前期自查工作要点

绿盟科技

CONTENTS

目 录

- 01 未知攻，焉知防
- 02 高壁深堑，步步为营

CONTENTS 目 录

- 01 未知攻，焉知防
- 02 高壁深堑，步步为营

01

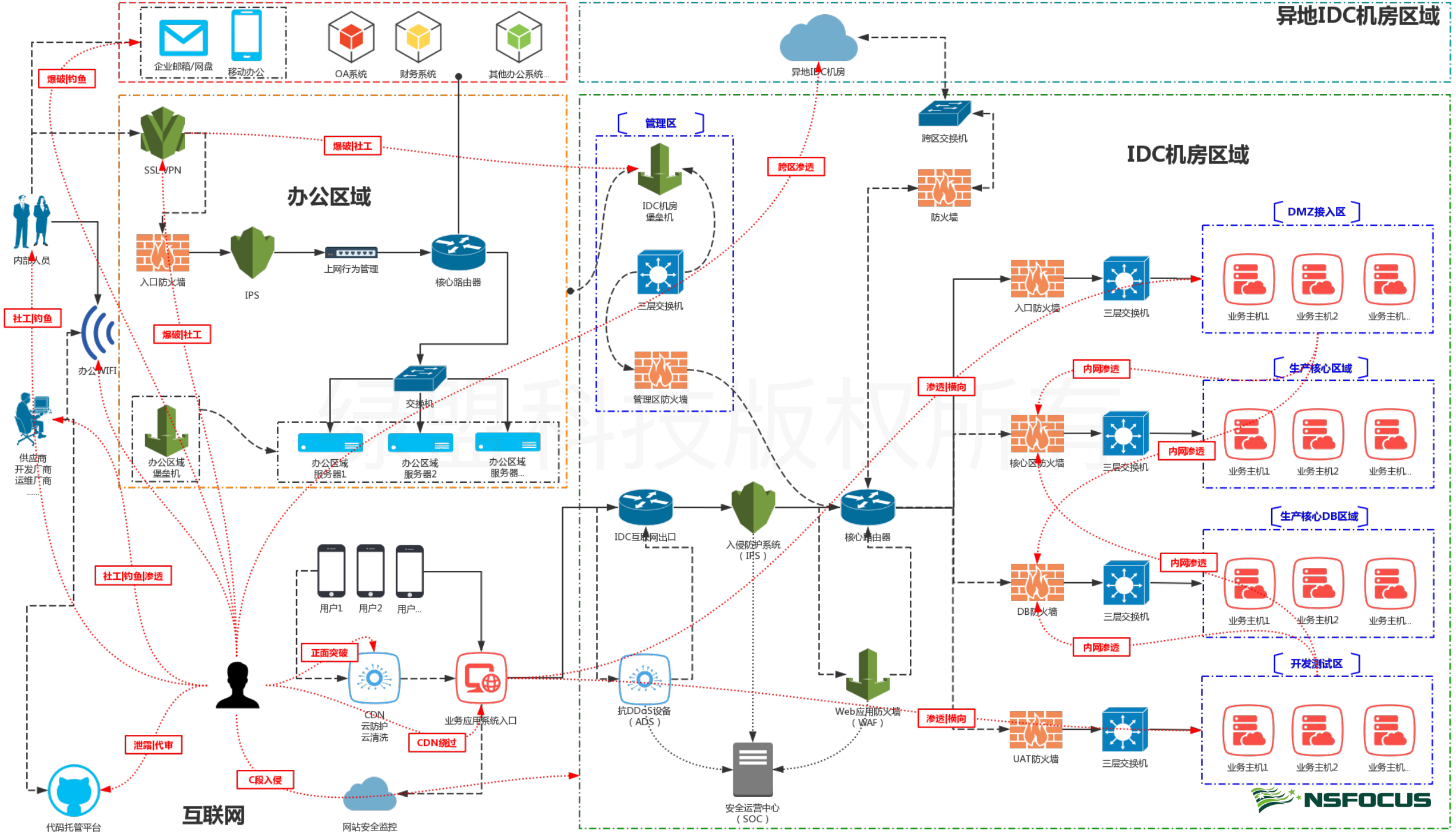
未知攻 焉知防

1. 护网常规入侵思路
2. 护网常用攻击手段

NSFOCUS

1.1

护网常规突破思路


异地IDC机房区域
企业邮箱/网盘
移动办公
OA系统
财务系统
其他办公系统...
异地IDC机房
爆破|钓鱼
办公区域
SSL VPN
爆破|社工
内部人员
入口防火墙
IPS
上网行为管理
核心路由器
社工|钓鱼
办公WIFI
爆破|社工
交换机
供应商
开发厂商
运维厂商
办公区域
堡垒机
办公区域
服务器1
办公区域
服务器2
办公区域
服务器...
管理区
IDC机房
堡垒机
三层交换机
管理区防火墙
跨区渗透
跨区交换机
防火墙
IDC机房区域
DMZ接入区
入口防火墙
三层交换机
业务主机1
业务主机2
业务主机...
生产核心区域
渗透|横向
内网渗透
核心区防火墙
三层交换机
业务主机1
业务主机2
业务主机...
生产核心DB区域
内网渗透
DB防火墙
三层交换机
业务主机1
业务主机2
业务主机...
开发测试区
内网渗透
渗透|横向
UAT防火墙
三层交换机
业务主机1
业务主机2
业务主机...
IDC互联网出口
入侵防护系统
（IPS）
核心路由器
社工|钓鱼|渗透
用户1
用户2
用户...
正面突破
CDN
云防护
云清洗
业务应用系统入口
CDN绕过
抗DDoS设备
（ADS）
Web应用防火墙
（WAF）
泄露|代审
C段入侵
互联网
代码托管平台
网站安全监控
安全运营中心
（SOC）
NSFOCUS

