小团队如何通过安全运营在蓝军的炮火中生存

郭威

深圳证券交易所　信息安全主管

关于我

1 从业经历

过去六年，在深交所从事信息安全工作

2 听过很多会

乌云2015白帽子大会
RSA/ISC/FIT/强网论坛/金融业网络安全论坛

3 也打过CTF

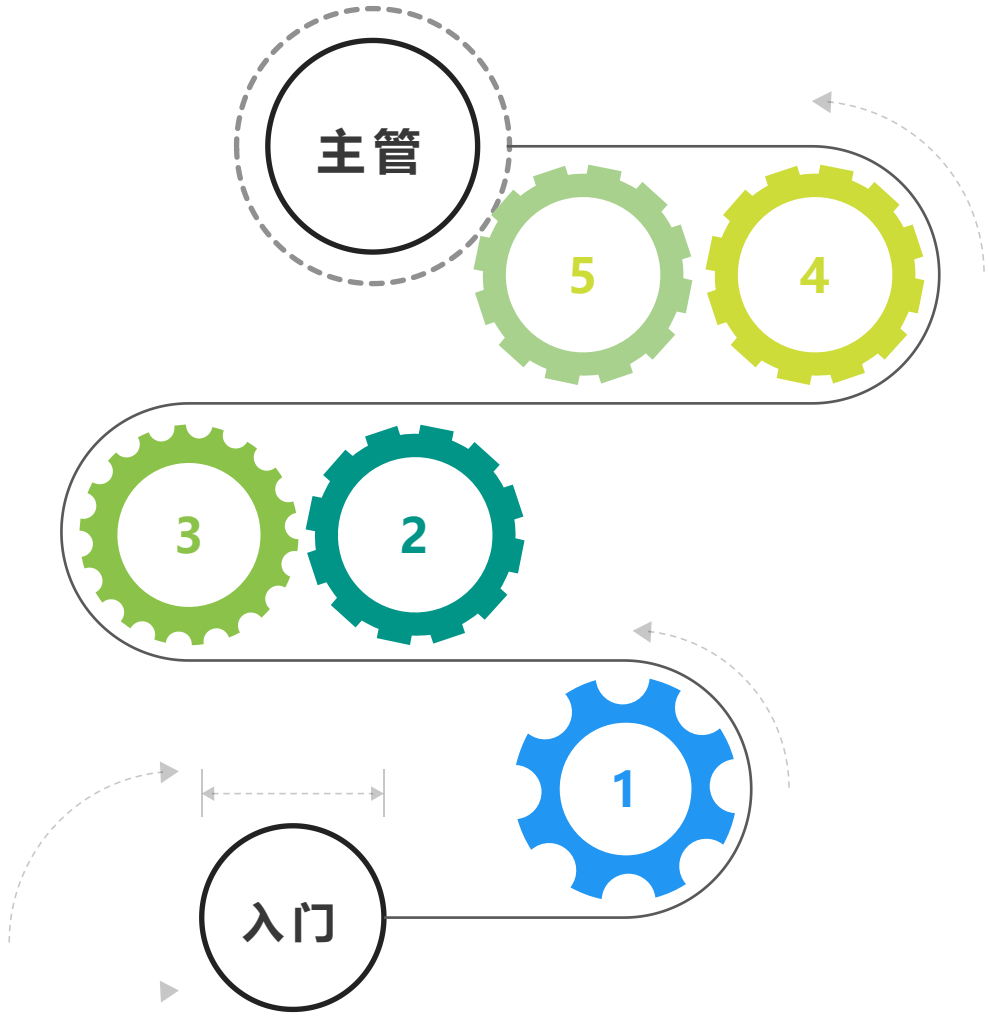
网鼎杯/中央企业网络安全技术大赛

4 读了一些书

《互联网企业安全高级指南》/《企业安全建设指南》
《0day：软件漏洞分析技术》/<hack like a legend>

5 看过众多产品

覆盖传统安全/数据安全/SOAR/态势感知



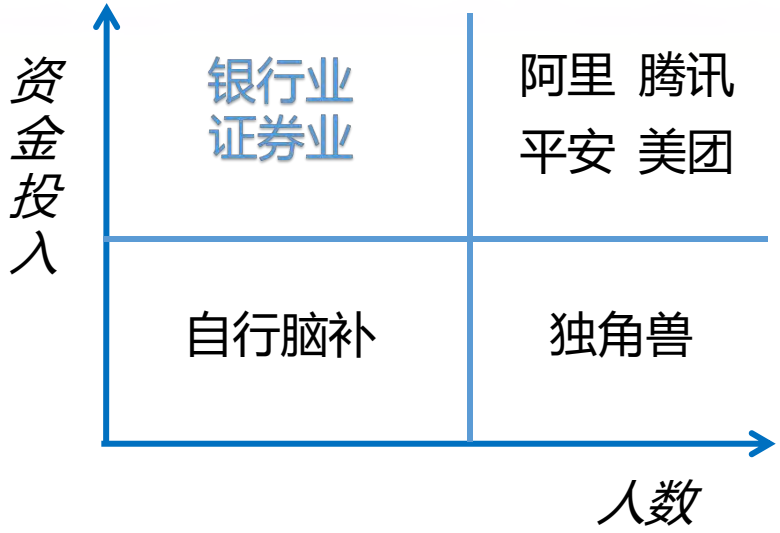
目录

01 序

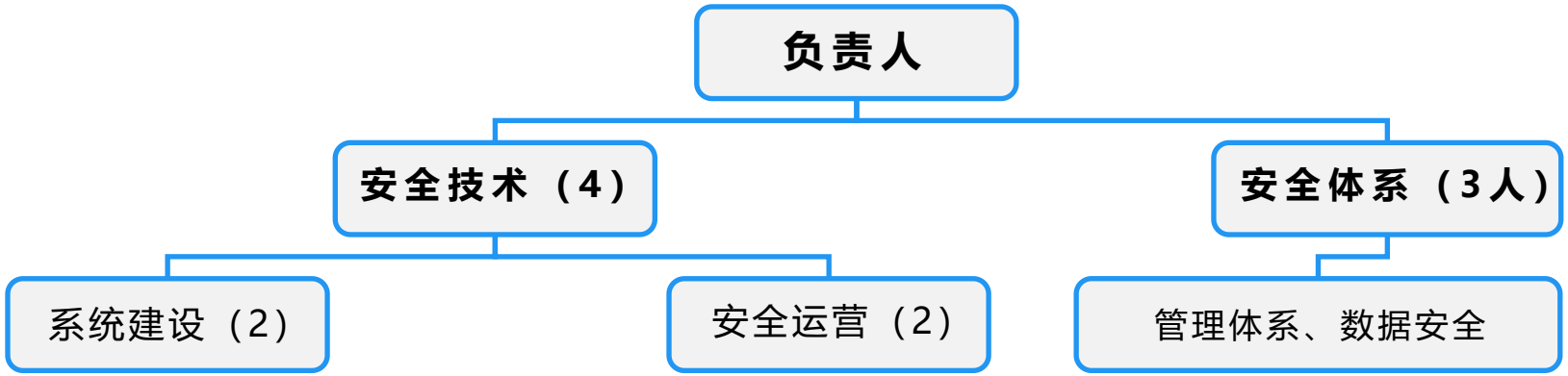
