NSC2@19

# 甲方安全建设之路

正保远程教育

李晨

# 目录

CONTENTS

NSC2@19

# 01

# 甲方安全的价值

# 安全事件频发

## 内网安全--勒索病毒

2017年5月12日起，在全球大范围内爆发的勒索病毒“WannaCry”对我国互联网络也构成了严重的安全威胁。由于受到勒索病毒波及，中石油部分加油站出现了加油卡、银行卡、第三方支付等网络支付无法使用的状况。

## 网络安全--Github

2018年3月2日，美国东部时间晚上12：15，知名代码托管网GitHub遭受到有史以来最严重的DDoS功击，峰值流量达1.35Tbps，这次攻击利用了Memcached进行放大攻击，是迄今为止有记录的最大一次 DDoS 功击。

## 数据安全--华住

2018年8月28日早上6点，暗网中文论坛中出现一个帖子，声称售卖华住旗下所有酒店数据，数据标价8个比特币，约等于人民币37万人民币，数据泄露涉及到1.3亿人的个人信息及开房记录，包括姓名、手机号、邮箱、身份证号、登录密码等。

## 账户安全--12306

2018年12月29日，12306 用户数据在暗网传播，这份 12306 的用户数据信息共有 60 万条，信息包括账号、密码、手机号、个人真实姓名、身份证号码、邮箱等重要信息，其中还包括了每个账户中所添加的联系人信息，数据总量更高达410万条。

## 业务安全--拼多多

2019年1月20日凌晨，拼多多被曝出现重大业务漏洞，用户可领100元无门槛券，且并非抢购，而是无门槛领取，优惠券可全场通用（特殊商品除外），有效期一年，黑灰产团伙盗取的相关优惠券，实际资损大概率在千万元左右。

