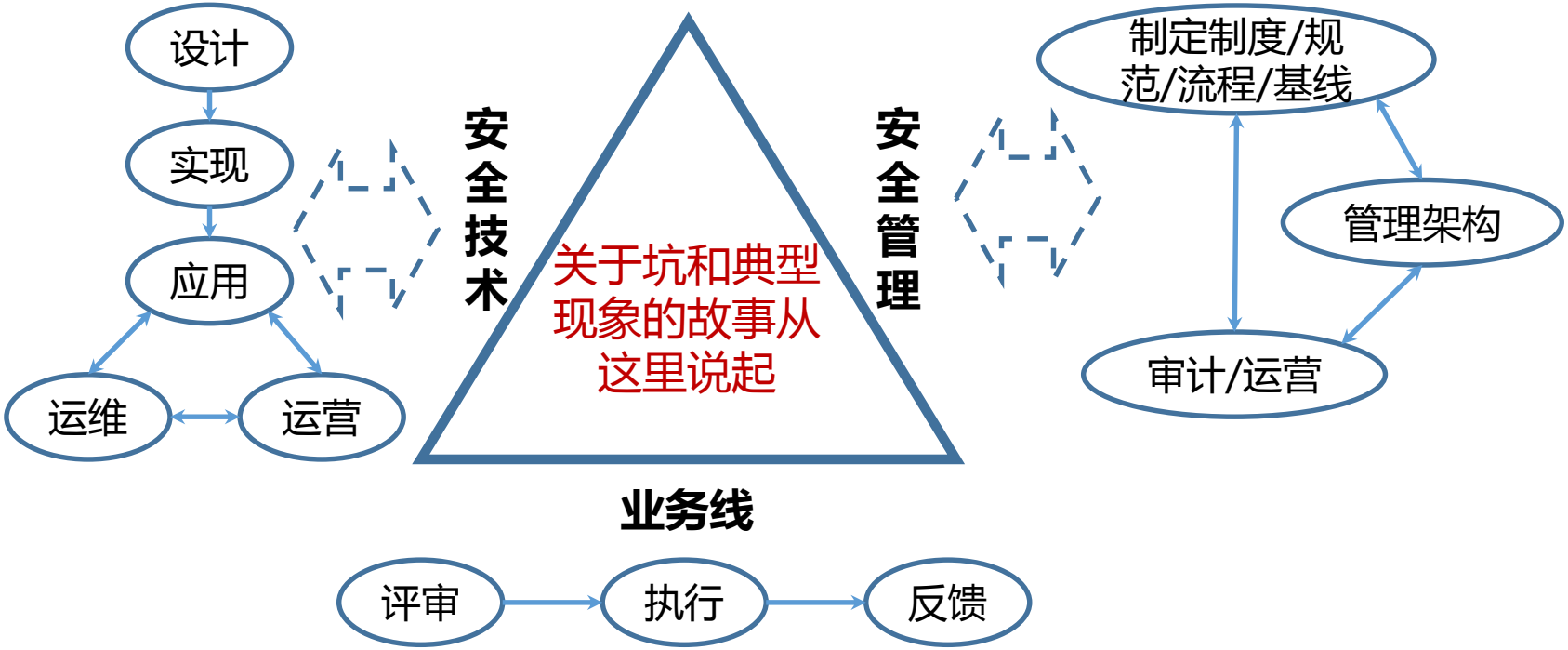
重点业务生命周期安全保障 → 为重点业务保驾护航

扫描、阻断、审计、监控、风控等 → 安全对抗的基础

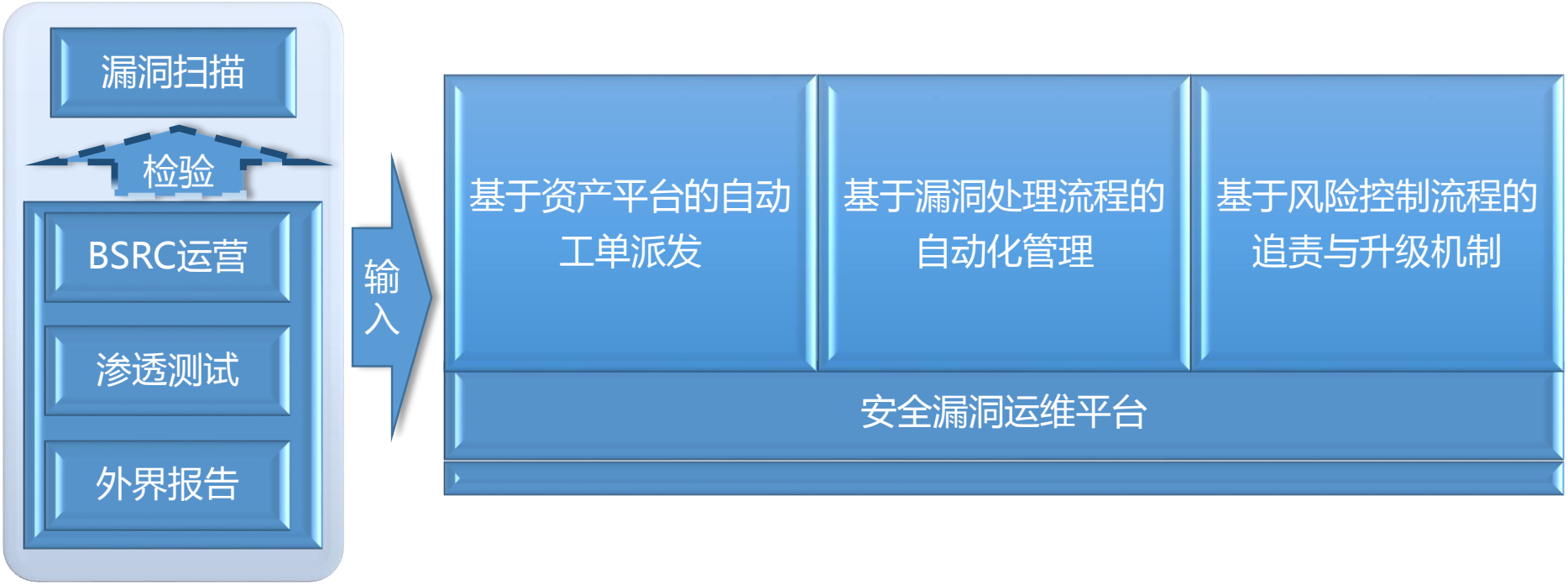
应急响应、漏洞收集、基线/策略、意识教育等 → 基本安全保障

当然实际情况并非严格如此

然而这个历程并不平坦


设计
实现
应用
运维
运营
安全技术
关于坑和典型现象的故事从这里说起
安全管理
制定制度/规范/流程/基线
管理架构
审计/运营
业务线
评审
执行
反馈

安全漏洞处理与管理


漏洞扫描
检验
BSRC运营
渗透测试
外界报告
输入
基于资产平台的自动工单派发
基于漏洞处理流程的自动化管理
基于风险控制流程的追责与升级机制
安全漏洞运维平台

安全漏洞修复中业务线的反应

- 信息泄露：删除泄露的资源
- SQL注入漏洞：修复发现的注入点
- 看似毫无影响的CSRF漏洞：忽略吧

这样解决了问题，但似乎有一丝丝的不安？

> 详细说明：
>
> http://[redacted]/info.php
>
> http://[redacted]/.git/config
>
> http://[redacted]/examples/jsp/
>
> http://[redacted]/.svn/entries

安全漏洞修复中业务线的反应

CSRF 漏洞接口：

http://[redacted]template/projectcreate

POST name=xss_payload&componentName=helloworld&id=1

Self-XSS 漏洞触发页面：

http://[redacted]/template/project

安全工程师：最终窃取了用户的认证信息，劫持了用户账户
RD：！！！这就修复漏洞去

安全工程师的汗与“汗”

- 汗：
  - 产品线的安全漏洞为什么还是这么多：不停的发单处理
  - 产品线同学总会有各种漏洞修复的疑问：不停的分析解释
  - 产品线同学修复漏洞至少Check 2次才能确保修复完成
  - 。。。

安全工程师的汗与“汗”：隔行

- “汗”：
  - **RD**：这个服务端的算法和校验方式别人不知道的。。。
  - **然而还是被黑了。。。**
  - **OP**：我通过Server配置限制了上传目录不可执行PHP。。。
  - **然而依旧被黑了。。。**

