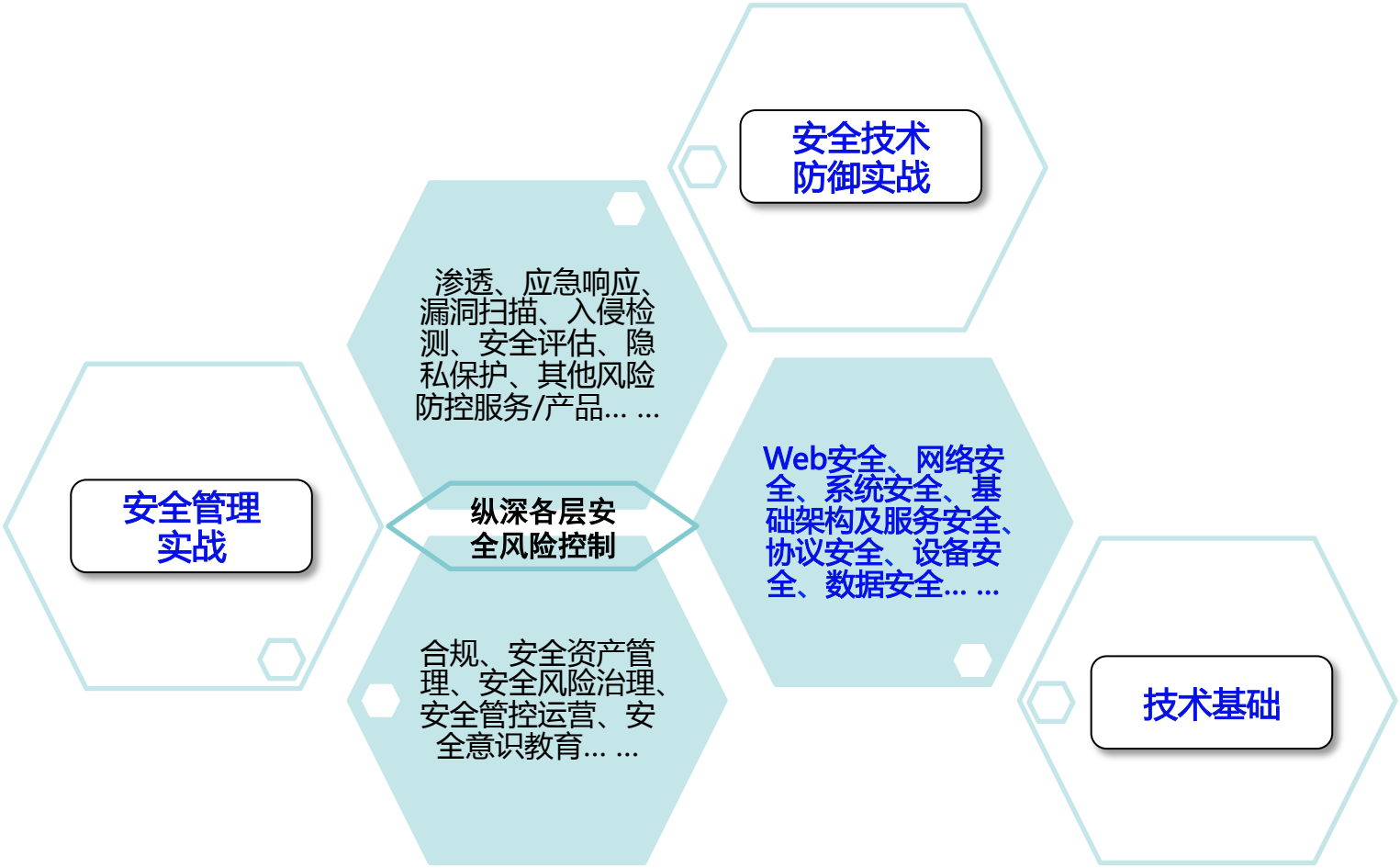
安全防御思维与能力提升分享

罗启汉

2018.11


起步

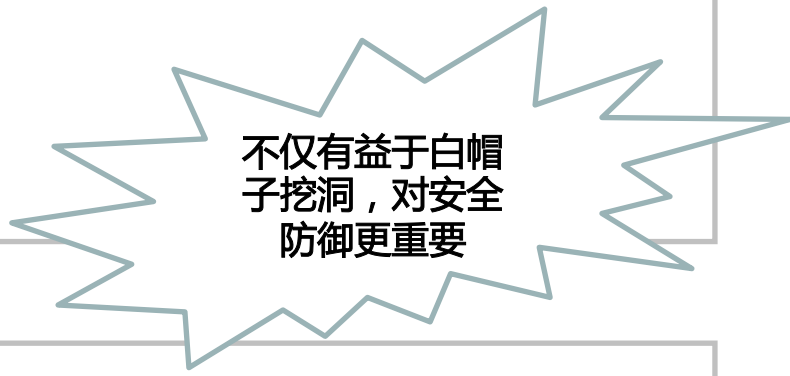
找到自己的初始位置


安全技术
防御实战
渗透、应急响应、漏洞扫描、入侵检测、安全评估、隐私保护、其他风险防控服务/产品… …
安全管理
实战
纵深各层安全风险控制
Web安全、网络安全、系统安全、基础架构及服务安全、协议安全、设备安全、数据安全… …
合规、安全资产管理、安全风险治理、安全管控运营、安全意识教育… …
技术基础

当应用一个成熟的库/组件出现异常时你如何反应？