## 应用安全--易到用车

2019年5月26日，易到用车服务器遭到连续攻击，给大量用户使用带来严重的影响。攻击者索要巨额的比特币相要挟，攻击导致易到核心数据被加密，服务器宕机。

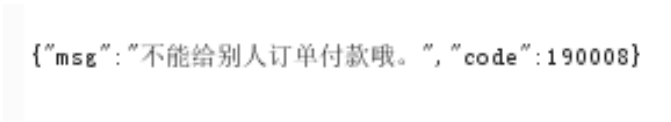
# 传统意义的安全价值

**法律法规：**

- 网络安全等级保护制度2.0；
- 网络安全法（2017年6月1日）；
- 数据安全管理办法（征求意见稿）；
- 儿童个人信息网络保护规定（征求意见稿）；


**企业止损：**

- 漏洞挖掘，降低安全漏洞被利用风险；
- 数据防护，降低数据被拖或被加密勒索的可能性；
- 防止越权，降低业务未授权功能被利用；

# 安全价值与业务结合

**安全标准合规**

安全合规体现在业务合作、项目对接过程中会更加顺其自然。

**数据勒索对抗**

业务用户数据被加密勒索、公司业务、财务员工甚至老板电脑数据被加密勒索导致损失。

**数据泄露影响**

**Github**、内鬼、应用漏洞泄露大量数据导致核心用户数据、业务数据被竞争对手获取。

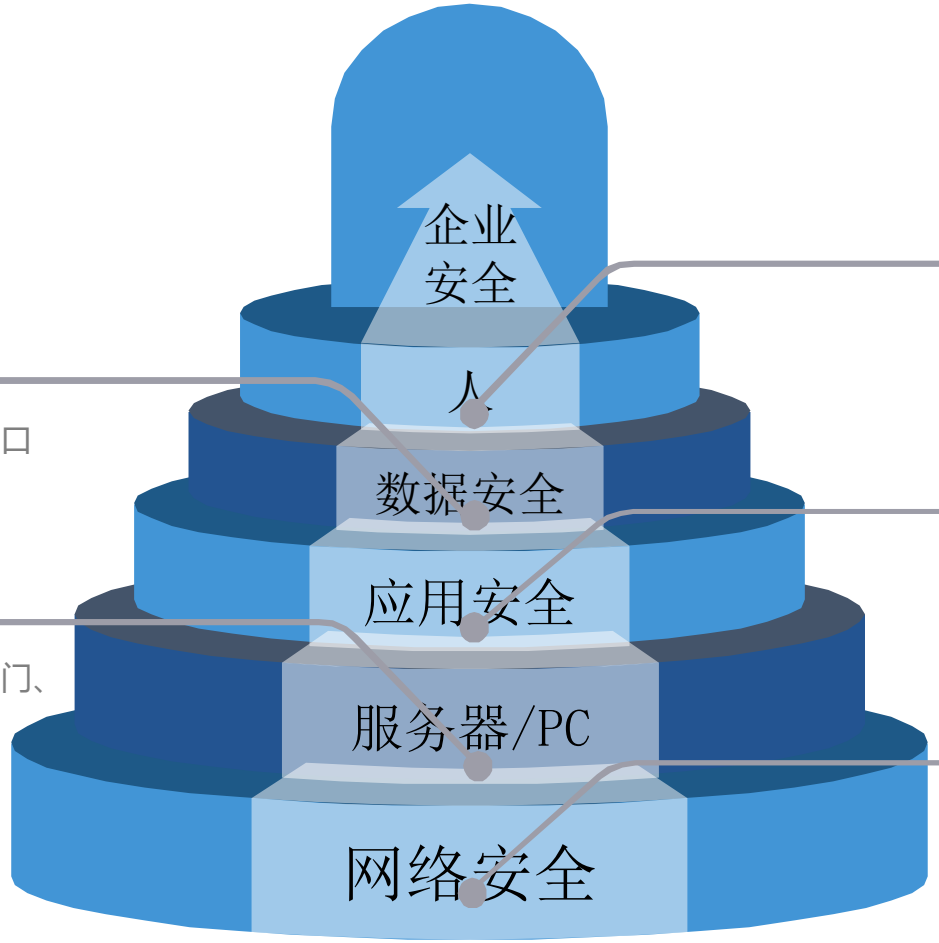
**业务破坏影响**

业务应用的可用性被**DDOS**攻击，业务之上的内容安全被利用传播涉政、涉黄言论。

# 02

# 安全建设的思路

# 安全风险识别




**意识、习惯**

安全操作规范、违规越权、无意识数据泄露

**业务、DB**

数据接口暴露、数据明文存储、弱口令与空口令问题

**服务、权限**

应用漏洞、基线配置、认证授权、弱口令

