GOPS2016 Shanghai

GOPS

2016 全球运维大会

重新定义运维

上海站

会议时间： 9月23日-9月24日

会议地点： 上海·雅悦新天地大酒店

主办单位： 开放运维联盟 OOPSA Open OPS Alliance　高效运维社区 GreatOPS Community

指导单位： 数据中心联盟 Data Center Alliance

B2B创业型企业的安全运营与驱动

卞军军 找钢网安全工程师

目录

发展史

- 2011.12.23年成立
- 全产业链钢铁电商
- 撮合+自营

规模


>>> NOW
to be continued
1400+人大团队
1家韩国海外分公司
家合作物厂
26家分支业务机构
1家新加坡海外分公司
1家武汉二级研发中心
6万+企业买家会员
1家长沙云电商研发中心
157家合作仓储及加工中心
18万+个人注册会员

找钢B2B特色

1. 用户
   - 用户规模相对稳定，或可控性增长
   - 访客相对集中

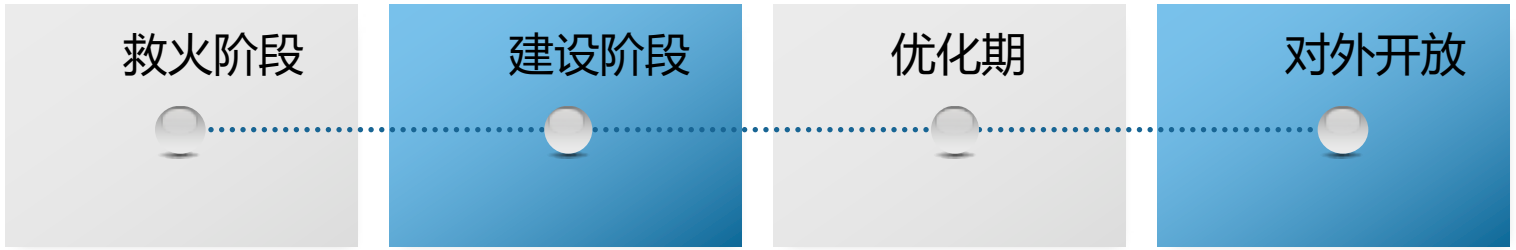
2. 业务
   - 相对于2C，服务群体集中，业务发展明确可控
   - 核心业务在内网
   - 偏向传统行业