安全工程师的汗与“汗”：制度与流程的问题

- “汗”：
  - **RD**：有漏洞的这个系统，相关项目组已经解散了。。。
  - **安全工程师**：。。。
  - **OP**：漏洞系统的IP是我帮别人申请的，但“别人”是谁让我想想。。。
  - **安全工程师**：。。。

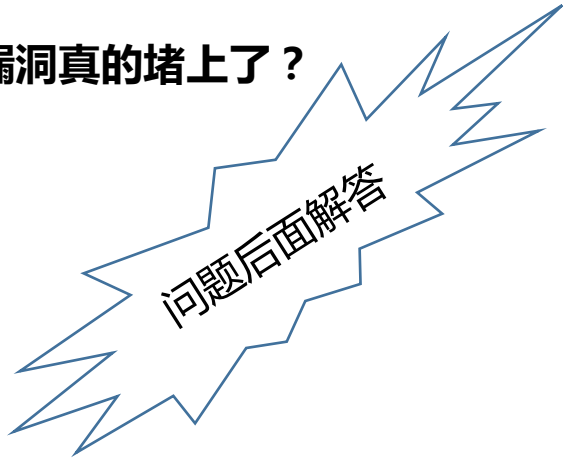
事件/0Day应急与管理

应急响应中业务线的反应

- **典型现象：**
  - **我们这个被入侵的系统没有记日志/日志只保存一天/。。。**
    - 没有资源、开发测试用、没有需求
  - **发生了安全违规，一线同学：我并不知道这已经违规了**
    - 翻译下：给我一个重视的理由
  - **这个点之前安全这边评估过的，责任应该主要在安全（然而通过邮件却找到了相反的结论，当然这不是这里的重点）**
    - 形成了安全只是一种阻碍的潜意识

应急响应中安全工程师的思路问题

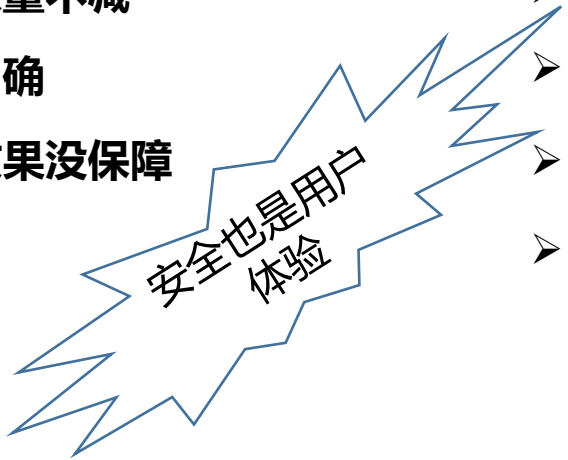
- **典型Case：**
  - **后台盲打：修复完漏洞，溯源与损失分析完成，这算完成多少分了？**
  - **ImageMagick：业务线排查修复完成，然后漏洞真的堵上了？**
  - **。。。**