1.2

护网常用入侵手段

a. 护网常用外部突破手段
b. 护网常用内网渗透手段

护网常用外部突破手段

APP

社会工程学

弱口令

注入攻击

入侵痕迹

Wi-Fi

NdayRCE

上传 getshell

VPN

子域名

边角系统

数据库

废弃资产

护网常用内网渗透手段

翻文件

环境变量

口令复用

Bash_history

网络连接

跳板选择

.ssh

访问历史

部署代理

内网漏洞挖掘

后门部署

权限提升

Dumphash

主机发现

内网端口扫描

系统信息

文件上传

攻击域控

CONTENTS 目 录

- 01 未知攻，焉知防
- 02 高壁深堑，步步为营

02

高壁深堑 步步为营

1. 护网前期自查工作清单
2. 护网前期自查工作要点

NSFOCUS

2.1

护网前期自查工作清单

护网前期自查工作清单

- 减少护网被攻击面
- 主动发现安全风险
- 闭环潜伏安全隐患
- 了解自身安全现状
- 完善安全监控能力
- 提高安全防护能力

目的

2.2

护网前期自查工作要点

互联网暴露资产自查

01

信息收集

- 互联网IP地址
- 域名
- 技术架构
- 关键字
- 供应商

02

深度挖掘

- 端口服务
- 子域名
- 测试/开发/环境
- 源代码
- 供应商环境

03

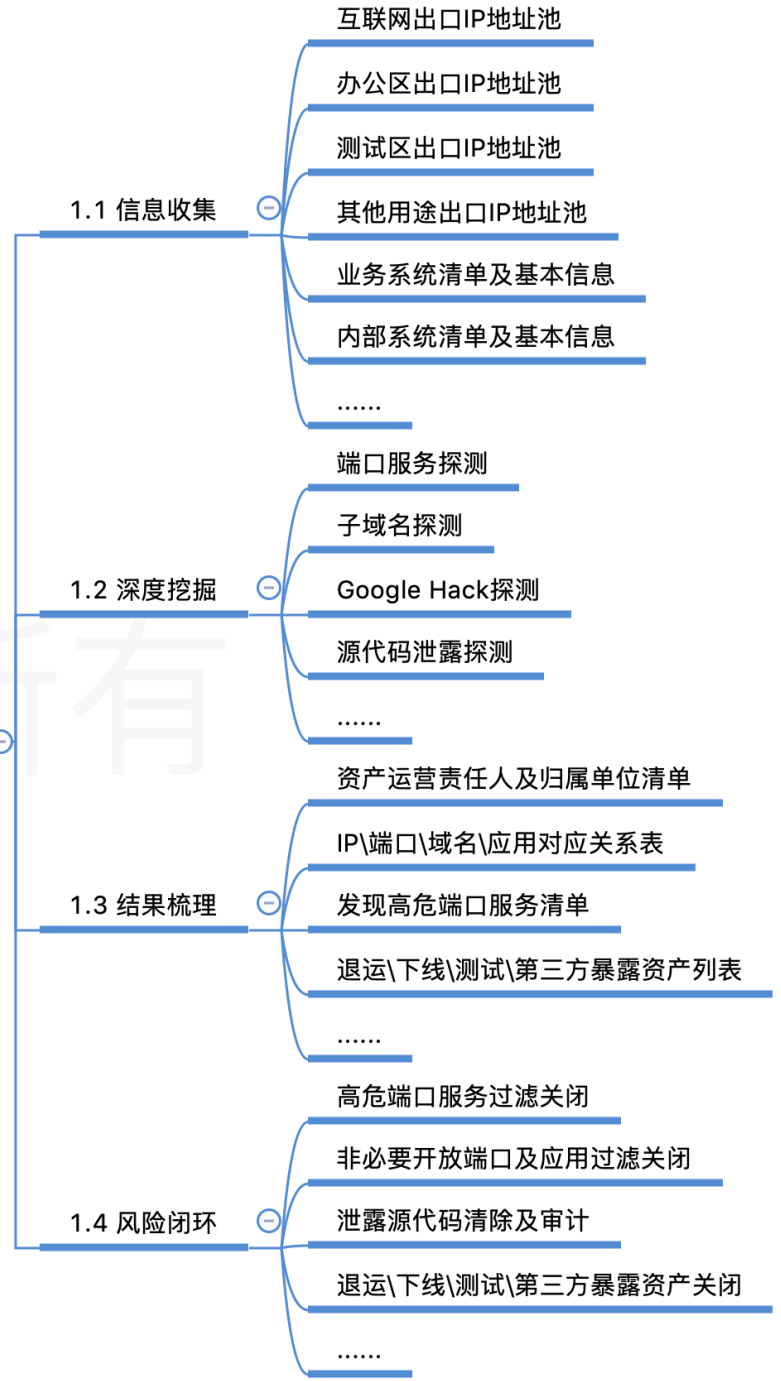
结果梳理

- 资产清单
- 映射关系
- 风险列表

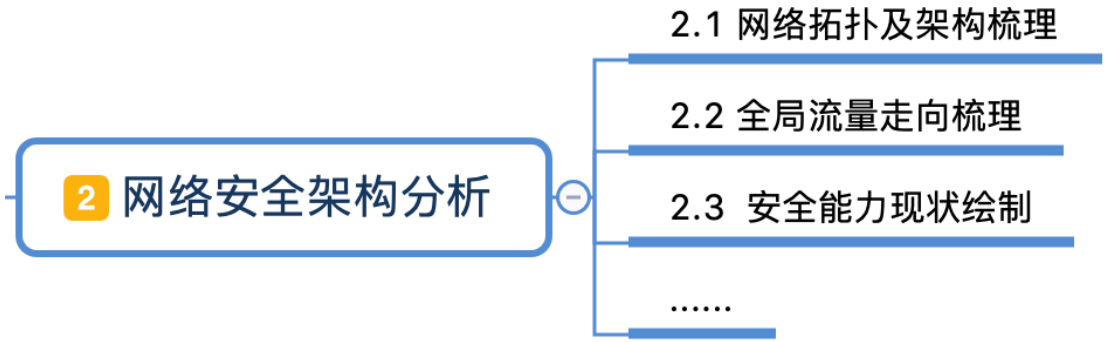
04

风险闭环

- 端口服务
- 测试/开发/退运/第三方
- 源代码
- 非必要应用



网络安全架构分析



- 办公网络拓扑
- 生产网络拓扑
- 跨区网络架构
- 互连网络架构

...