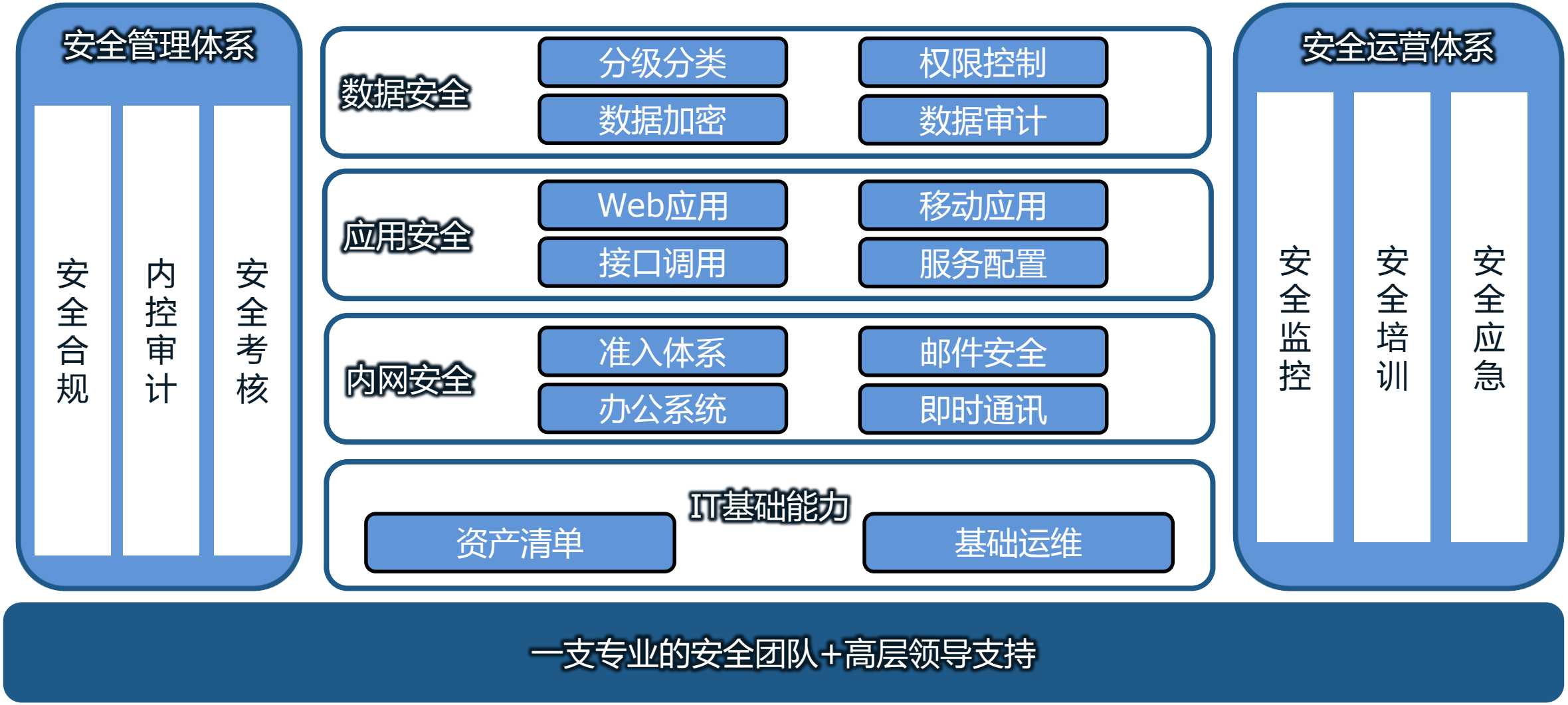
**OS、远程**

系统漏洞补丁、账户权限、弱口令、病毒后门、远程管理、认证授权

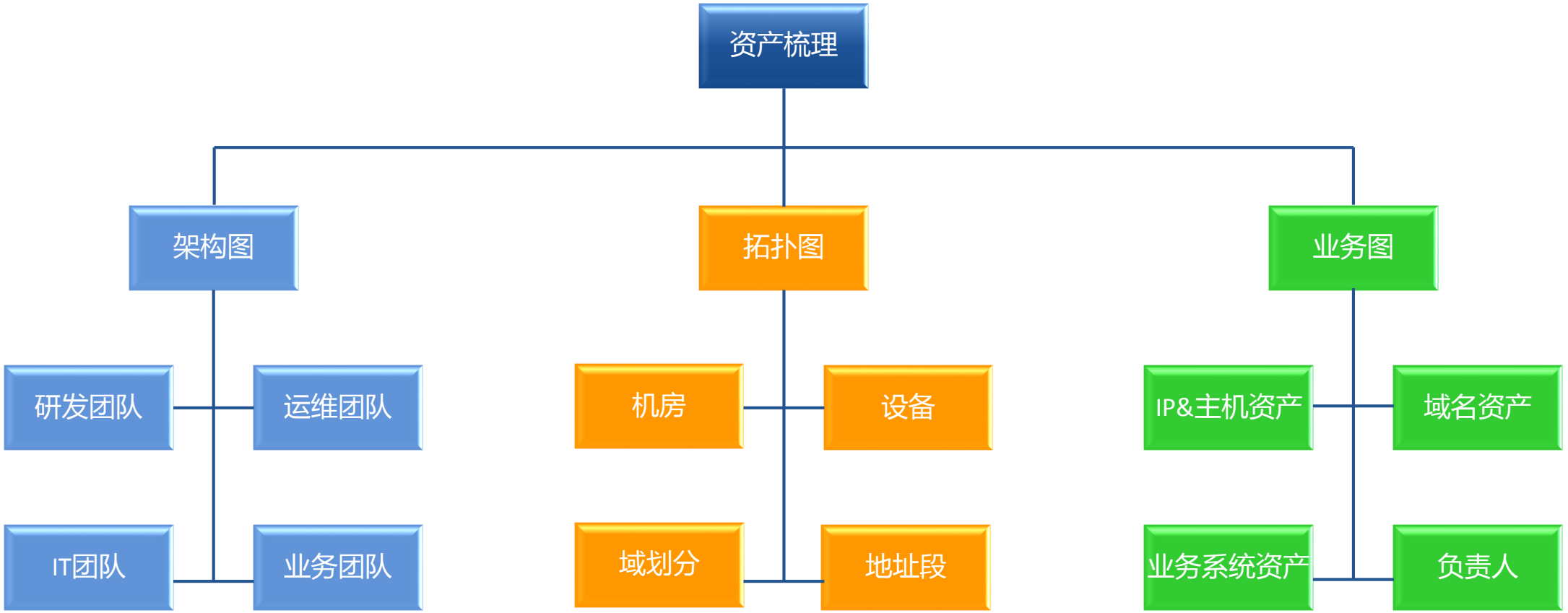
**边界、设备**

边界策略不当、策略失效、安全例外规则
设备弱口令、设备漏洞、不安全配置、权限控制

# 信息安全体系框架


安全管理体系
安全合规
内控审计
安全考核
数据安全
分级分类
权限控制
数据加密
数据审计
应用安全
Web应用
移动应用
接口调用
服务配置
内网安全
准入体系
邮件安全
办公系统
即时通讯
IT基础能力
资产清单
基础运维
安全运营体系
安全监控
安全培训
安全应急
一支专业的安全团队+高层领导支持