从现象和“坑”中走出

◆ 业务线

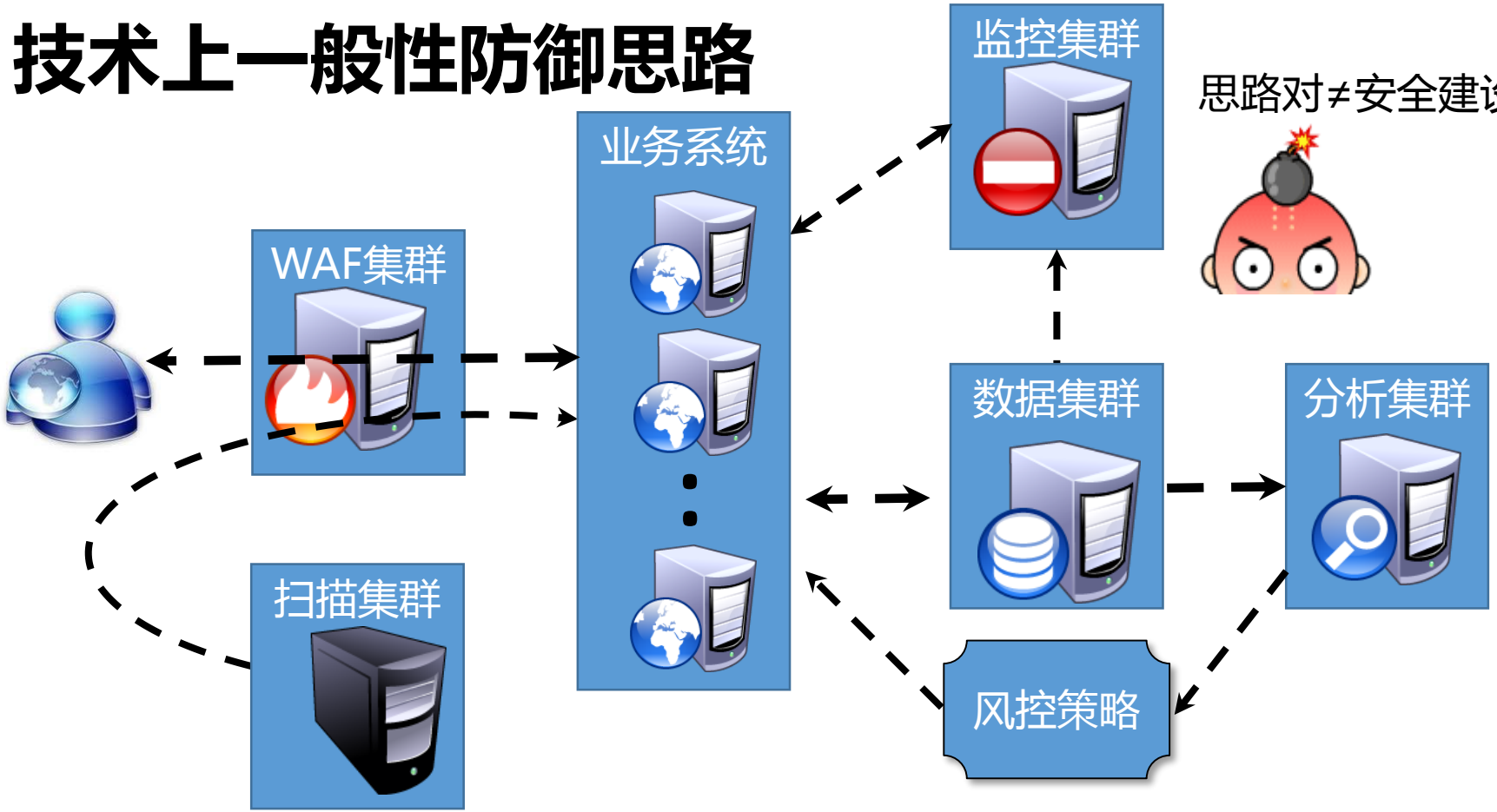
- 对安全问题及相应风险无知
- 安全问题的数量不减
- 资产归属不明确
- 规范执行力效果没保障
- 主责意识差