网络拓扑及架构梳理

- 业务流量
- 互联网流量
- 安全域间流量
- 跨区流量

...

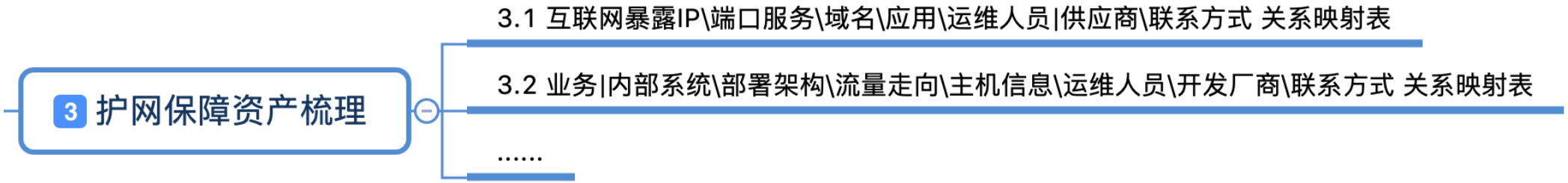
全局流量走向梳理

- 安全监测能力
- 安全防护能力
- 安全防护策略
- 安全保护机制

...

安全能力现状绘制

护网保障资产梳理



加快事件定位速度

在成立护网保障小组后，清晰的关系映射表可帮助安全监控人员快速定位受安全事件影响的资产。

减少应急响应时间

应急响应人员可根据清晰的关系映射表，建立应急沟通渠道，并协调相关人员快速处理安全事件。

提高安全监控效率

安全监控人员可根据清晰的关系映射表，把主要精力放在比较脆弱及较为容易入侵的途径，提高监控效率。

缩短事件上报流程