历史遗留问题

- 物理安全混乱
- 应用部署不合理、未标准化
- 手动发布，失误多，易发故障
- 监控不全面，故障定位困难

目录

通用公式



第三方平台安全漏洞
当前面临的攻击

生产网络和办公网络
内部IT扩展至全公司

自研工具

安全对外开放

救火系列

- 高危漏洞修复
- 外网安全测试
- 安全规范发布
- 安全开发培训
- 安全平台建设

安全体系建设

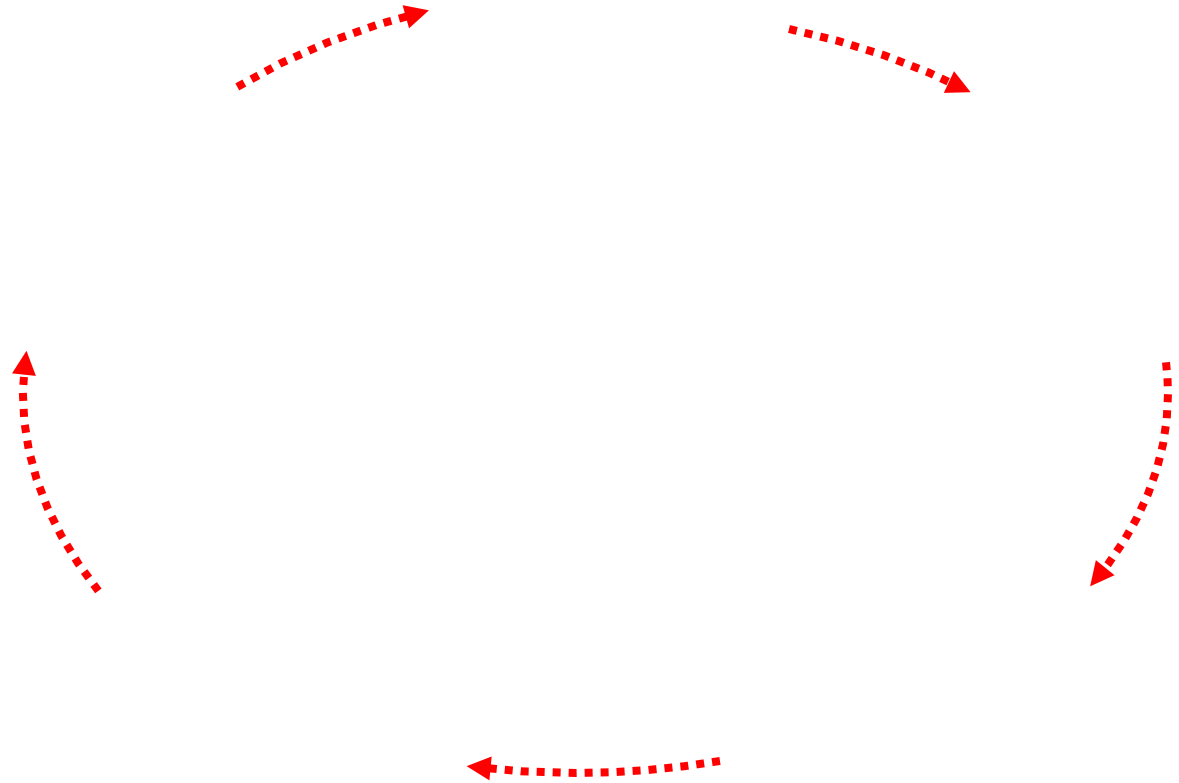
物理安全
网络安全
系统安全
数据安全

认证服务
授权服务
加密服务
目录服务
日志服务
web服务

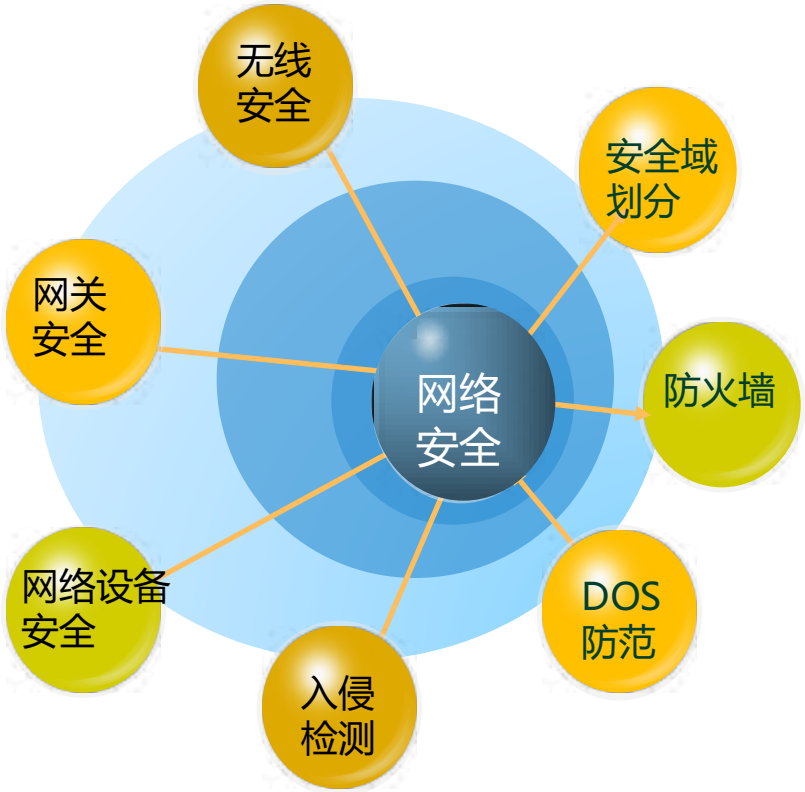
资源管理
身份管理
访问管控
流程管理

安全监控
事件响应
变更和配置管理