# 安全建设-资产梳理


资产梳理
架构图
拓扑图
业务图
研发团队
运维团队
IT团队
业务团队
机房
设备
域划分
地址段
IP&主机资产
域名资产
业务系统资产
负责人

# 安全建设-基础安全

NSC2@19

## 等级保护

- 安全管理制度建立
- 安全域划分
- 安全基线配置

## 安全测试

- 常规周期性安全测试
- 项目迭代安全测试
- 第三方安全测试

## 安全运维

- 安全设备运维
- 安全系统运维
- 安全应急响应

## 账户审计

- 邮箱账户审计
- VPN账户审计
- OA账户审计

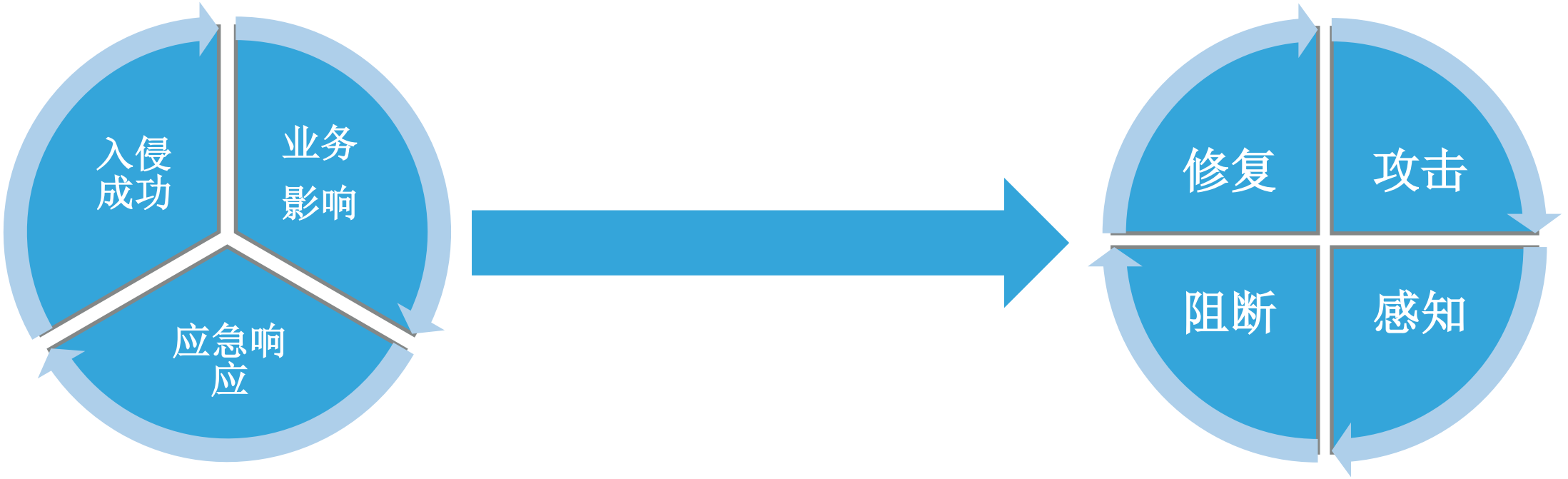
## 边界监控

- 对外资产变动监控
- 敏感端口开放监控
- 端口安全漏洞监控

## 策略管控

- 防火墙策略管控（安全域）
- 映射策略管控（对外）
- 例外策略管控

# 安全建设-安全演进




**被动感知阶段**

**运维及业务通知安全排查问题**

**过程感知阶段**

**安全指导运维及业务应对攻击**

# 安全建设-防护演进

## 入侵阶段

HIDS（主机入侵检测）

- 应用信息识别
- 基线安全检查
- 进程连接检测
- 计划任务巡检
- 用户信息核实
- 登录日志审计

## 攻击阶段

监控中心（日志告警）

- 应用攻击规则告警
- 系统命令规则告警
- 业务逻辑规则分析
- 业务受攻击程度

## 探测阶段

巡风（资产识别）

- IP资产CMDB自动录入
- 自动化周期性扫描
- 业务风险识别

攻 击 路 径