快速定位安全事件影响资产，减少应急响应时间，提高安全监控效率等均能加快事件上报的速度，可减少丢分，帮助得分。

全面基础安全自查

01

漏洞扫描

- 覆盖主机、设备、应用
- 使用多种工具复合
- 轮询多遍避免遗漏

02

配置核查

- 脚本进行基础检查
- 人工进行结果分析
- 关注实际效果而非合规

03

弱口令扫描

- 覆盖主机、应用、服务
- 口令组成规律
- 企业特征口令
- 常见弱口令

04

入侵痕迹排查

- 隐藏创建账号
- 未知网络连接
- 非法创建进程
- Weshell、僵木蠕

05

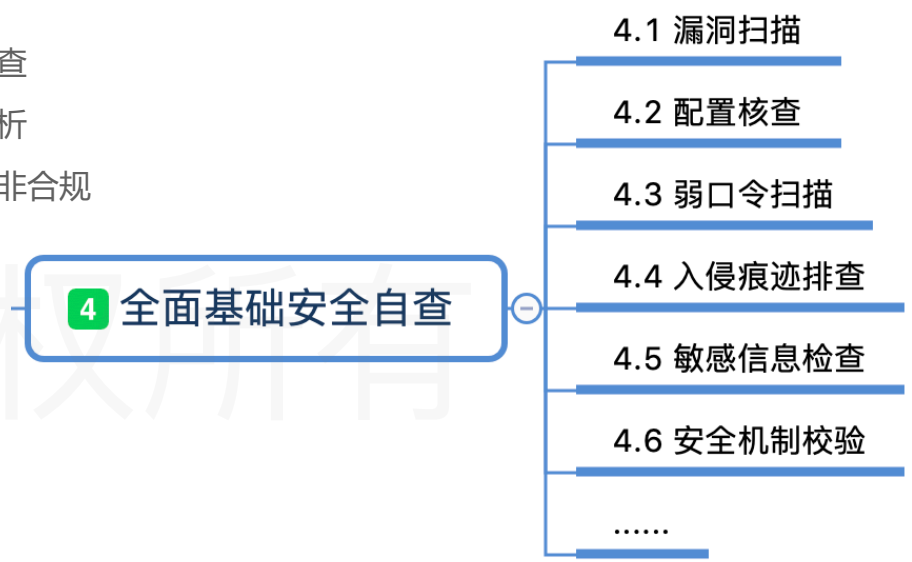
敏感信息检查

- 命令操作记录
- 关键备份文件
- 桌面敏感文件
- 开发过程文档

06