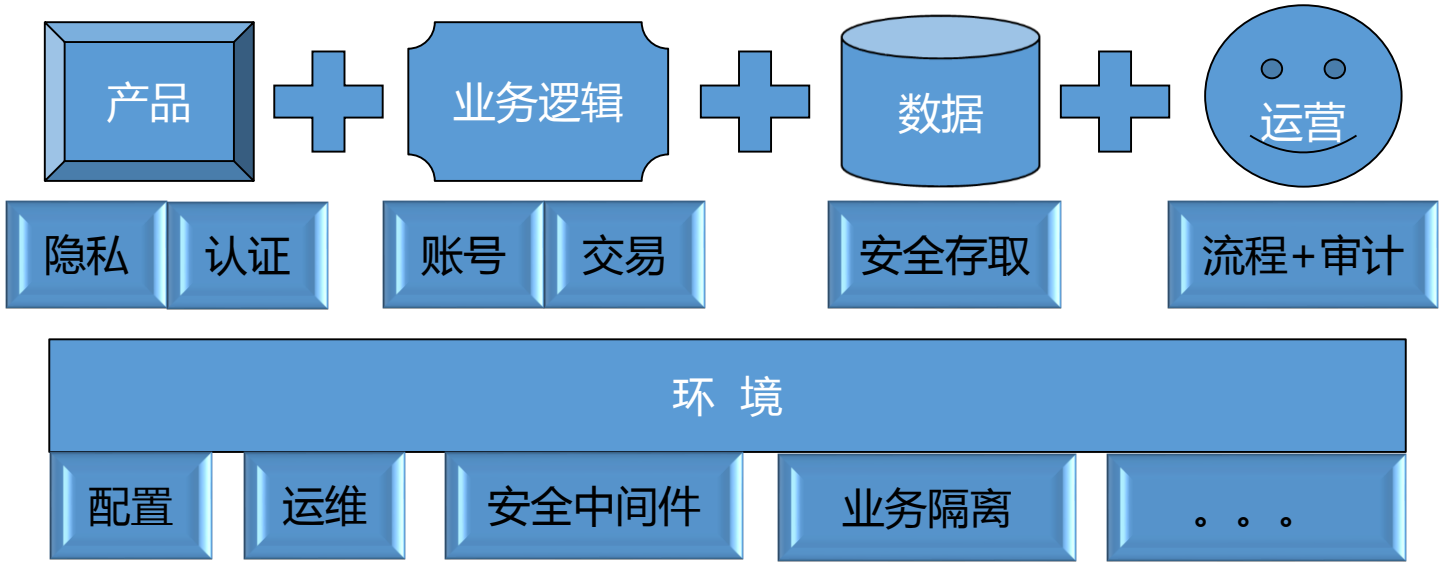
◆ 安全建设

- 安全培训、安全教育、安全制度
- 赋能：扫描、安全库、指南、规范
- 制度化、流程化
- 技术支撑、安全教育、安全追责
- 形成安全管理架构并明确职责

技术上一般性防御思路



重点业务线还应更多考虑



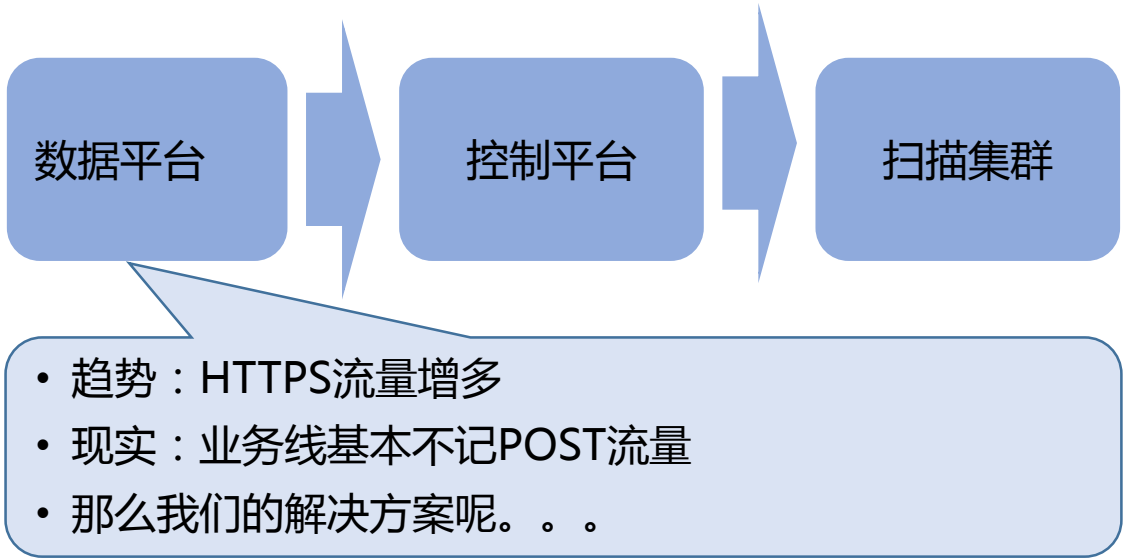
总有问题等待解决？

- **多维度安全风险识别**
  - 聚焦**变化（包括新增）、可控性、核心资产**