安全思维要求：

- 对问题的敏感性：批判质疑精神、不放过一个小Bug
- 专研精神：要知其所以然
- 然后举一反三

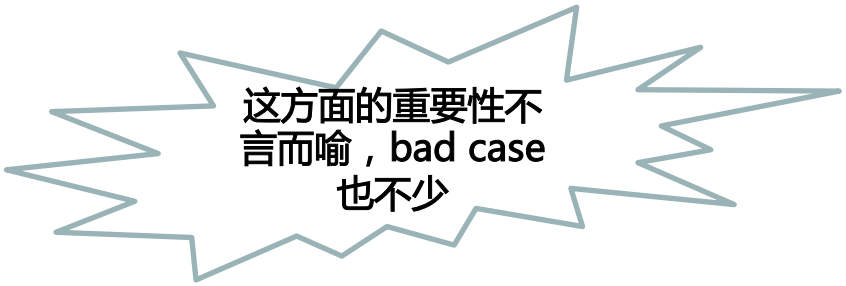


- Case 1：https://www.exploit-db.com/exploits/35892/
- Case 2：https://bugs.php.net/bug.php?id=69364

- 问题 1：宽字节注入场景有哪些？
- 问题 2：曾经的Web Server解析漏洞还有另类的存在么？
- 问题 3：防御性场景中，观察到运维层面异常是否会去分析可能隐藏的安全隐患？