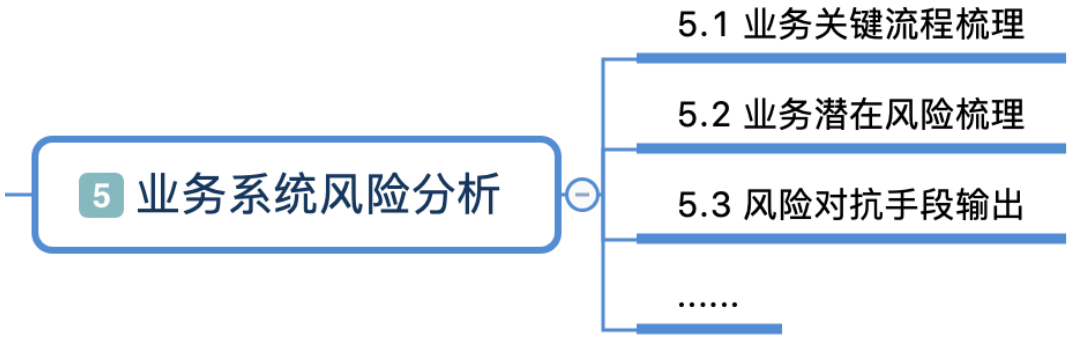
安全机制校验

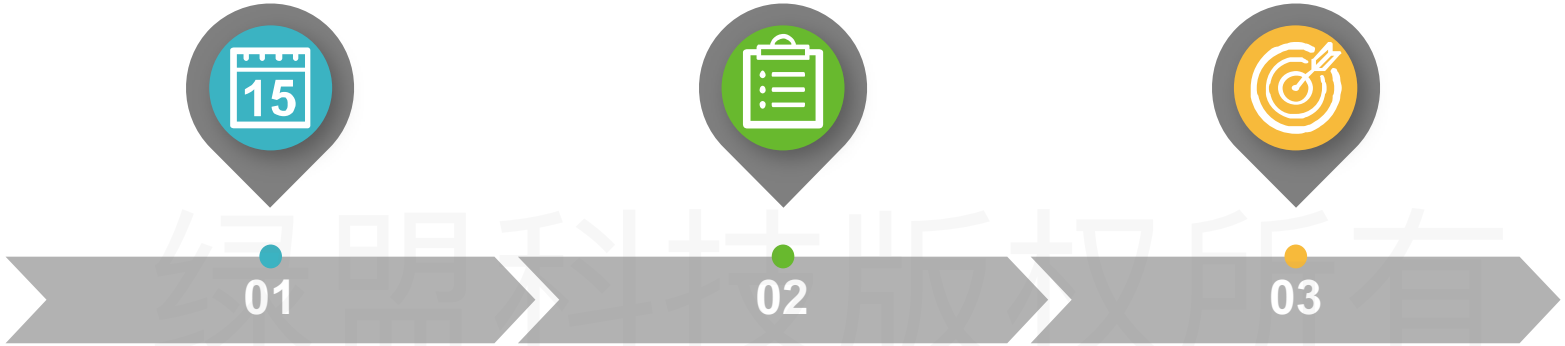
- 安全监控校验
- 安全防护校验
- 网络策略校验
- 安全策略校验



NSFOCUS

业务系统风险分析





业务关键流程梳理

主要梳理各系统关键流程，如登录、认证、查询、申请、审批、交易等，绘制相应时序图，为威胁分析及风险发现提供基础。

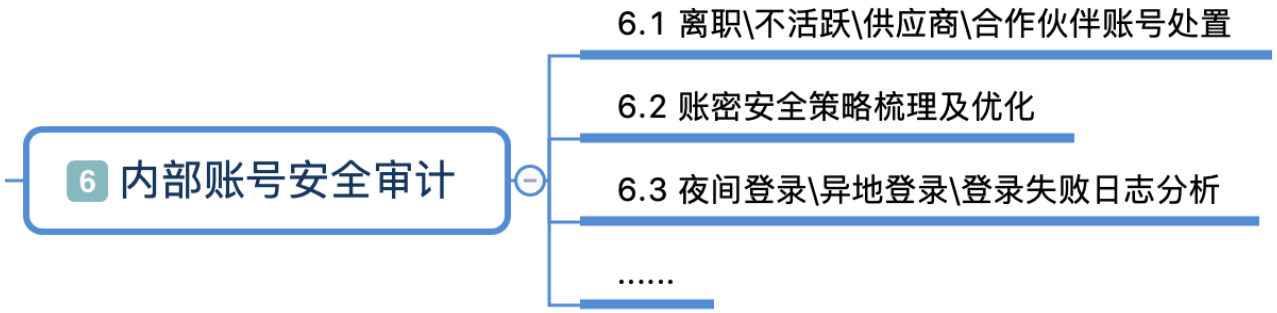
业务潜在风险梳理

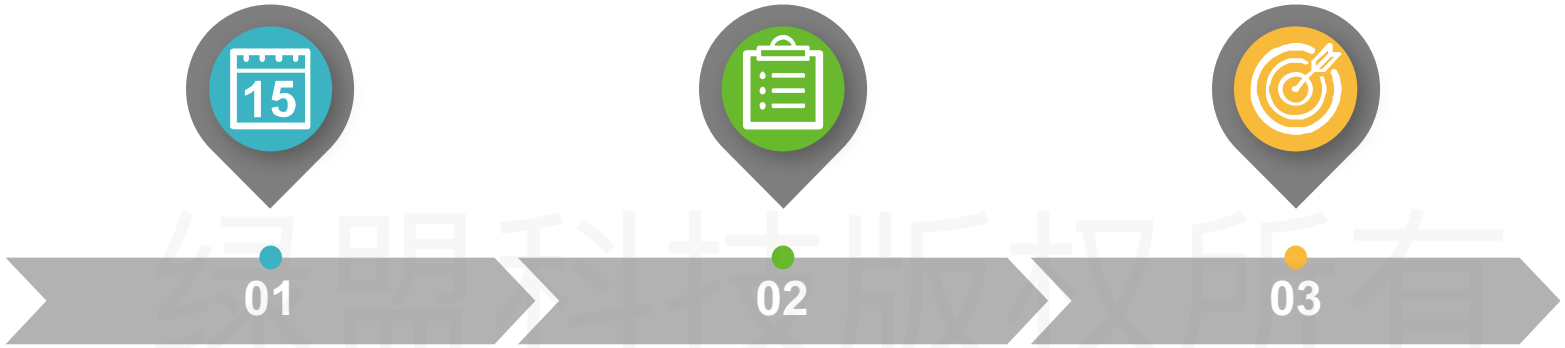
根据业务关键流程时序图，分析各关键业务流程中，可能会遭遇到哪些攻击，造成哪些危害。是否造成敏感信息泄露或严重安全风险，整理风险列表。