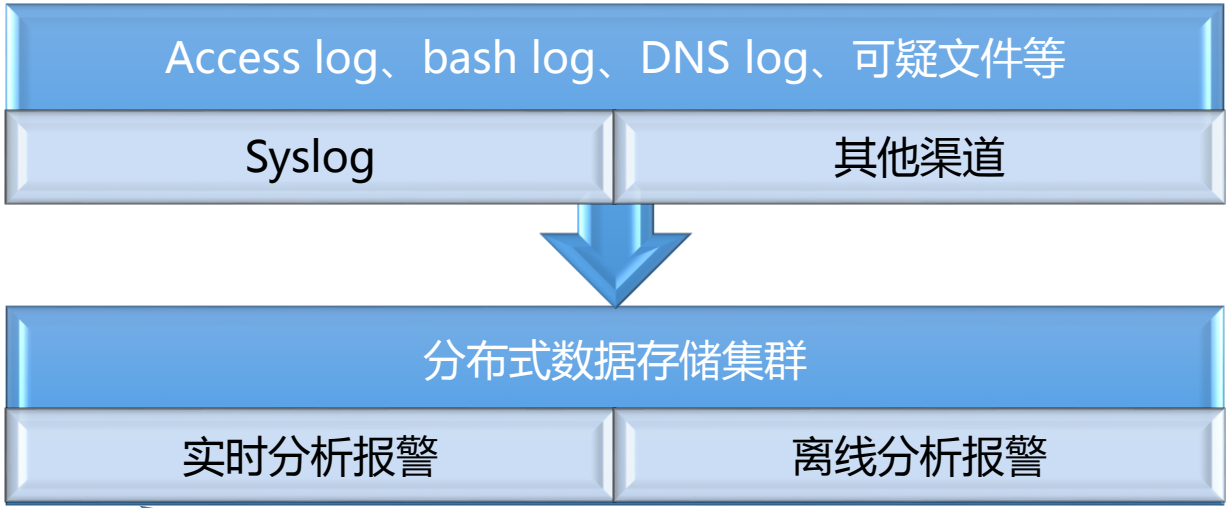
变化	业务、边界、攻击利用、产品技术等
可控性	网络环境、研发质量、人员意识等
核心资产	业务、数据、内部关键服务等

- **风险降低/规避**
  - 定位**缺失能力、方案**

漏洞扫描：数据源问题



入侵监控：方案是否与时俱进了？



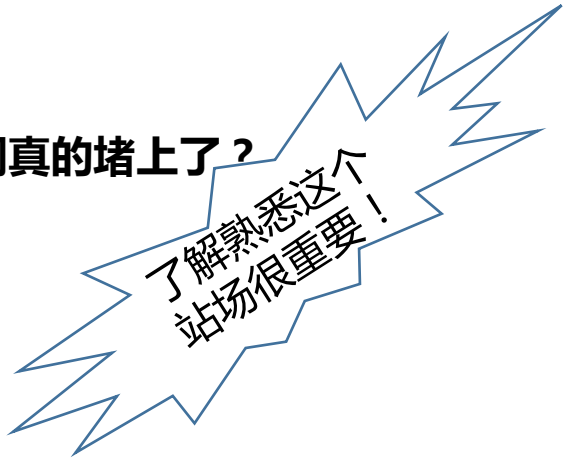
- 趋势：新型绕过、容器/虚拟化提供计算、SSRF成为关注点等
- 那么我们的解决方案呢。。。