安全补丁管理
灾难恢复

防泄密
桌面安全
终端安全
准入控制
VPN安全
源码安全



网络安全

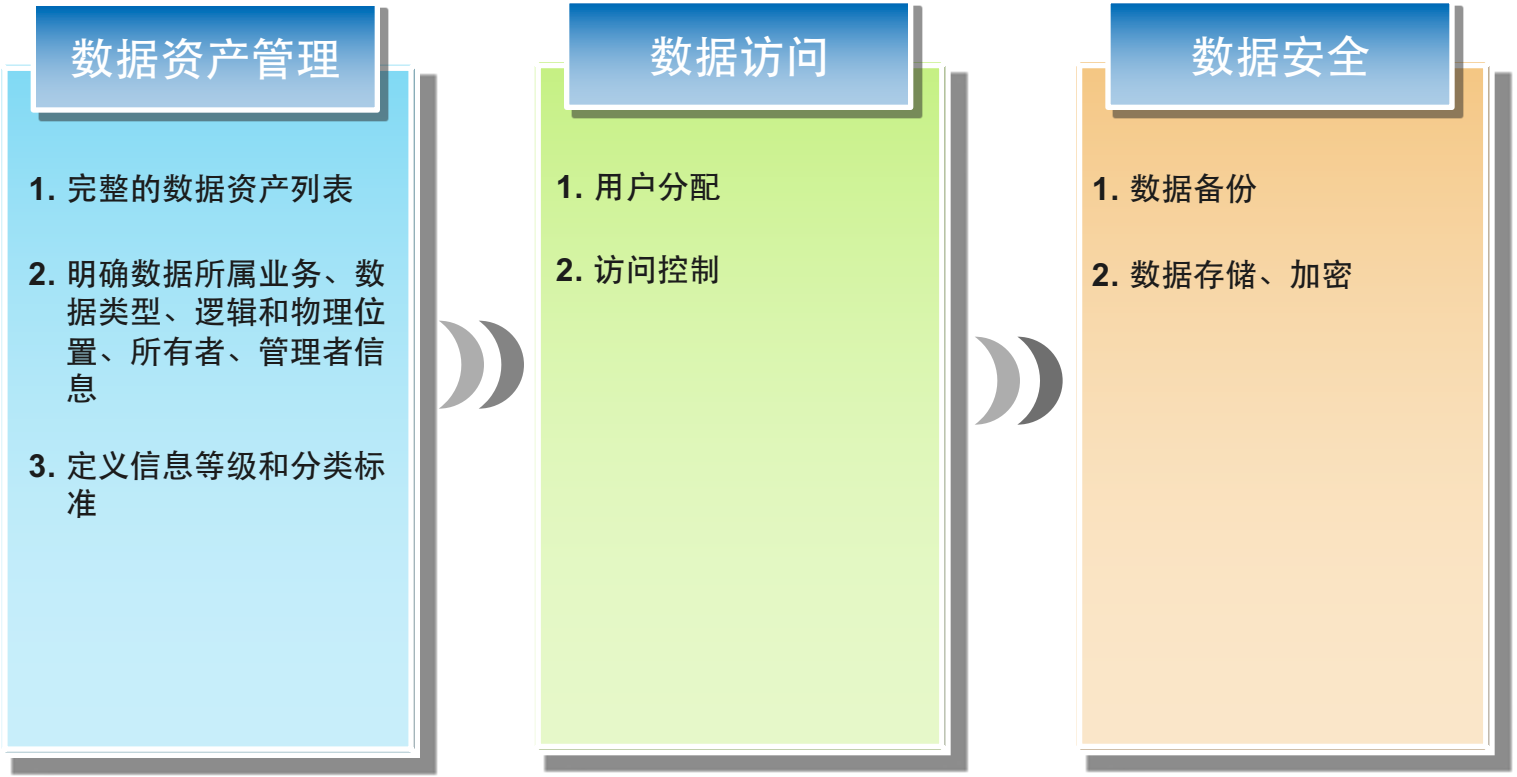


参考！=照搬

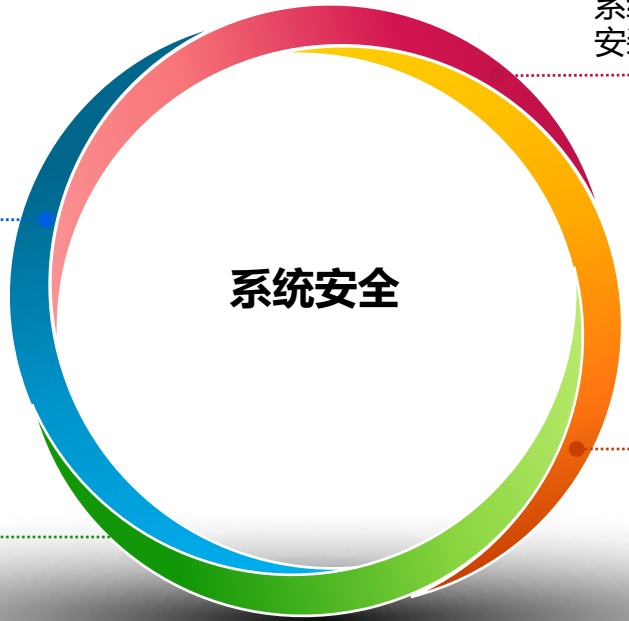
适合自己的安全体系

- 安全域划分：南北向最小化原则，东西向业务隔离
- 无线安全：内网用户域账户登录，外网用户二维码授权访问
- DOS：运营商+加速乐
- 入侵检测：自建告警机制

数据安全


数据资产管理
1. 完整的数据资产列表
2. 明确数据所属业务、数据类型、逻辑和物理位置、所有者、管理者信息
3. 定义信息等级和分类标准
数据访问
1. 用户分配
2. 访问控制
数据安全
1. 数据备份
2. 数据存储、加密