背景介绍

KEY1：何谓“小团队”？

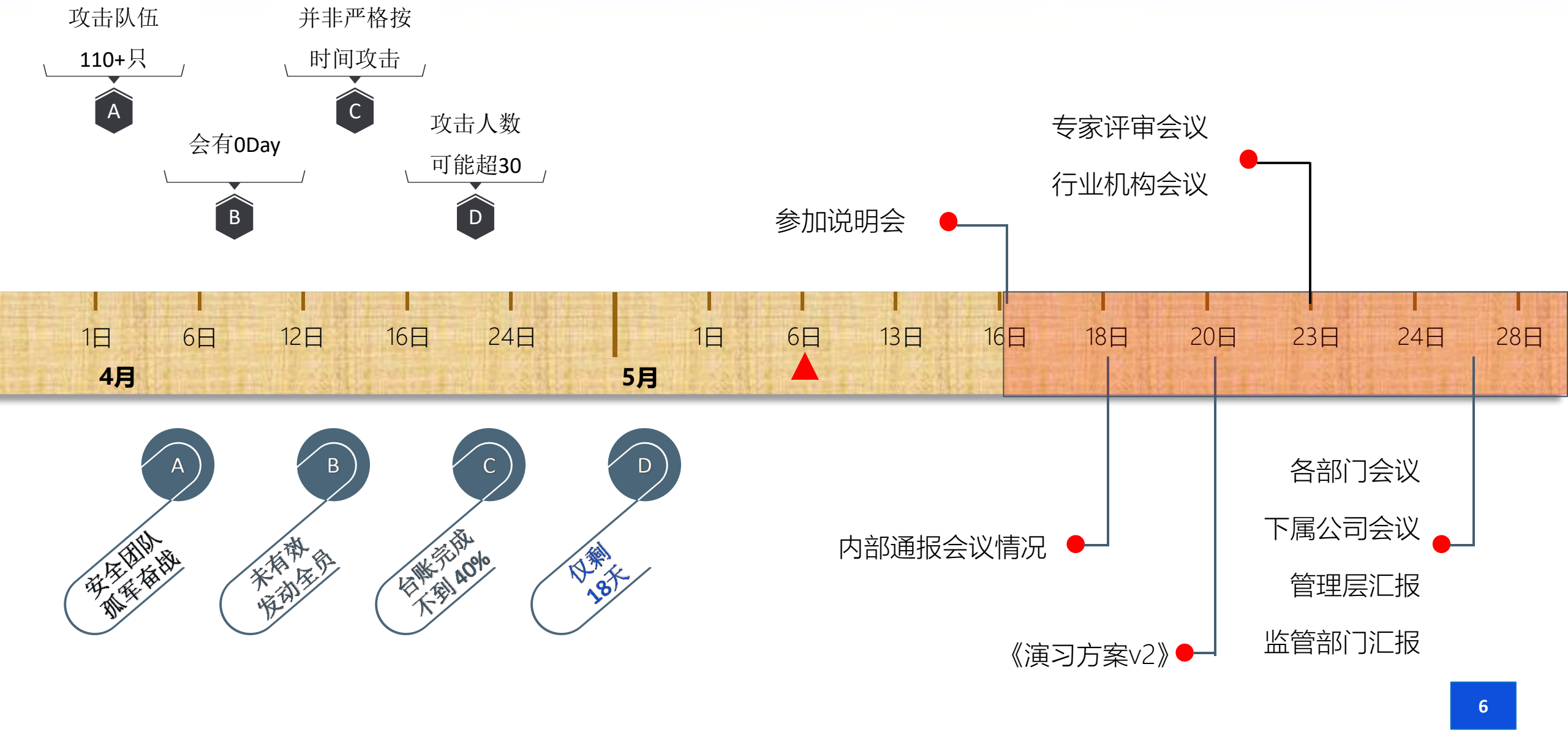
- 绝对人数少
- 工作范围广
- 团队独立



- 成员8人（<1%）
- 负责全公司安全管理制度落地、网络安全防护
- 安全小组独立于运行部门



KEY2：“蓝军”是谁？


攻击队伍
110+只
A
并非严格按
时间攻击
C
会有0Day
B
攻击人数
可能超30
D
专家评审会议
行业机构会议
参加说明会
1日
6日
12日
16日
24日
4月
1日
6日
13日
16日
18日
20日
23日
24日
28日
5月
A
安全团队
孤军奋战
B
未有效
发动全员
C
台账完成
不到40%
D
仅剩
18天
内部通报会议情况
《演习方案v2》
各部门会议
下属公司会议
管理层汇报
监管部门汇报