# 03

# 安全落地与实践

# 自上而下的管理体系


## 垂直管理

向上汇报：管理思维，贴合业务，结果导向

向下管理：工程思想，落地实践，赏罚分明

## 水平管理

跨部门横向沟通：解决问题为核心，互利互惠

# 虚拟安全团队建立

## 1 指导安全开发规范

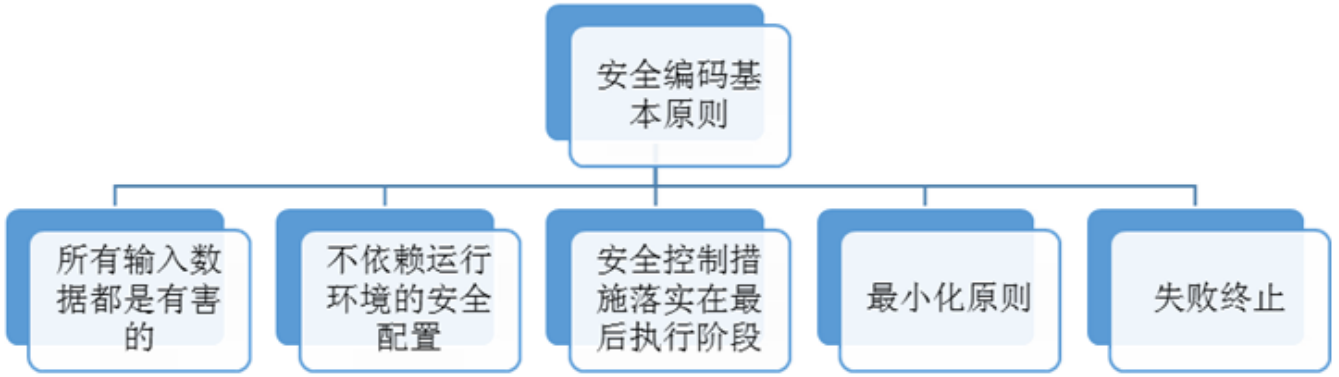
安全开发规范的制定、落地、实施的领头羊

## 2 共享漏洞修复方案

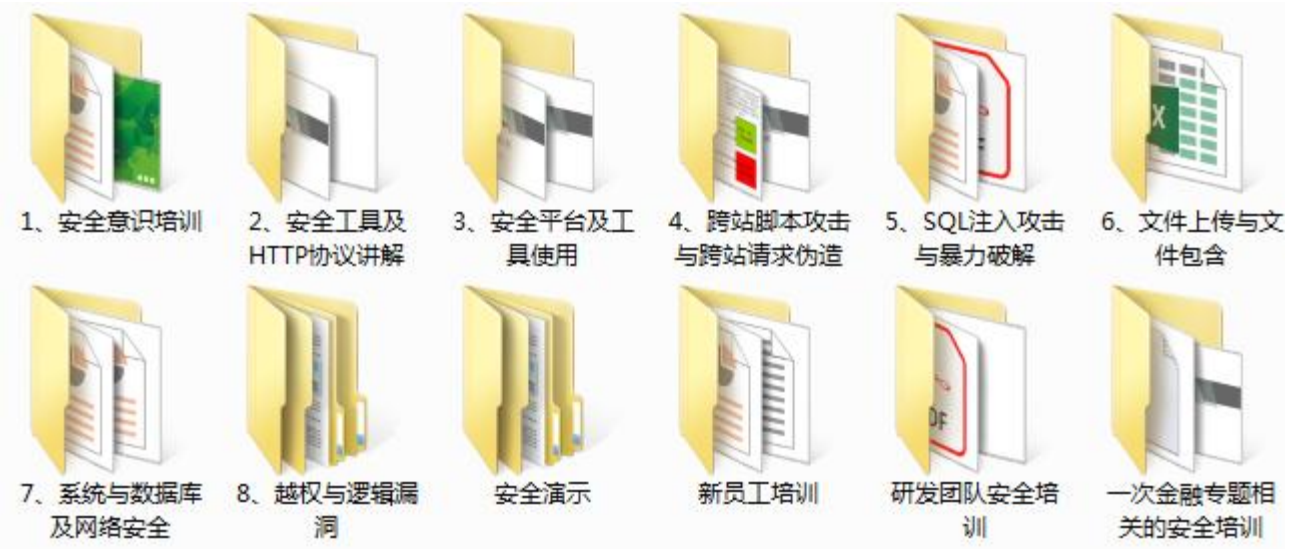
定期例会共享安全问题与修复

## 3 整理问题代码案例

协助整理一份错题集，防止重复错误发生。

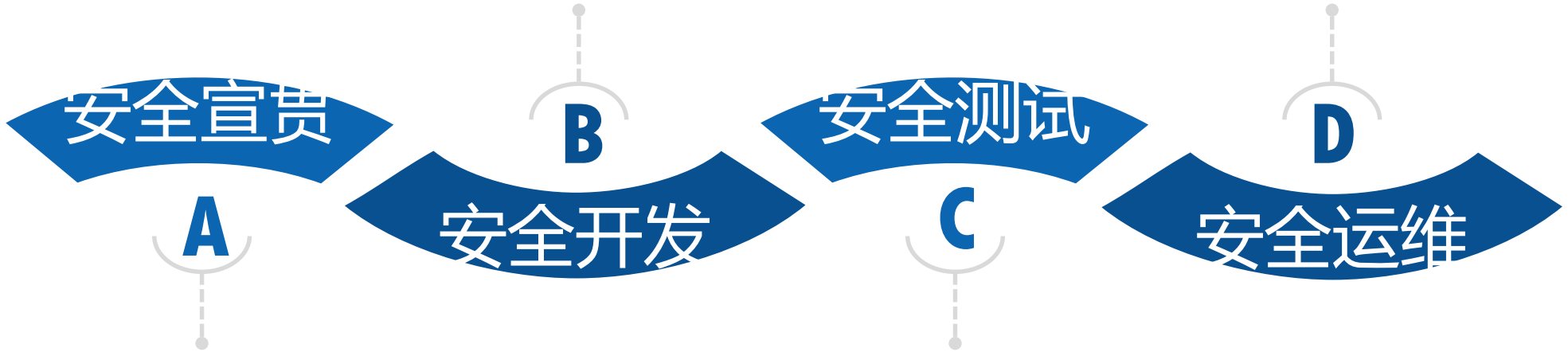



安全编码基本原则




不断细化的安全培训体系

# 因地制宜的SDL




**建立安全培训体系**
明确培训目标，分割培训群体，切实将安全意识、安全技能、安全规范覆盖培训到相应群体

切合当前业务使用主流开发语言，与研发**共同商定**安全开发规范并落实

迭代性安全测试，将安全测试**嵌入到上线流程**中，切实监控版本情况

安全扫描、安全监控、安全应急

# 04

# 安全痛点与思考

# 安全建设痛点与思考

**领导不重视安全**

向上管理、结果导向
换位思考、管理思维

**害怕背锅**

适度背锅、强身健体
过度背锅、灰飞烟灭

**问题修复周期长**

水平管理、互惠互利
垂直管理、自上而下

**人员不足**

二八原则、事半功倍
从无到有、从有到优

NSC2@19

# 感谢各位