系统安全



操作系统安全

系统软件标准化
安装权限关闭

系统安全基线
账户、端口、服务巡检

数据库

数据库安全基线
开发规范
访问控制

桌面工作站、笔记本电脑安全

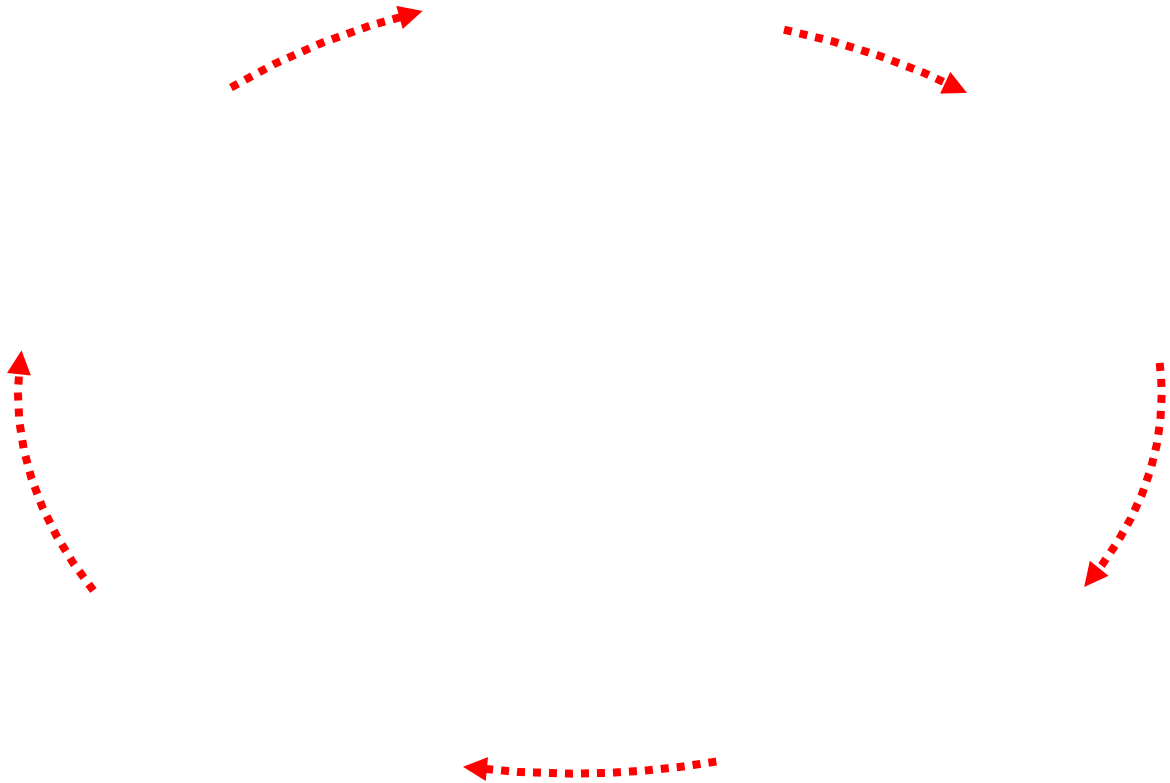
物理安全
账户密码安全

文件传输管控
文件系统安全