KEY3：“炮火”打哪儿来？

WEB漏洞

网站是不是存在SQL注入？
专区会不会存在LFI？
硬件证书系统是不是有漏洞？

网络漏洞

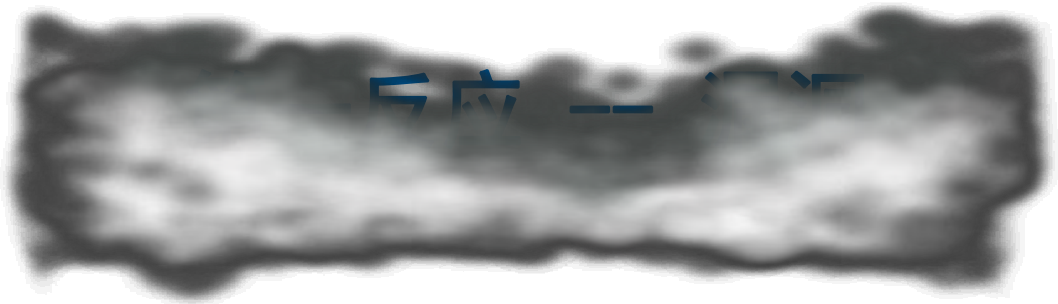
是否有服务器偷偷开放了DB服务？
网络权限是否控制了非80和443端口访问？
互联网资产是否有遗漏？

社工

员工是否会被钓鱼？
领导的弱口令改了没有？
会不会被物理入侵？

信任底线

如果防火墙被绕过了怎么办？
如果出现了0Day长驱直入到内网怎么办？
供应商会不会泄露网络拓扑？



工作台账V1.0

安全组工作台账V1.0

资产排查	DMZ、开发测试、托管、下属公司
风险排查	已知漏洞复核、互联网资产安全检测、基线核查、用户弱口令、LED、弱口令
防护与监测	VPN加固、AD、PoC系统、主机安全、邮箱、蜜罐
专区防护	WEB扫描、渗透测试、部署WAF、日志监控、用户钓鱼测试、老专区防护
重要设备防护	代理服务器、文件交换系统、网盘、堡垒机、防病毒

工作台账V1.0 存在的问题

安全组工作台账V1.0

- 资产排查
- 风险排查
- 防护与监测
- 专区防护
- 重要设备防护

本质

风险驱动

典型特点

自下而上

自上而下的视角

内部员工

密码泄露
钓鱼邮件
操作指引

外部人员

合作数据
账号共享
权限残留

异地中心

物理入侵
终端管控
网络准入

下属公司

物联网
LED 大屏
后勤人员

很多问题看起来是技术问题，其实是管理问题

-- 群众

02 点

管理类工作

- 压实主体责任
- 健全组织领导
- 完善应急处置流程

压实主体责任

所内管控

领导层
员工
系统管理员
异地中心

- 管理层汇报、监管层汇报
- 安全员专题会议《关于重申信息安全工作纪律有关事项的通知》
- 《加强网络安全防护自查表》
- 钓鱼邮件培训
- 《工作人员信息安全工作指引》