作为安全（管理/技术）工程师需具备的基本素质

- 分享与开放沟通、遵守安全法规：持续能力提升的基础
- 安全与保密意识：安全防御角度的工程师必然接触了解得很多



Question

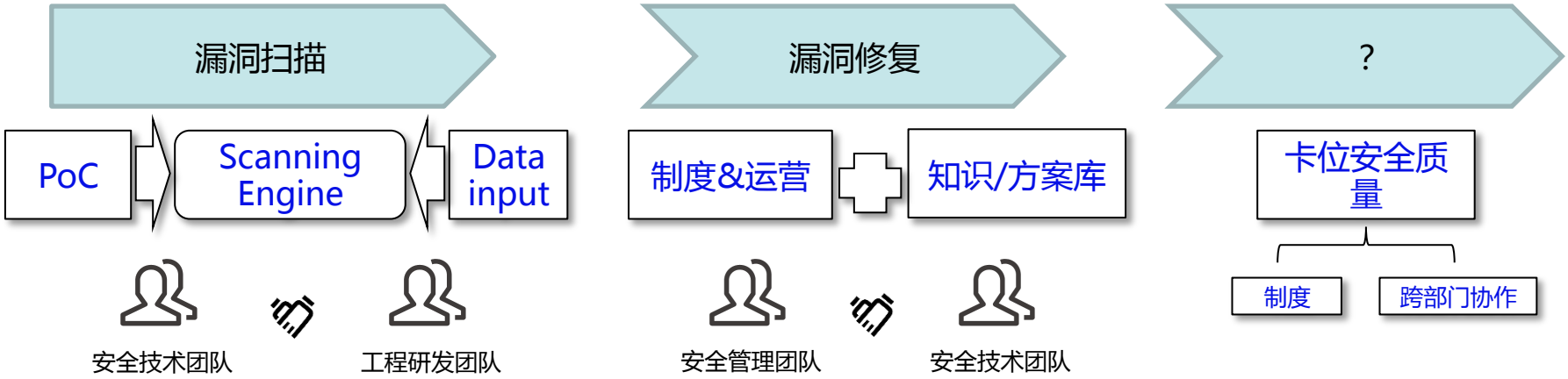
然后我们再看看如何实战做安全防御角度的工作？

安全防御建设：协作非常重要

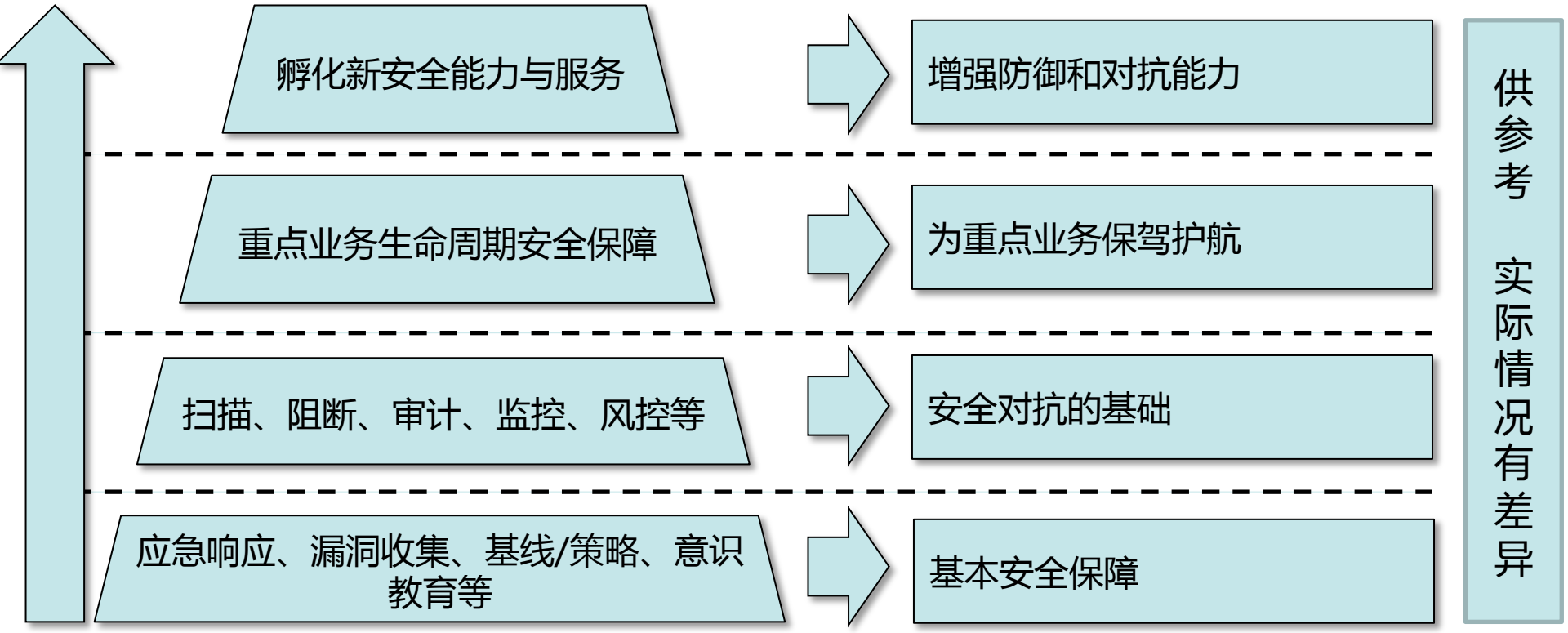
核心是：分工、明确流程与制度、必要时强制安全质量控制

来个典型场景：漏洞扫描与修复

- 当你是在负责几个系统的安全时，很可能发现漏洞→修复漏洞→确认修复→上线整个过程就你一个人搞定了
- 如果你是负责几十上百甚至更大规模的业务系统呢？如果业务系统迭代很频繁呢？1到2个人全栈搞定就很困难了（仅仅是漏洞检测修复这方面）