主机访问控制

管理员/root权限回收

物理安全

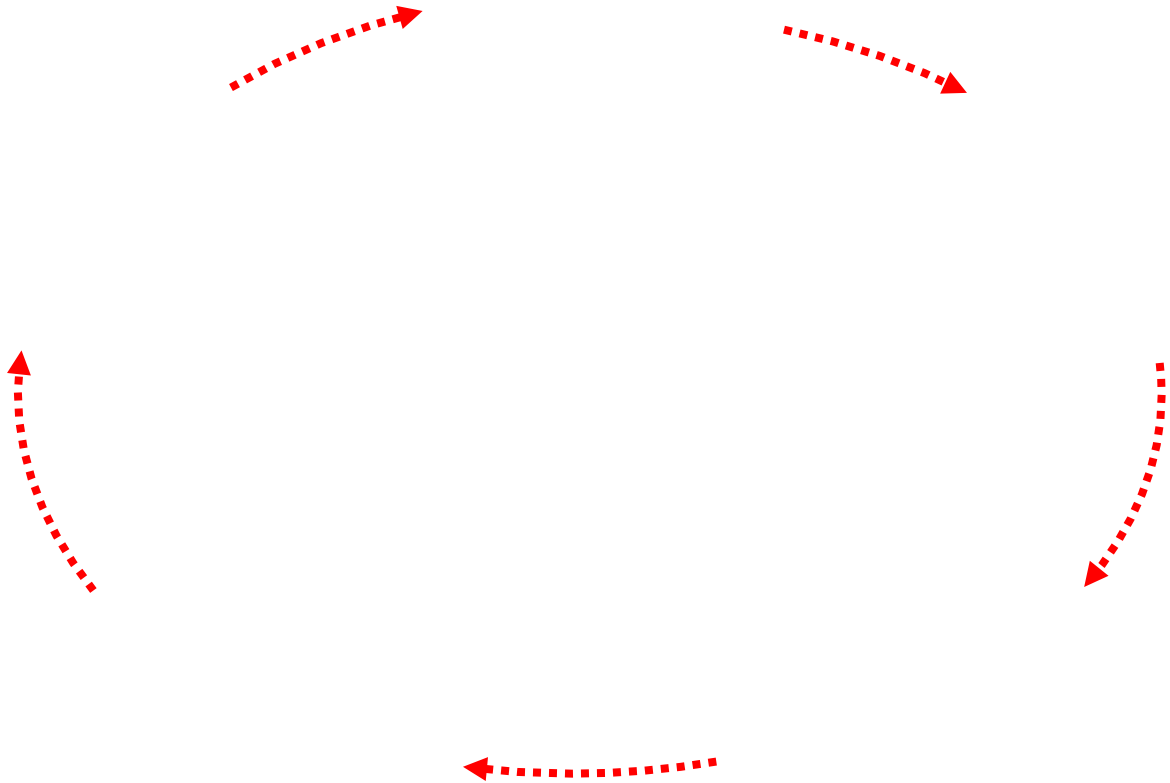


了解业务

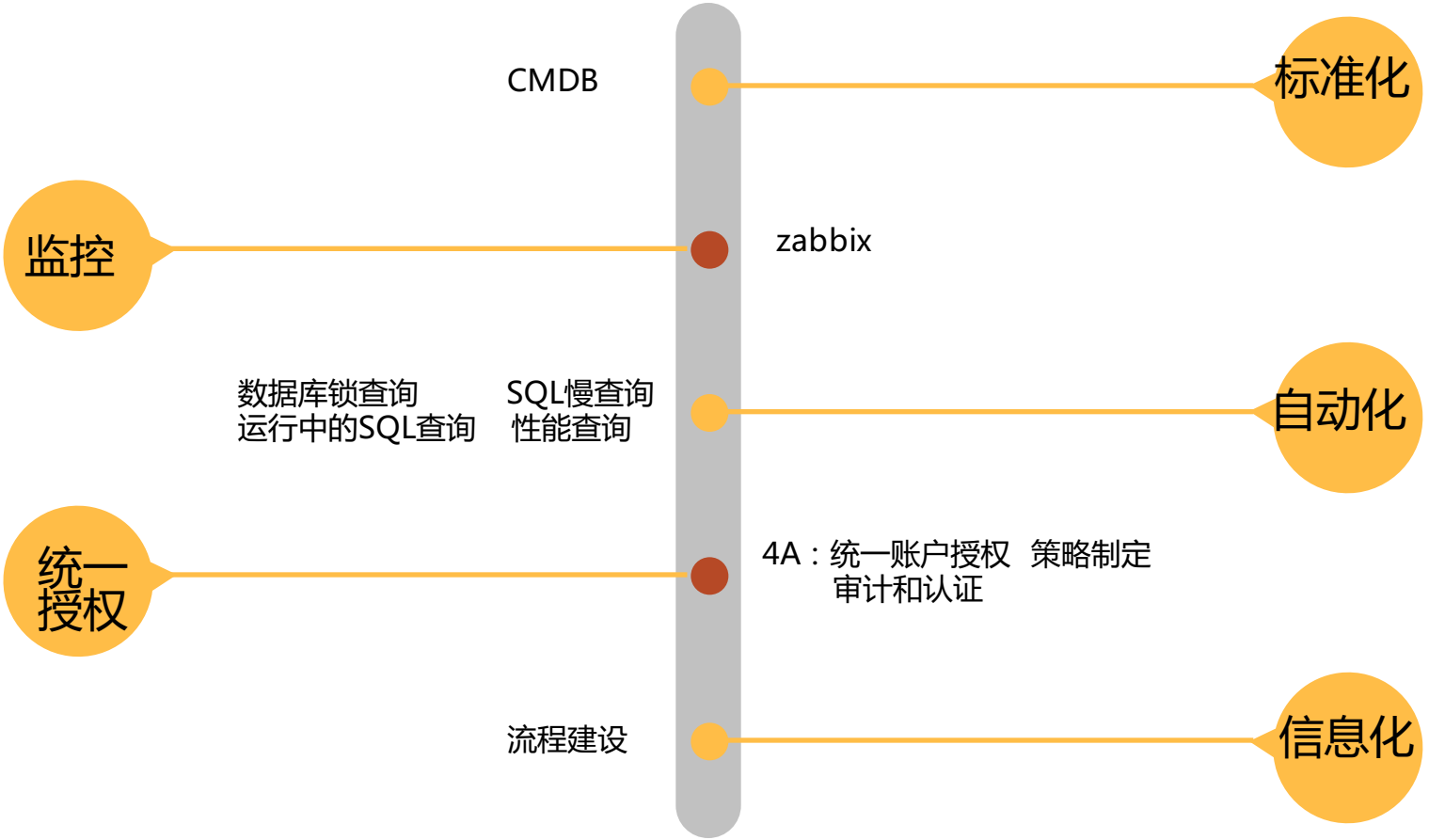
- 核心业务是什么？
- 保护对象是什么？
- 当前危机是什么？
- 如何保护？