监督下属公司

多个下属公司

- 召开专题会议，通报演练工作。
- 要求下属公司形成工作台帐，提交总部进行评审。

协调外部单位

关联单位
服务商

- 关联单位：核心机构、经营机构。
- 供应商《责任书》：
  - 不存在未修复的已知漏洞
  - 未泄漏与深交所合作期间获取的敏感数据

健全组织领导

建立组织架构

成立攻防演练指挥部（扩大到业务部门、下属公司、关联机构）
成立演练工作小组（囊括运行、开发、安全等部门）

制定应对方案

1、制定演习方案。
2、制定演习工作台帐。

明确职责分工

制作职责说明书

完善应急处置流程

01 事件分类

参照《信息安全事件分类分级指南》

- 网络扫描窃听事件
- 后门攻击事件（木马事件）
- 漏洞攻击事件
- 拒绝服务攻击事件
- 网络钓鱼事件

02 职责分工

三组联动

- 分析组：监控设备告警、分析告警的影响、全网排查
- 处置组：决策、资产定位、应急响应、工具准备
- 消息组：下达、上传、事件闭环、汇总
- 值班表

03 明确流程

PDCERT模型

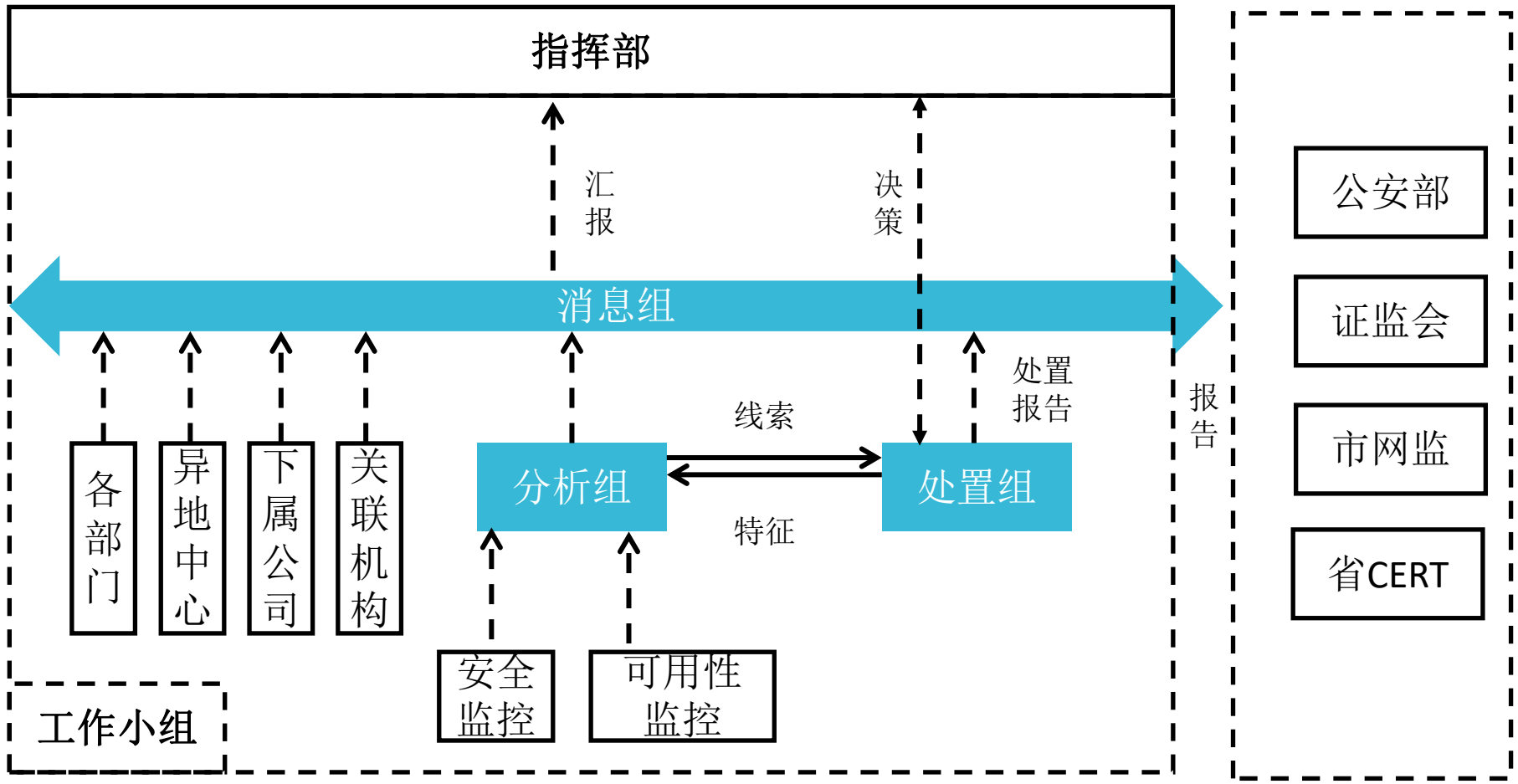
- 6个阶段：准备、诊断、抑制、根除、恢复、跟踪
- 明确各类安全事件中三个组的工作内容
- 常见抑制措施：网络隔离、关机、修改DNS、黑名单

04 规范手段

沟通和汇报

- 违反**保密规定**，无意泄露信息
- 内外沟通渠道分离
- 日报、周报
- 每日复盘会议
- 工作总结

完善应急处置机制（人员分工）



1. 消息组：5人
2. 分析组：14人
   （其中监控9人）
3. 处置组：N

应急处置举例

环节	说明
P 准备	1、 部署反垃圾邮件网关。 2、 进行邮箱日志采集。 3、 部署邮件防 APT 设备。
D 诊断	1、 员工反馈给 3000 或安全组，安全组进行分析。 2、 邮箱管理员对拦截邮件，尤其是触发敏感关键词的进行分析，筛选出可疑邮件。 3、 安全组根据可疑邮件标题进行影响范围分析。
C 抑制	1、 根据诊断分析结果，通知所有收件人进行防范。 2、 对于已经点击的用户，进行断网处理。 3、 将发件人放入黑名单。
E 根除	运行了恶意程序，进行安全处理。 点击链接泄漏了敏感信息，要求立即更改相关信息。
R 恢复	N/A
F 跟踪	对发件人的所有邮件进行分析。

员　工　向消息组反馈收到钓鱼邮件

消息组　在漏洞管理系统录入信息
并向分析组人员派发工单

分析组
1、查看邮件沙箱告警，无告警
2、人工分析链接和内容，关联情报数据
3、影响分析：利用SIEM完成

处置组　根据分析结果，进行封禁
通知其他受影响用户进行处置

应急处置举例（图）

index=exchange “恶意邮件关键词”
| table message_subject, recipient_address, OriginalFromAddress, sender_address