风险对抗手段输出

根据业务潜在风险列表，输出相应风险对抗手段，需要关注时效性，分为临时对抗手段以及长期对抗手段，保障系统安全。

内部账号安全审计





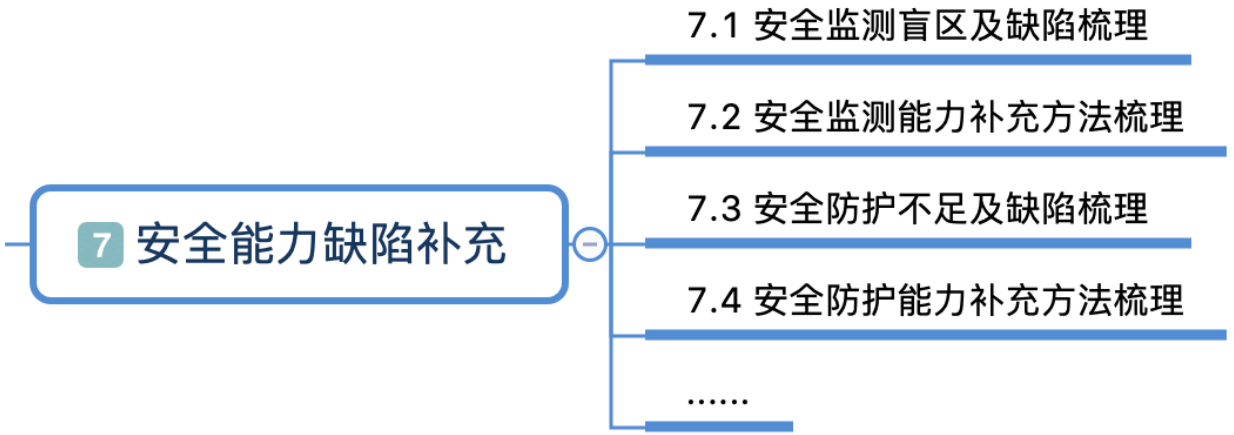
为避免在护网期间因为内部人员/供应商信息泄露或因历史遗留问题，造成账密泄露，需要对VPN、堡垒机、应用系统、设备及主机等现存账号进行梳理，将离职/不活跃/供应商/合作伙伴账号进行回收或密码重置。并且确保专人专用，执行权限最小化原则。

对VPN、堡垒机、应用系统、设备及主机等当前账密安全策略进行梳理，例如是否启用双因子认证、是否已设置防暴力破解机制、密码复杂度是否满足要求等，并且根据实际情况，提出临时解决方案和长期解决方案，进行优化。

对VPN、堡垒机、应用系统、设备及主机等账密相关日志进行审计，关注如凌晨登录、异地登录、登录频繁失败等异常登录行为，并且及时与账密所有者进行确认，处理相关事件。

NSFOCUS

安全能力缺陷补充



安全监测盲区及缺陷梳理

根据当前安全能力现状图以及护网常规突破思路，分析当前在护网期间安全监测能力存在哪些盲区，现有的安全监测手段存在哪些缺陷，如主机间横向攻击无法监测、安全域间攻击行为无法监测、网站监控仅监测可用性平稳度等。形成相关问题列表。

安全监测能力补充方法梳理

根据安全监测盲区及缺陷问题列表，按照企业实际情况进行分析，为满足时效性，提出临时解决方案和长期解决方案。临时解决方案如设备租赁、开源平台工具使用、厂商沟通等。长期解决方案如设备购买、平台自研、能力构建等。