安全评估：每个阶段的评估重点

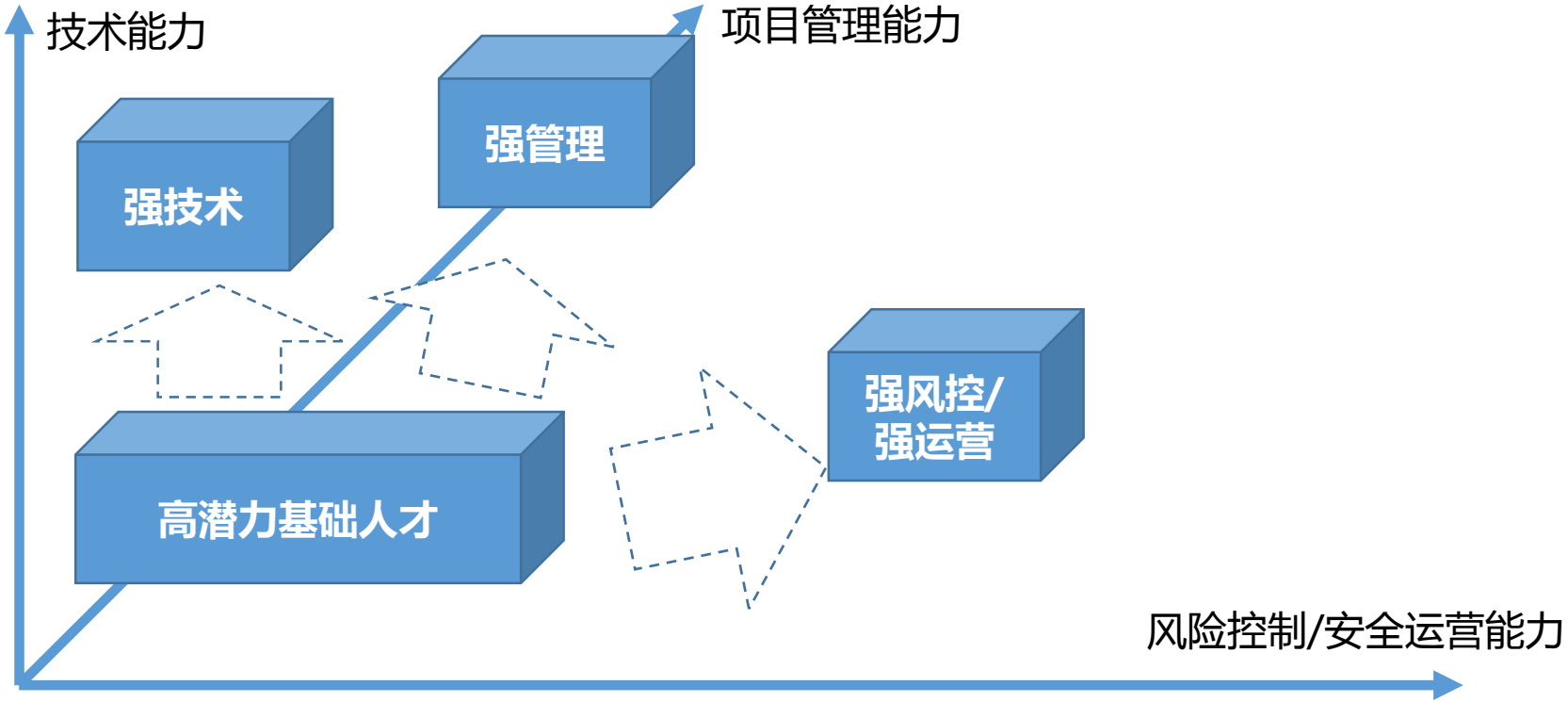
- 几个典型的Case：
  - 从弱账户业务到强账号业务：账号安全评估与保障能力必须跟上
  - 业务重心走向移动端：移动应用安全评估与保障能力必须跟上
  - 业务合并、业务拆分：过渡期安全评估与保障能力必须跟上
  - 。。。

再来看看安全工程师在应急中的问题

- **典型Case：**
  - **后台盲打：修复完漏洞，溯源与损失分析完成，这算完成多少分了？**
    - 还有解决面的风险+执行力问题：根据RD的意识和研发质量看，所有后台都需排查加上Httponly。另外规范/指南呢？
  - **ImageMagick：业务线排查修复完成，然后漏洞真的堵上了？**
    - 边界/源头堵上了么：产品库、框架？
  - 。。。



背后应该有怎样的安全人才支撑？



高潜力

- 有技术基础
- 学习能力强
- 安全思维：批判性、逻辑性、“猥琐”、最小化
- 其他：实战型、自我驱动型、情商高。。。

各角色相互协作才可能做好安全建设

- **高潜力基础人才：**实战在企业安全站场、未来的骨干
- **技术型高工：**应急响应、各安全技术方向的规划者、架构设计与研发、技术成长导师
- **风险控制/安全运营人才：**安全运维质量控制、风险管理、安全培训、流程/制度/规范/基线等落地审计与运营、安全社区运营等
- **管理型人才：**了解技术、熟悉业务，依托安全技术与安全管理、以项目方式打造出产品、服务，并产生可见的安全价值

管理型人才重要之处

- 需要拆分安全技术与安全管理（风险控制&安全运营）的任务并管理协同性
- 需要跨团队、甚至跨部门合作来完成某项安全产品/服务的落地以及最终产生安全价值
- 需要有运营意识，来提升安全实实在在的影响力

Q&A!