疑虑和驱动力

参会代表：演习工作是我们今年的政治任务之一

疑虑

① 生产环境主机要装Agent？出现可用性问题怎么办？

② 这段网络流量难弄啊，要新增设备、跳线，好麻烦。

③ 对测试环境安全要求降一降，弱口令、不打补丁应该接受？

④ VPN一定要短信验证码吗？图形验证码行不行？

解药

① 生产环境主机安全agent全覆盖。

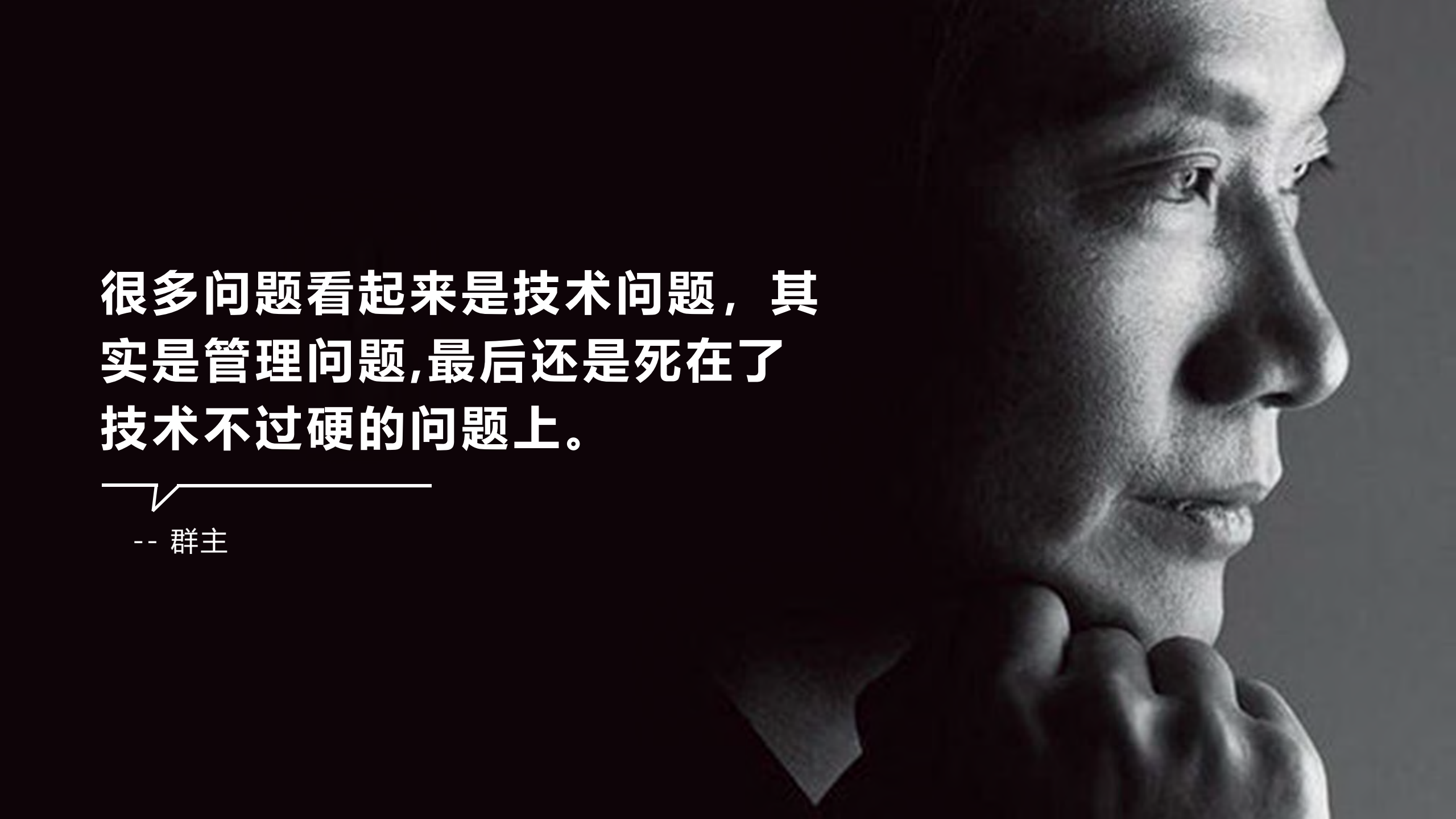
② 流量尽可能抓全。

③ 测试环境在往年都是被攻击的入口。

④ 图形验证码早已被证明很容易绕过。

驱动力：合规驱动　风险驱动　党性驱动

召开评审会议：公安、电力、银行、攻击方代表


很多问题看起来是技术问题，其实是管理问题,最后还是死在了技术不过硬的问题上。
-- 群主

03 点

技术类工作

- 攻击面分析
- 纵深防御
- 基础工作

技术思路

总体思路

攻击面分析

从边界到内部
站在攻击者的角度，枚举所有可能的攻击路径

筑牢基础

定调：被攻陷是肯定的，但不能犯低级错误
如补丁、防病毒、弱口令、误配置

纵深防护

时间有限、人力有限、设备有限
从重点抓起，再扩散到普通系统

1、攻击面分析

分类	范围	风险项	应对安全措施
边界	DMZ-专区应用	基于硬件证书的身份验证机制出现问题，导致登录被绕过	接受。通过提升预警能力来弥补。
		攻击者盗用合法用户身份，如部分非证书站点存在用户弱口令、用户电脑被攻击者控制。	1、获取用户名清单，安全组提前进行TOP7000弱口令检测，对发现弱口令的责令修改。[07] 2、修改专区登录页面验证码机制，改为每次都需要输入验证码。[33]
		应用自身存在漏洞，被利用后获取应用或者主机权限，进入隔离层。	对专区进行带证书的WEB扫描。[31]
	DMZ-远程办公	VPN用户存在弱口令或口令被暴力破解，攻击者成功进入隔离层。	登录双因素，加入短信验证码[12-3]
	物业网	物业设备（视频监控、考勤、门禁等）网络被攻击者在现场控制	接受。物理安保已经比较严格。
	终端接入子区	攻击者到物理场所绕过准入，如直接使用打印机网线	接受。物理安保已经比较严格。
	流量出口	分析预警能力不足：目前仅部署了防火墙，无法记录原始流量，无法对上行数据包内容做安全分析。	正在部署NDR类产品[14-1]

[N]：代表安全小组单独的台账编号

1、攻击面分析（续）

分类	范围	风险项	应对安全措施
内部	隔离层桌面云	控制员工的VDI，进而对公共服务器发起攻击，如域控、内部邮箱、安全助手、OA等。	VDI与服务器网段有防火墙隔离，有ACL策略。
	隔离层子区	服务器存在高危漏洞，如弱口令、未更新严重漏洞补丁	1、开展服务器基线核查，确保密码策略有效实施。[03-1] 2、5月底前开展一轮内部扫描，确保已知的RCE漏洞全部修复。[01-5]
		内部服务器密码复用（非弱口令），出现“一处失陷，多处失陷”的情况。	接受。需要运行部研究解决方案。
		网络设备ACL规则粒度过粗，或存在误配置，导致出现不应该允许的网络通道。	网络组检查跨层防火墙策略，尤其是any类型的规则，确认是否合理。[03-5]
		管理员在服务器或终端上明文存放敏感文件，如网络拓扑、账号密码等信息。	发通知要求所有服务器管理员自查，禁止在邮箱、文件目录存防明文密码，相关邮件删除，相关文件考虑用excel加密保护。[91]
		域管理员在非常用终端输入账号密码信息，导致凭证泄漏。	要求域管理员禁止在非本人终端、服务器输入域密码。对于先前输入过的服务器，做重启处理。[90]
		服务器防病毒未统一管控，攻击者可以退出防病毒软件之后再安装恶意软件。	将服务器防病毒的本地管理员权限收回，统一管控。[54]
		服务器间跳转，攻击者在内网横向移动。	1、服务器被划分为多个VLAN，通过ACL进行控制。 2、服务器登录绕行会产生监控告警。 3、主机上的爆破、扫描等行为会产生监控告警。