安全防护能力不足及缺陷梳理

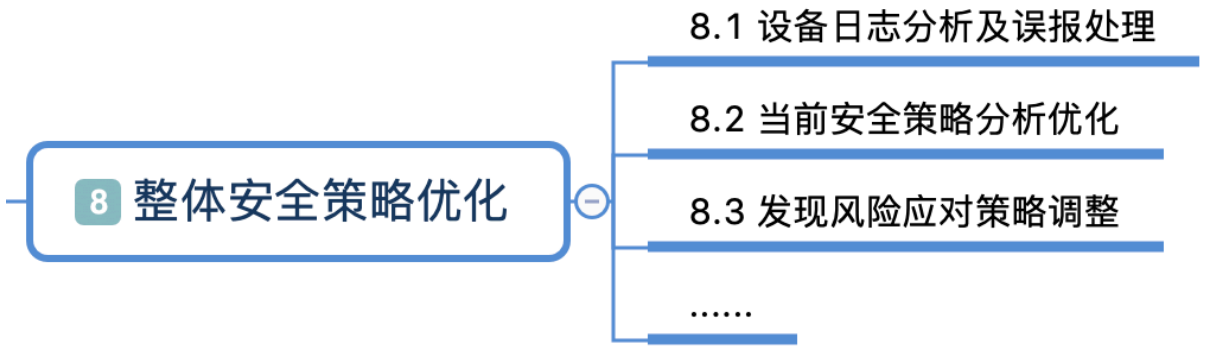
根据当前安全能力现状图以及护网常规突破思路，分析当前在护网期间安全防护能力存在哪些不足，现有的安全防护手段存在哪些缺陷，如缺乏主机安全防护、缺乏Web攻击防护、入侵防护系统仅支持暴力破解及扫描防护等。形成相关问题列表。

安全防护能力补充方法梳理

根据安全防护盲区及缺陷问题列表，按照企业实际情况进行分析，为满足时效性，提出临时解决方案和长期解决方案。临时解决方案如设备租赁、开源平台工具使用、厂商沟通等。长期解决方案如设备购买、平台自研、能力构建等。

NSFOCUS

整体安全策略优化



设备日志分析及误报处理

针对各类设备安全日志进行分析，如VPN、堡垒机、防火墙、WAF、IPS、安全沙盒等。各类设备应关注重点事件，如VPN关注异常登录、堡垒机关注异常操作、防火墙关注异常连接、WAF|IPS关注攻击允许行为及误报事件等，因业务系统差异性，各类安全设备存在不同情况的误拦误报，需要将发现的风险和误拦误报及时进行处理。

当前安全策略分析优化

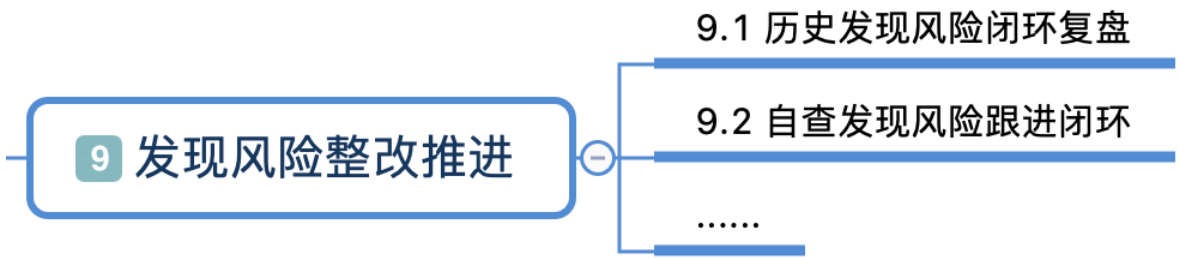
根据日志分析及误报处理的结果，对网络设备策略、安全设备策略、主机策略等进行调整和优化。如安全设备针对业务系统技术架构，自定义拦截规则，开启相应监测和防护；网络设备开启白名单机制、防护机制等。

发现风险应对策略调整

综合之前发现的如高危端口暴露、存在高危漏洞、账密无双因子认证、攻击未有效拦截等各类风险，需要相应针对已发现的风险进行策略调整，降低风险发生概率。

NSFOCUS

发现风险整改推进



历史发现风险闭环复盘

对以往发现的安全风险进行梳理，尚未解决的高中风险需要快速进行闭环，针对历史上发生的重要安全事件需要进行复盘，总结教训，提升意识，并确认已无潜在风险。

自查发现风险跟进闭环

对整体前期自查工作中发现的风险及问题进行汇总整合，并且形成相应的跟踪表，设立每项风险闭环的责任主体和负责人，并根据实际情况，选择合适的手段，规定整改deadline。及时跟进，直至各项风险闭环。

FAQ

谢谢！

NSFOCUS