协作只是起步，安全防御是系统性工程



安全问题解决中应认知到的问题与对策

从现象和“坑”中爬出

- 业务线
  - 认知差异：对问题及风险无知
  - 安全能力受限：安全问题不减
  - 资产信息缺失
  - 规范执行力效果没保障
- 安全防御方
  - 安全培训、安全教育、安全制度
  - 赋能：控制、安全库、指南、规范
  - 制度化、流程化、平台化
  - 技术支撑、安全教育、安全追责

不要被非安全思维带偏

- 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

详细说明：

http://[redacted]/info.php

http://[redacted]/.git/config

http://[redacted]/examples/jsp/

http://[redacted]/.svn/entries

不要被非安全思维带偏

CSRF 漏洞接口：

http://[redacted]template/projectcreate

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

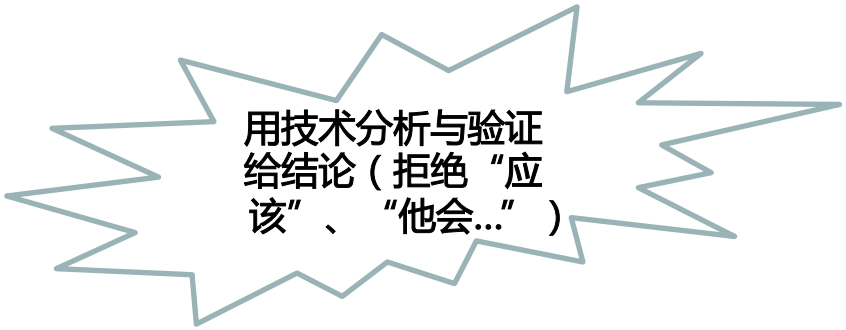
Self-XSS 漏洞触发页面：

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

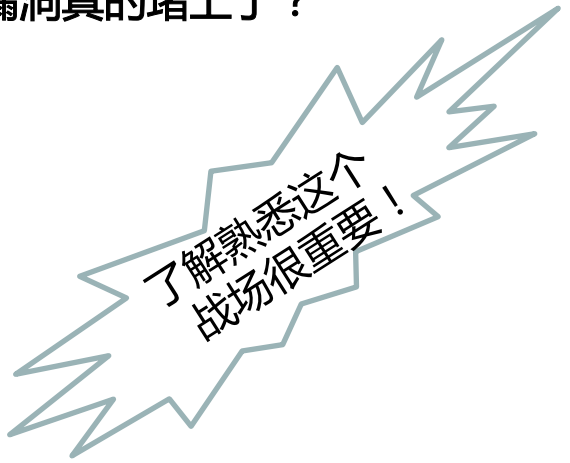
不要被非安全思维带偏

- Case 1：
  - RD：这个服务端的算法和校验方式别人不知道的。。。
  - 白帽子应该知道这里面的坑
- Case 2：
  - OP：我通过Server配置限制了上传目录不可执行PHP。。。
  - 安全是否要直接信任这一结论？



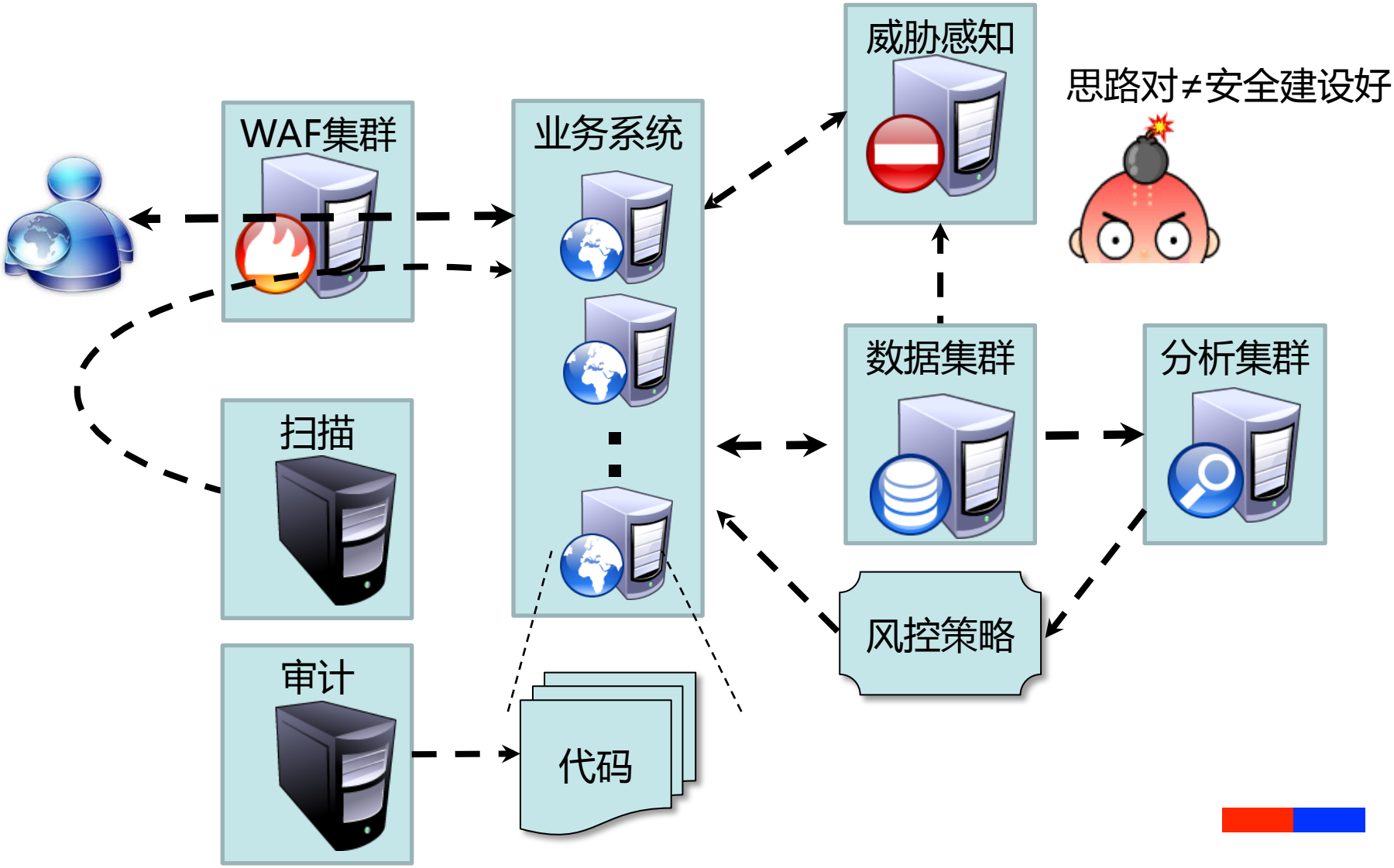
每个安全问题的解决都要判断是否是一个面的问题

- 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？
  - 。。。



安全防御能力建设中应具备的思维与能力

典型防御能力布局示意图

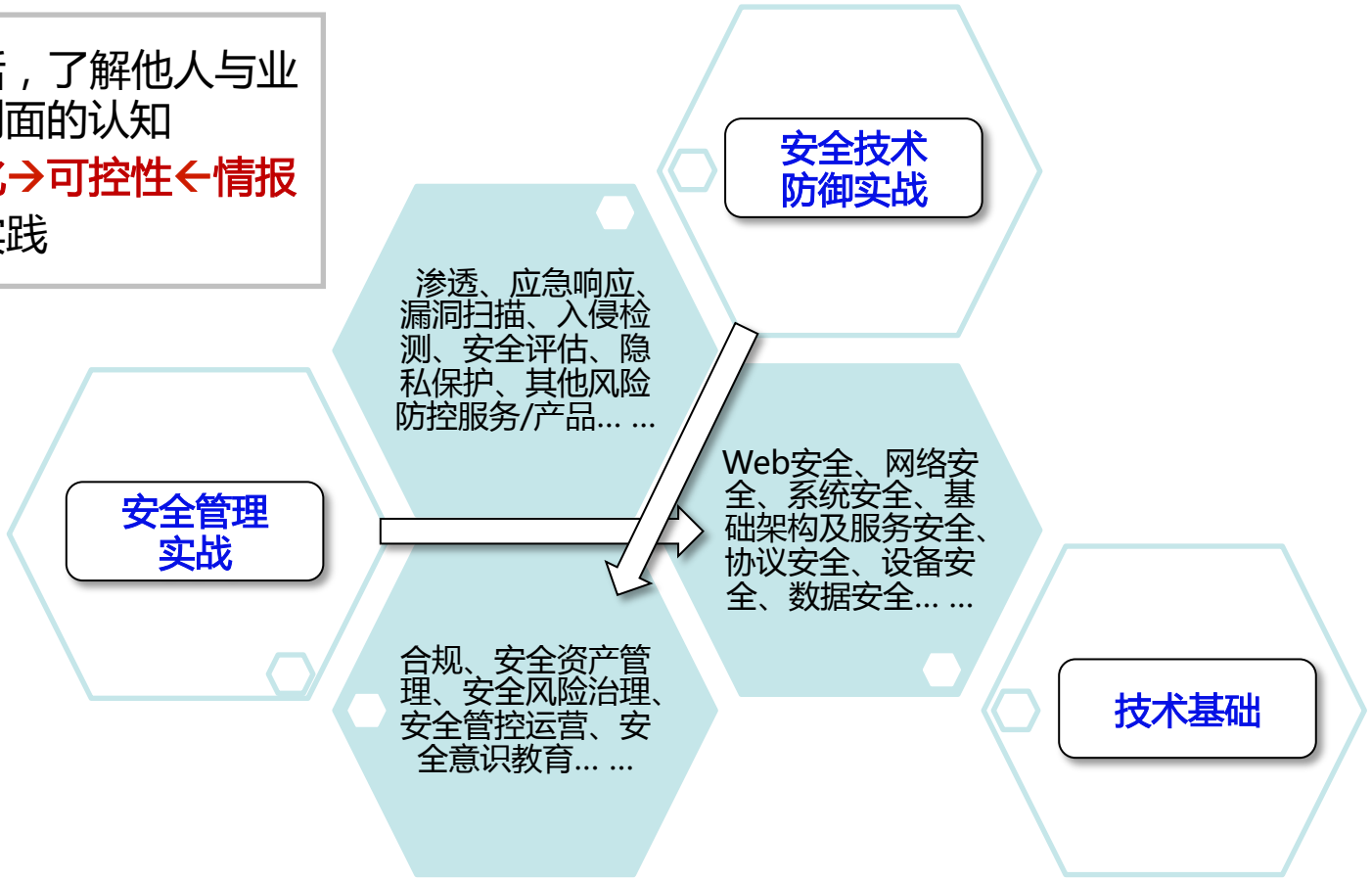


问题来了

- 人力有限，典型防御能力采购就可以快速补位？
  - 性能可满足？
  - 集群可扩展？
  - 策略“松紧”与业务匹配？
  - 误报量运营可接受？可优化到可接受程度？
- 有了防御能力，如何落地生效？
  - 深入了解业务和业务系统
  - 与自身基础环境融合，往往需要多方协作，沟通与推进是常态
  - 如何让沟通与推进有效？案例教育、法律法规宣贯、制度策略
  - 安全防御不是有了安全工程师就可以搞定一切，多方协作是必须的

突破天花板

- 不要一直低头干活，了解他人与业界的工作，提升到面的认知
- 对变化敏感：**变化→可控性←情报**
- 保持归零状态的实践



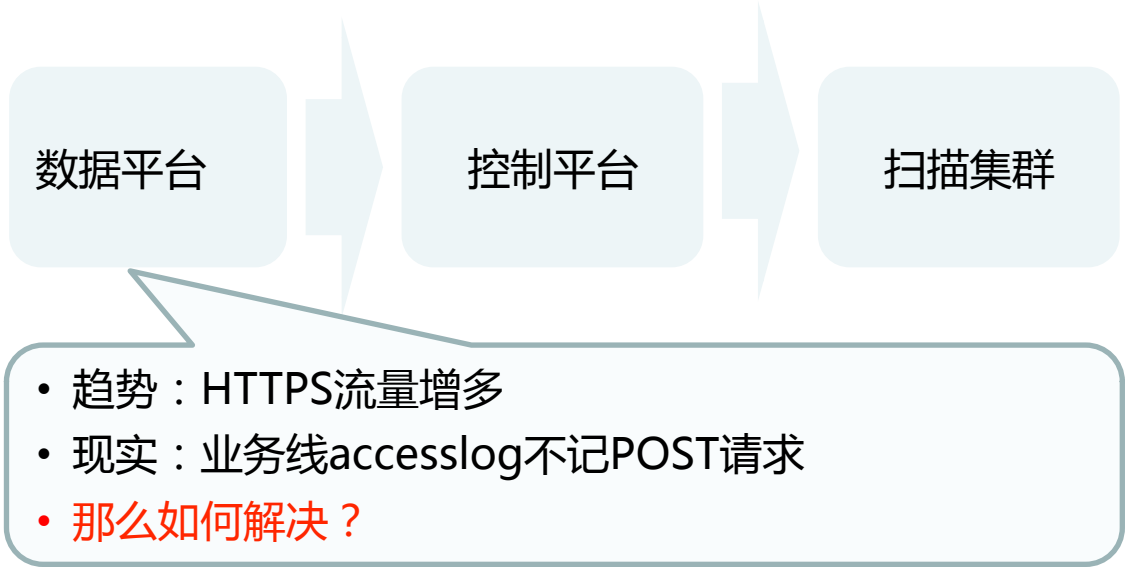
总有问题等待解决？

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

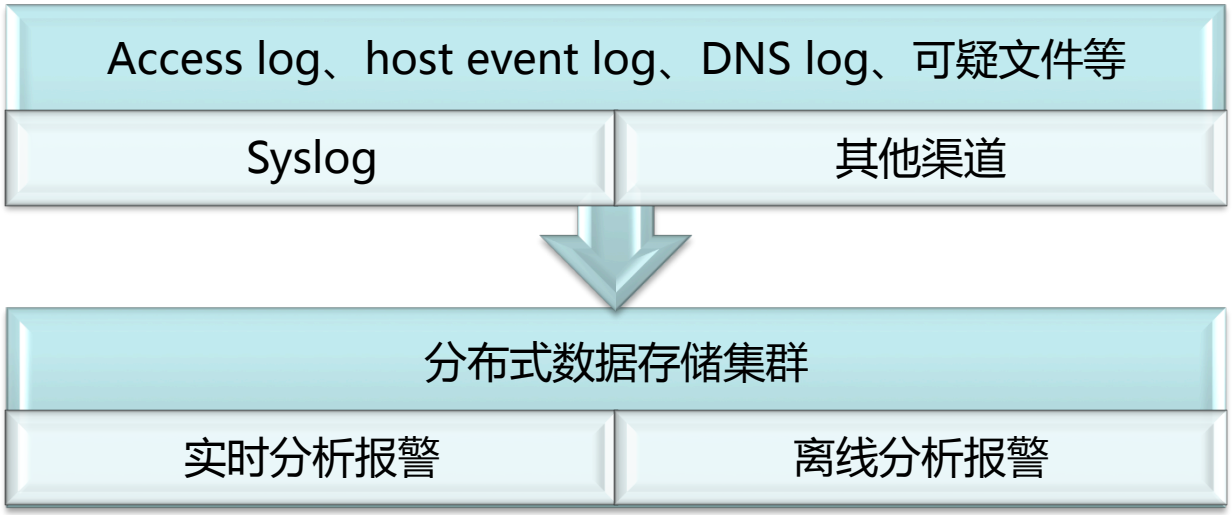
变化	业务、边界、攻击利用、产品&系统&网络技术等
可控性	网络环境、研发质量、人员意识等
核心资产	业务、数据、内部关键服务等

- **风险降低/规避**
  - 定位缺失能力、方案
  - 不要被动等到能力过时

漏洞扫描：数据源问题


数据平台
控制平台
扫描集群
• 趋势：HTTPS流量增多
• 现实：业务线accesslog不记POST请求
• 那么如何解决？

入侵监控：方案是否与时俱进了？



- 趋势：新型绕过、容器/虚拟机提供运行环境、新型漏洞利用等
- 那么数据采集、威胁检测模型还有效么？

Q&A

谢 谢 !