2、筑牢基础

补丁

期间：10个0Day、月度补丁
分布式漏扫工具：RCE全部修复，否则关机处理（含测试环境）
漏洞修复：快速推动。Redis升级、IIS升级、OS升级

防病毒

windows：覆盖率
linux：EDR进行扫描

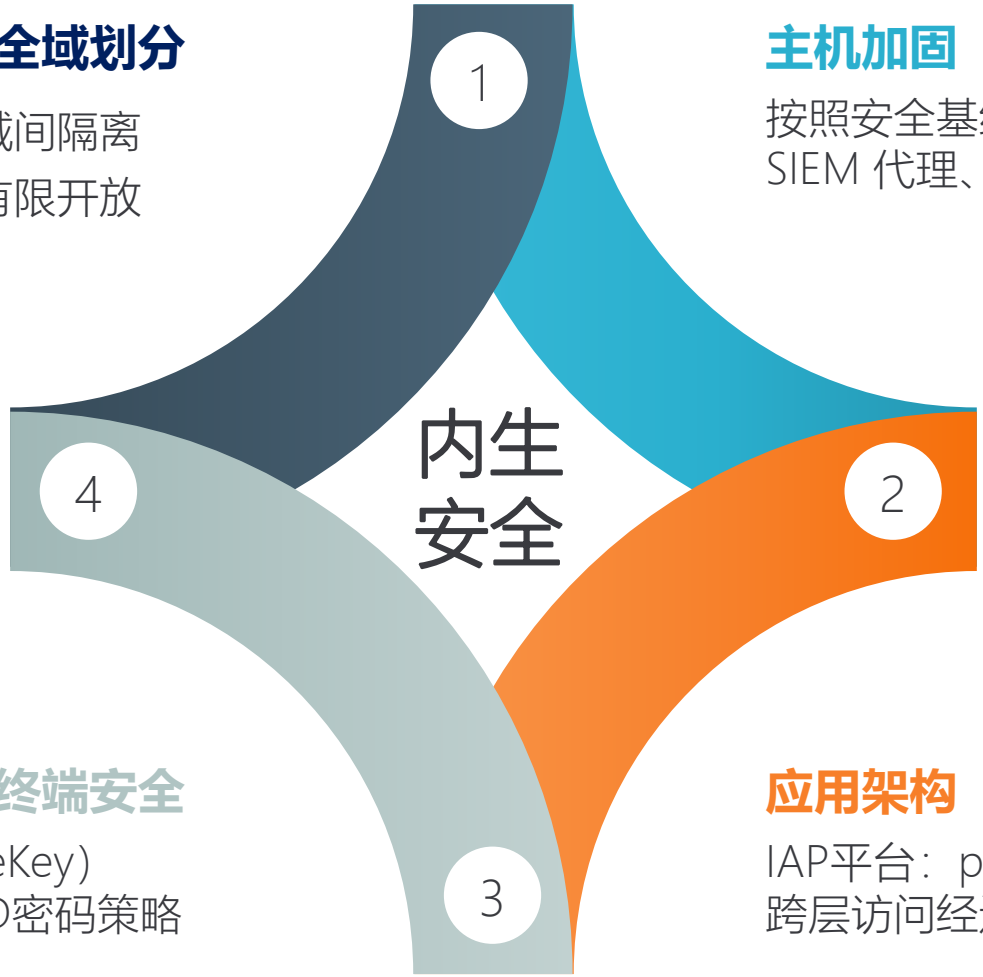
弱口令

- AD弱口令：脚本检查
- 系统弱口令：HIDS
- 应用弱口令：脚本检查

误配置

渗透测试（4轮）
HIDS
权限设置过大、demo目录

3、纵深防护--内生安全



安全域划分

网络架构：三横三纵、域间隔离
安全原则：默认阻断、有限开放

主机加固

按照安全基线制作模板
SIEM 代理、防病毒、HIDS

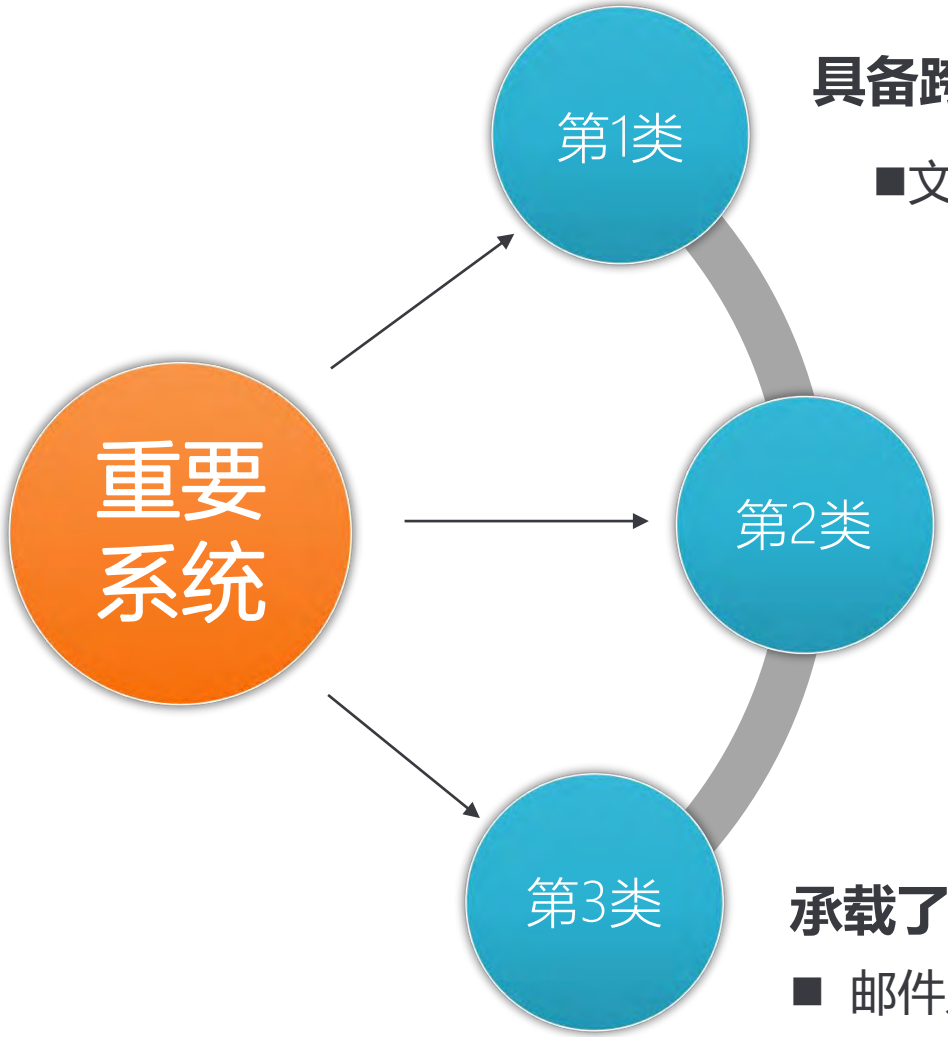
终端安全

外部：SSO（CAS+LDAP+eKey）
内部：SSO (多套AD），AD密码策略
办公终端：桌面云

应用架构

IAP平台：proxy+中间件+应用+DB
跨层访问经过防火墙 => 流量采集

3、纵深防护--重要系统梳理



具备跨网或跨域能力

■文件交换系统、漏洞扫描系统、运维监控系统

具备集中管理功能

- Agent进行集中管理：联软安全助手、日志收集分析系统、自动化运维平台
- 对用户进行集中管理：域控、SSO
- 对系统进行集中管理：堡垒机、虚拟化平台

承载了重要数据

- 邮件系统、中心数据库、源码服务器、OA、Wiki

3、纵深防护--重要系统防护

网络防护
限制访问源IP
非允许IP登录告警（含尝试）

应用防护
日志必须完整采集
账户梳理

行为分析
网络连接分析
进程分析

主机防护
部分开启软件防火墙
windows：防火墙必装
linux：hids必装

数据防护
对部分DB进行语句审计

3、纵深防护--覆盖矩阵

类型	系统名称	网络防护	主机防护	应用防护	数据防护	行为分析
具备跨网或跨域能力	文件交换系统	IPTables	HIDS	渗透整改		后台登录监控
	漏洞扫描系统		AV/HIDS	日志		运行时间监控
	运维监控平台		HIDS	日志		运行时间监控
具备集中管理功能	安全助手	源IP限制	HIDS	日志 禁用命令推送	DB审计	web命令执行
	域控	源IP限制 禁止反连	HIDS	日志	ATA	网络流量