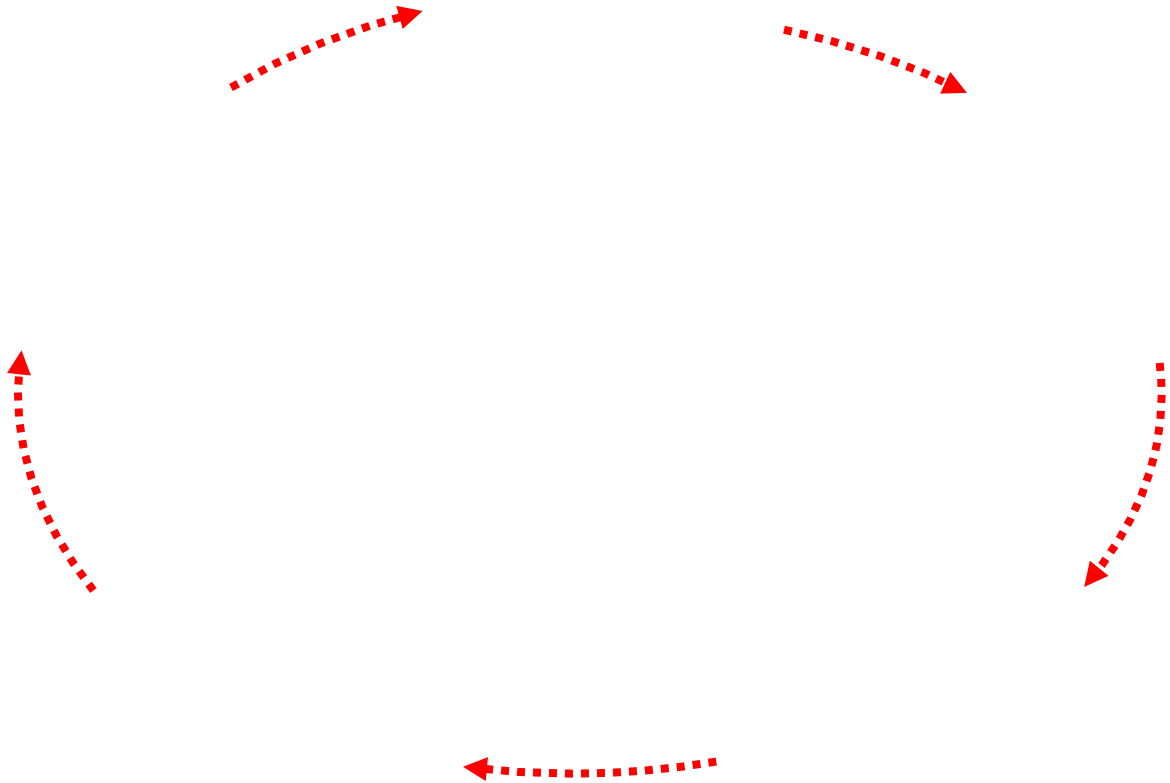
应用安全


应用
安全
安全
评估
核心业务PRD阶段安全评估
应用安全
风险
认证、授权访问、数据加密、
不可否认性、完整性
STRIDE威胁建模
日志和审计
恶意访问、攻击预警



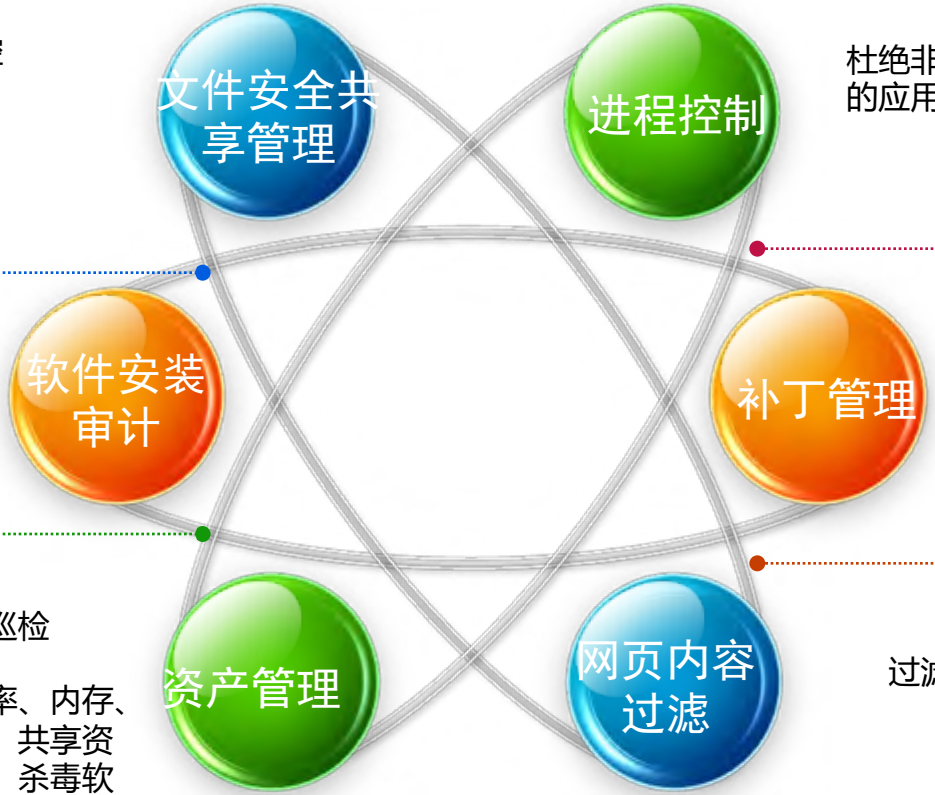
运维安全


CMDB
标准化
监控
zabbix
数据库锁查询
运行中的SQL查询
SQL慢查询
性能查询
自动化
统一授权
4A：统一账户授权 策略制定
审计和认证
流程建设
信息化



桌面安全

共享目录、文件监控
文件上传检测



杜绝非法软件，屏蔽无关工作的应用程序

软件标准化
未授权不能私自下载
安装软件需审批

缺失补丁定期检测，运维判断是否需要安装

资产登记、信息收集定期巡检

配置管理监控：CPU使用率、内存、磁盘空间、终端网络状况、共享资源、屏幕保护、系统时间、杀毒软件版本

过滤恶意网页、非法内容

终端安全

A 终端行为监控

- 软件监控
- 上网行为监控

B 资产配置管理

- 主机信息
- 网络参数

C 终端远程维护

- 及时发现远程终端硬件变更并告警

D I/O接口管理

- 允许和阻断对受控终端各种输出设备的访问

E 系统账户监控

- windows账户Guest账户检查
- 空密码、弱密码、无密码账户检查
- 密码策略设置检查
- 密码周期检测

防泄密

移动存储管理

介质初始化
注册授权
移动设备检查

传输管理

内网资料上传网盘行为检测

网络存储管理

github上传检测
公司资料禁止拷贝、对外传输

准入控制

终端、网络、应用、边界

谁能接入内网

哪些终端能够接入内网

终端要满足哪些条件才能接入内网

内网中不满足条件的终端如何修复

客户端、主机、应用

基于网络的准入--802.1x

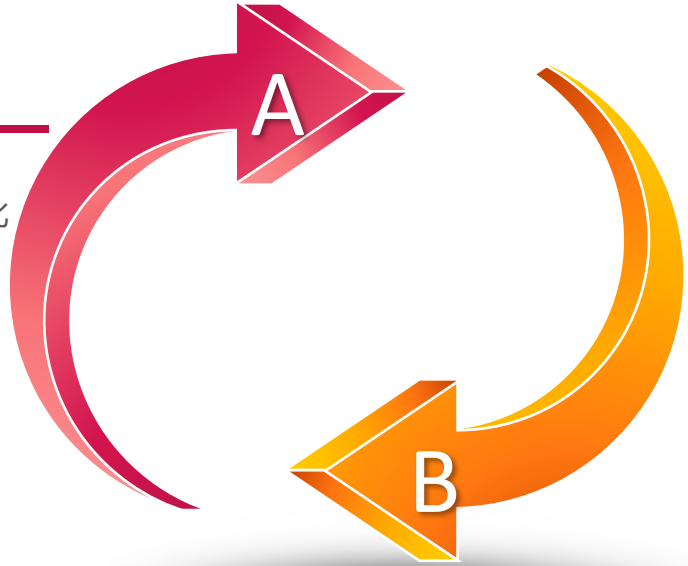
基于主机和应用--

DHCP\Web\Mail\web proxy\DNS

VPN安全

A 管理

VPN开通和申请必须经过审批
VPN日志定期分析



B 配置

VPN变更需走流程
VPN公网地址管理
闲置账户定期确认处理
会话超时设置，连接数<=1,异常登录
录IP限制登录
VPN接入需使用双因素认证方式

源码安全

Git统一管理，授权访问
编写或调整代码之前，相应设计文档保存至项目管理平台。代码提测之前先迁入Git
测试源码时需从Git获取，然后编译测试

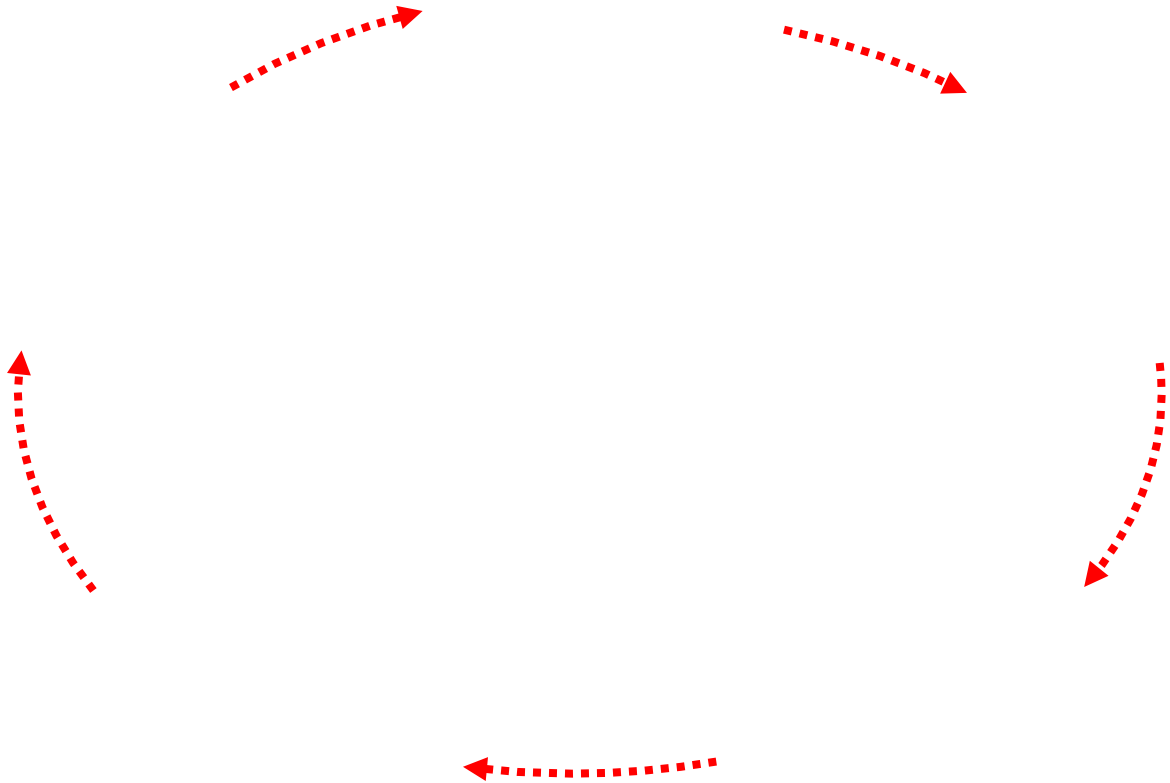
源码完整性检测

域账户登录Git服务器，源码访问需开发团队负责人授权
离职或调岗员工，需清除其源码及权限
涉及存储源码的服务器转作它用之前需由专员清除代码

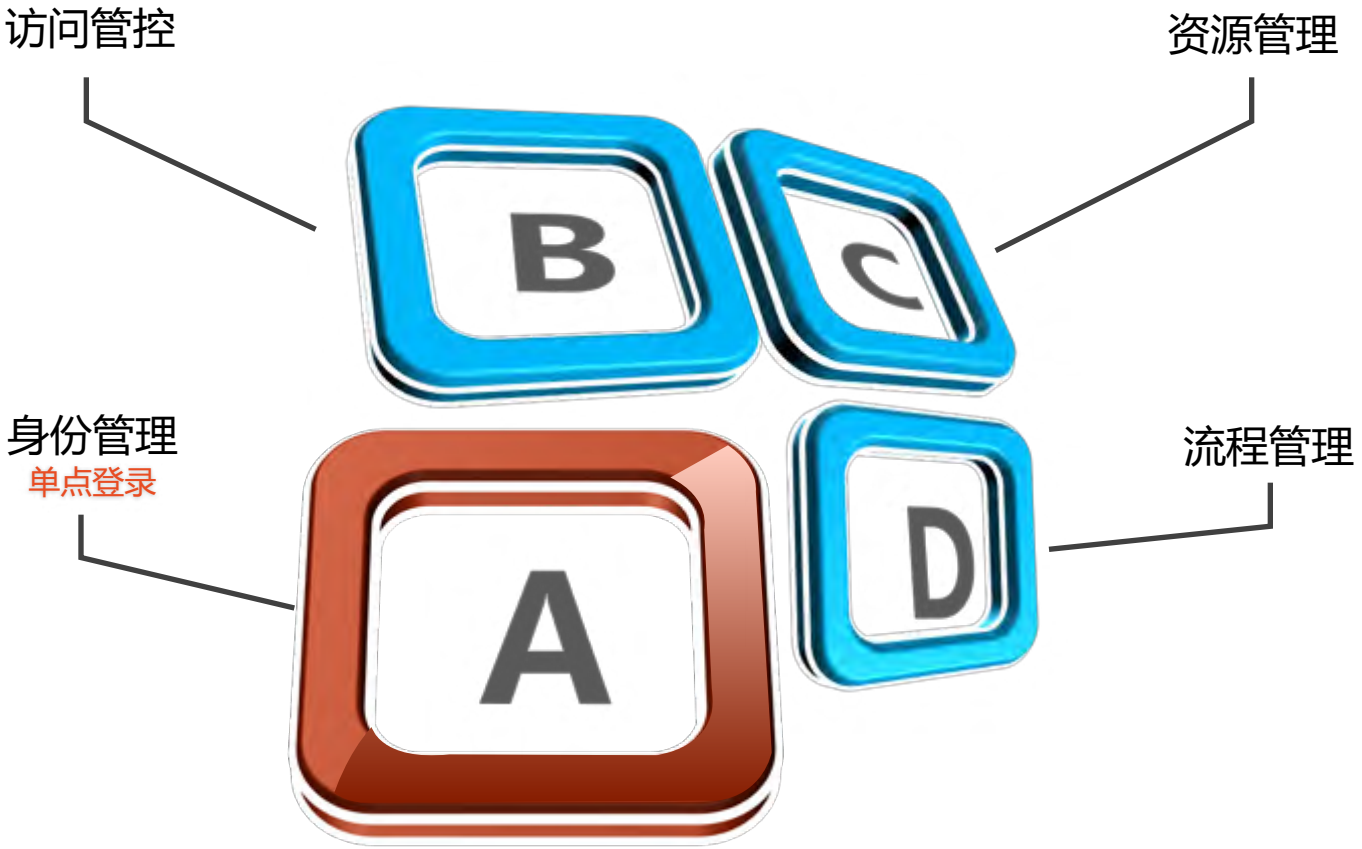
源码的授权访问

源码不得对外传输（网盘、Github、QQ、邮件等）
源码以任何介质存储备份的，需专员负责保管
因合作需向外传输源码的，需签订保密协议

禁止复制和传播



授权和访问控制



目录

资源分析

- 人力资源
- 阻力和助力

救火阶段

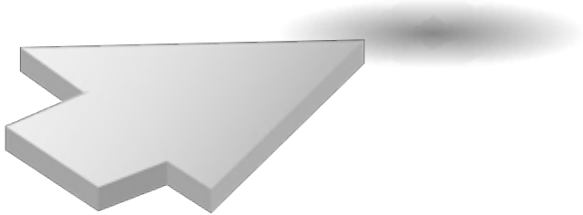
- 实时跟踪
- 主动出击
- 紧迫盯梢
- 及时曝光

日常运营阶段

- 明确责任人
- 定时跟踪
- 流程约束
- 松弛有度
- 奖惩制度

建设阶段

推广阶段&落地



平衡

业务

安全