	堡垒机		AV/HIDS	日志 双因素	N/A	绕行告警
承载了重要数据	源码系统	IPTables	N/A	日志 帐号清理		越权读取数据分析
	OA		HIDS	渗透整改	DB审计	web命令执行
	WIKI	N/A	N/A	N/A	N/A	N/A

默认：1、网络域间隔离；2、跨域访问禁止；3、关闭反向连接

4、安全防护框架

新增　计划

总控层安全	建立集团化的安全全局视图	SIEM 威胁情报　态势感知
用户层安全	管控普通员工、操作人员	安全客户端　堡垒机 双因素认证　绕行策略
数据层安全	管控办公文档数据、业务系统数据的主动、被动外泄	数据防泄漏　文印一体化　水印　API安全 邮件DLP　文件交换　数据脱敏　数据库审计
应用层安全	管控各类应用系统自身的安全性	安全规范　应用防护　信道加密　蜜罐 防篡改　应用漏扫　ATA
系统层安全	管控主机、终端等设备	安全基线　漏洞扫描　AV　蜜罐 终端安全　补丁管理　HIDS
虚拟层安全	管控服务器虚拟化、桌面虚拟化等平台的安全	云平台监控　主机异常　虚拟应用 主机加固　VPC
网络和物理层安全	管控网络、物理空间的安全	安全域划分　防火墙　入侵检测　门禁授权　NTA 网络准入　异常流量　上网行为　环境监控　NDR

04 面

总结

- “安全运营”定义
- 安全运营举例
- 重新审视“安全运营”

“安全运营”定义

职业欠钱

“为了实现安全目标，提出安全解决构想、验证效果、分析问题、诊断问题、协调资源解决问题并持续迭代优化的过程”

01

以终为始

以目标为导向
安全与业务相适应

02

持续迭代

是一个持续迭代的过程，
只有进行时
量化是持续迭代的手段

03

手段不限

管理和技术不分彼此

04

态度转换

由被动解决问题，向主动寻找问题转换

《我理解的安全运营》，职业欠钱，2018.7，https://zhuanlan.zhihu.com/p/39467201

CASE1：WEB应用上线前扫描

WEB 应用上线前要通过扫描器检测，不存在严重漏洞

原先

安全组担负扫描职责，成为瓶颈：

① 上线时间紧张，发现问题来不及整改

② 系统扫描时间长

③ 系统并发性能不足

现在

由测试团队负责：

① 安全组负责搭建、维护多套扫描环境

② 制定报告的通过标准

③ 对报告进行抽查

对漏洞进行统计分析，开展“开发安全专场培训”

CASE2：日志收集分析系统运营

1、合规；2、发现安全风险

原先

几乎沦为摆设：

① 从最初100台设备，减少到40多台设备。（孤岛严重）

② 其他团队不参与

③ 刻板报告模板，一次巡检要4个小时

④ 数据保存半年

现在

真正运转起来：

① 写入主机安全基线，生产系统全覆盖

② 对24h未接入设备进行监控

③ 根据各类检查、渗透测试结果不断进行规则优化

④ 热数据一年，冷数据十年

- 口号：“日志是基础，规则很关键，运营才核心”
- 在演练、攻防中不断提升系统的曝光度

CASE3：员工安全责任落实

让全体员工能参与到安全建设工作中

通常

信息安全不出技术部门：

① 大领导不改密码

② 业务部门不装杀毒软件

③ 没有面向全公司的宣传和教育渠道

④ 对员工无任何约束能力

我们

全局管理：

① 建立信息安全组织架构，定期向管理层汇报。各部门设安全员。

② 制定个人信息安全量化积分，与部门考评挂钩

③ 每年开展信息安全考试、全员培训、钓鱼邮件测试

- 口号：“信息安全，人人有责”
- 打造安全团队靠谱的形象

重新审视“安全运营”

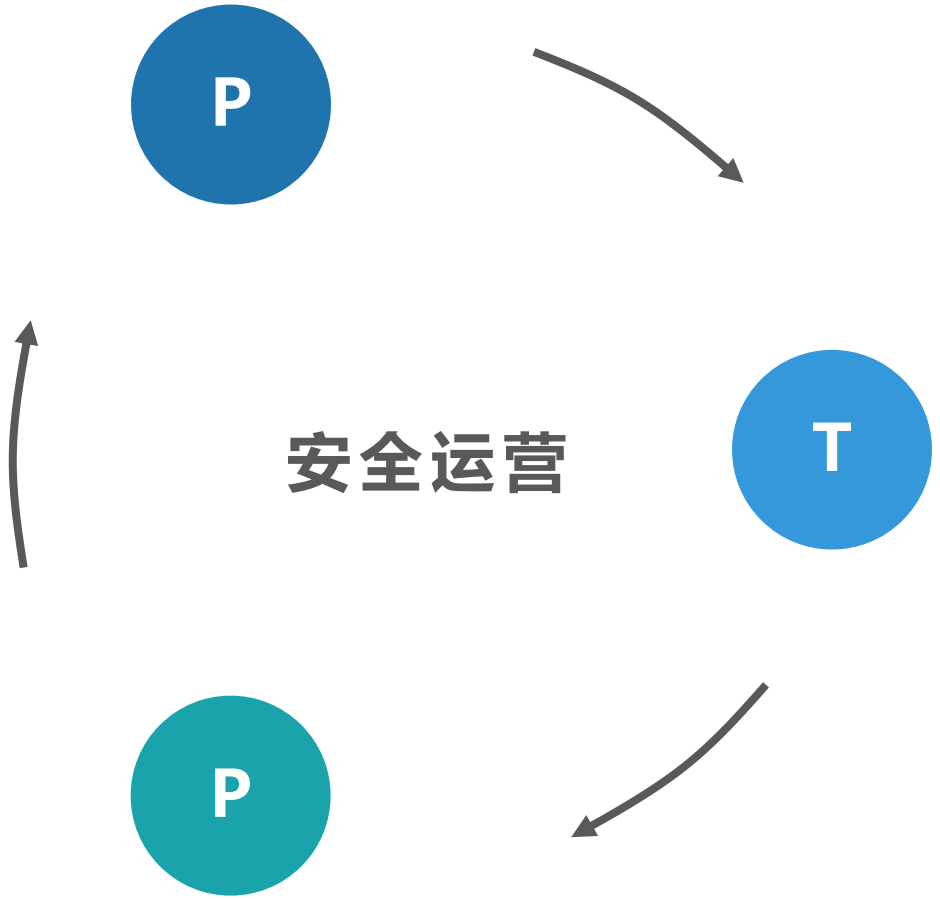
> “为了实现安全目标，提出安全解决构想、验证效果、分析问题、解决问题并持续迭代优化人员、流程和技术的过程”

Process流程

安全员制度，覆盖所有部门
信息安全管理体系
应急预案

People人员

量化积分、意识培训
专职安全岗位
培训、交流、技能考核



技术Tech

日志收集与分析系统
漏洞管理系统
主机漏洞扫描系统
Web扫描系统
漏洞通报
渗透测试
流量分析系统（集成威胁情报）
补丁扫描：HIDS

当前状态

- 网络安全域
- 补丁管理
- 安全基线
- 规划、设计阶段安全需求

- 收缩攻击面
- 消耗攻击资源
- 拖延攻击时间

- 数据全面采集
- 监控响应
- 消费情报
- 红蓝对抗
- 人的参与

- 机器学习
- 行为建模
- 攻击者画像
- 生产情报

- 法律手段
- 反制措施
- 自我防卫

网络安全防御是一个动态迭代的过程，我所正处于，并将长期处于“主动防御与智能化迭代”阶段

<The Sliding Scale of Cyber Security>, Robert M. Lee,2015, SANS 美国系统网络安全协会

“安全运营“最终目标

战时如平时

- 疯狂封IP、下线服务，不可持续发展
- 必然路径：梯度覆盖 -> 自动化 -> 智能化
- 太多告警等于没有告警，要求日告警数量控制在100以内，越少越好
  - 关联规则不断优化
  - 提升端的安全覆盖率
  - 引入新技术，发现深层次威胁
- 不要寄希望于单纯外购产品解决所有问题，当前引入的产品要充分接口化。

THANKS

2019北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE