



网络安全创新大会
Cyber Security Innovation Summit

(照片部分由主办方添加)

甲方视角下的攻防演练部署

棉花 某航司安全专家

攻防演练行动目的

检验各单位信息基础设施和重点网站网络安全的综合防御能力和水平，实战验证相关单位“监测发现、安全防护和应急处置”的能力，发现并整改网络系统存在的深层次安全问题。

2020年攻防演练整体安排

时间：

攻击队伍：

防守单位：

目标范围：参演单位的关键基础设施及重要信息系统单位

专家组：

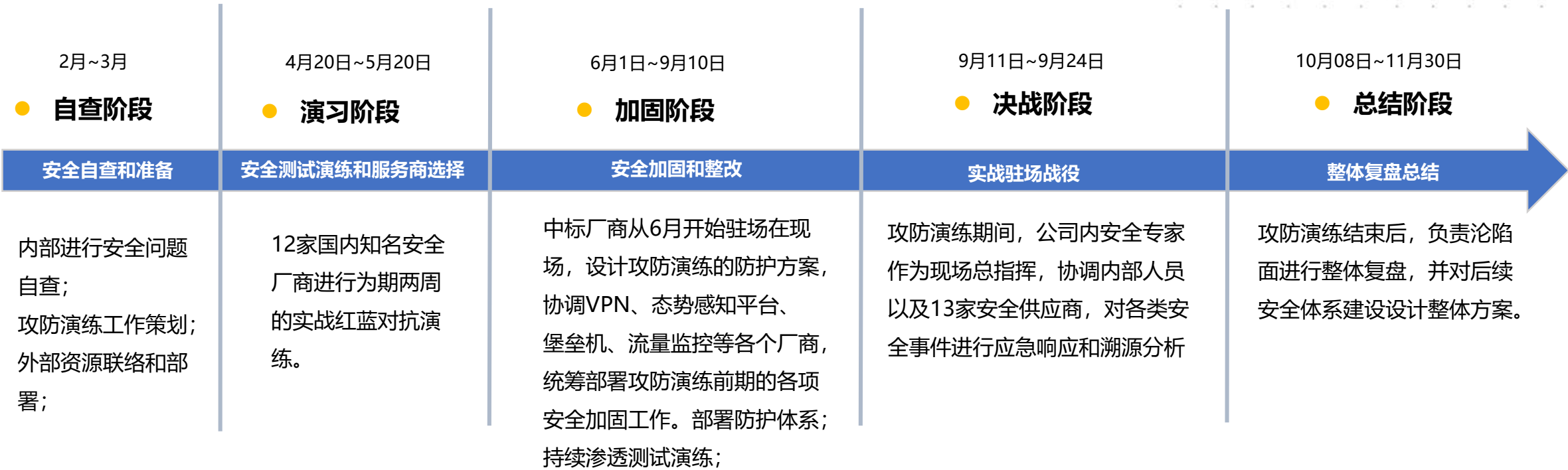
攻防演练行动实施方式

组织部门负责组织攻防演练演习行动，由安全厂商、电信运营商、金融业、高校、科研院所等信息安全专业人员组成攻击队伍，对政府机关、重要事业单位、大型国企等单位的关键信息系统进行集中攻击，而目标单位作为防守方对攻击进行实时防御拦截；
被攻破的单位和防护标杆会被作为典型案例
攻防演练演练已成为每年例行工作，重点单位申请固定预算，作为例行工作推进；

重点覆盖单位类型

工信部、海关总署、交通运输部、国税总局、国家邮政局、
国家电网、南方电网、民航总局、三大航司、城市商业银行、
中核集团、中石油、中石化、中交建、中外运、中铁建、
中国移动、中国联通、中国电信、人民网、央视网、新华网

2020 攻防演练防护过程回顾



组织保障

行政层面集团领导高度重视，成立多层级的保障组织，各工作小组职责明确，协同工作，保障攻防演练工作有效进行。

资源保障

提前进行资源统筹，包括内外部人员统筹安排、安全防护、检测产品、安全服务资源等。

安全检测加固

目标系统进行独立安全域划分、识别系统存在的薄弱环节、进行有针对性的整改加固。

提升监测和响应能力

在现有防护体系基础上，部署能力更强的网络安全监测设备，提升网络安全事件的监测能力，发现安全攻击立刻采取措施，中断攻击行为。

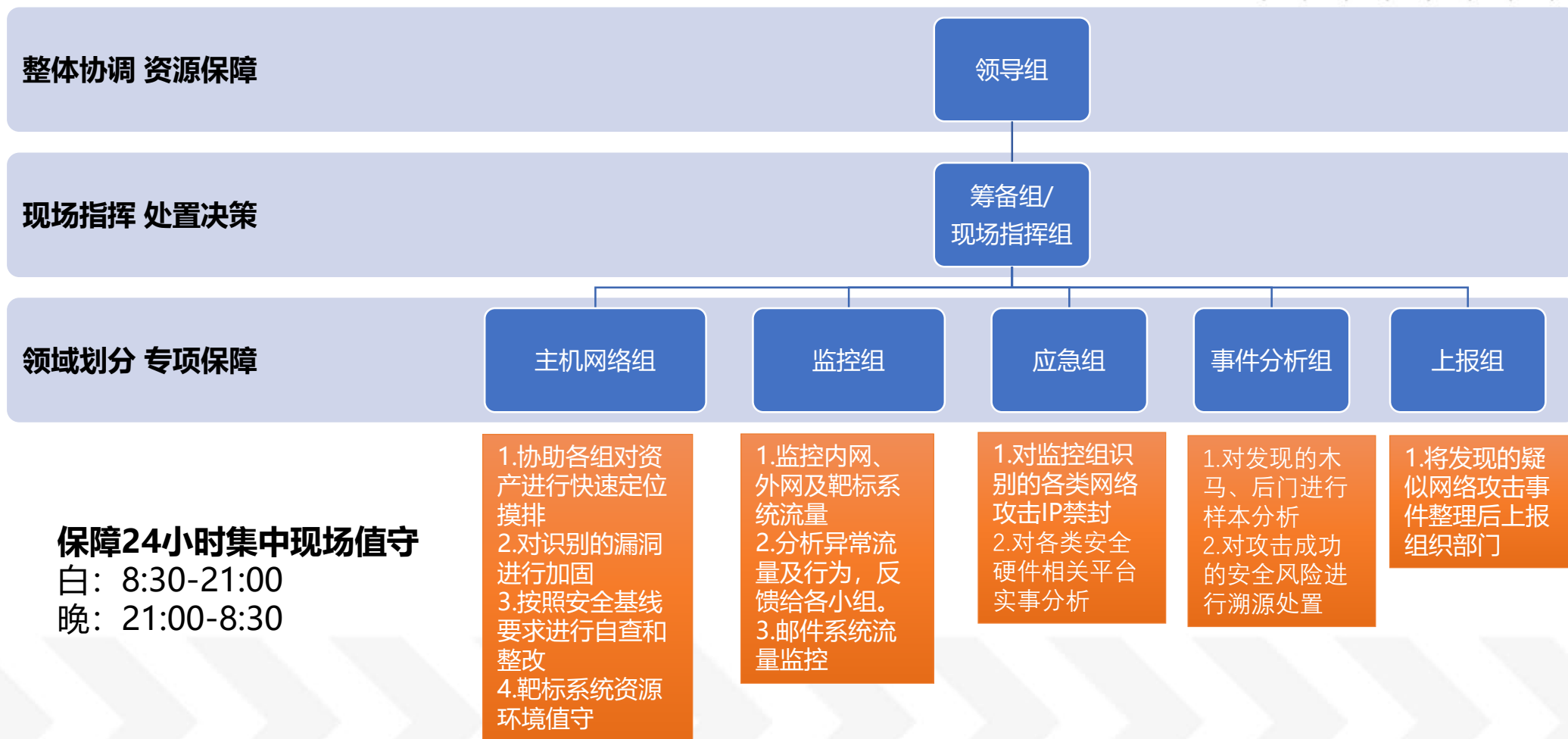
攻防演练预演习

基于真实场景进行攻防演练预演习，固化攻防演练保障流程，提高攻防演练工作效果和效率。

攻防演练初始阶段准备-组织保障

设立攻防演练专项保障组织架构，专业分工协同保障

组织架构覆盖应用、主机、网络、机房等各层级部门



攻防演练初始阶段准备-资源保障

- 互联网、广域网专线出口：Waf、IPS、防火墙、旁路封禁设备等;主机安全防护、域控安全防护等

安全防护

- 互联网、广域网专线出口、数据中心：流量溯源、态势感知探针、威胁情报、邮件溯源平台系统

检测产品

- 多轮全网漏洞扫描
- 多轮渗透测试、三轮红蓝实战演习、全程攻防演练专家团队协助等

安全服务

- 攻防演练专家、安全渗透专家、流量分析专家、攻防演练甲乙双方项目经理等

人员统筹

基于攻击者视角的攻防演练思路

模拟黑客的动机和目的，站在敌人的角度思考攻击，例如：

- 我们的敌人是谁？如何模拟敌人的攻击？
- 我们的目标是？
- 攻击路径和攻击方式的覆盖率？
- 攻击过程的隐蔽性、攻击完成后的痕迹清理
- 面对上百支战队，需要自动化防御能力



白帽子黑客，点到为止

- 立体纵深防御体系，防御协同（检测、止血、加固、溯源、反制）
- 基于外部黑客/黑产视角，及外部检验能力

从甲方的角度来讲，要想知道如何针对性的防御，在除了被动性的防御也要从攻击者的角度来对攻击者的攻击路线和手法进行了解，以便更好的在边界防御，纵深防御的理念下对攻击对各个环节进行加固。

网络攻击过程总览



攻击前准备阶段

- 目标定位
- 信息搜集和敏感信息提取
- 工具准备

入侵控制阶段

- 武器与资源准备信息提取
- 漏洞攻击
- 木马植入
- 搭建隐蔽隧道
- 入侵内网

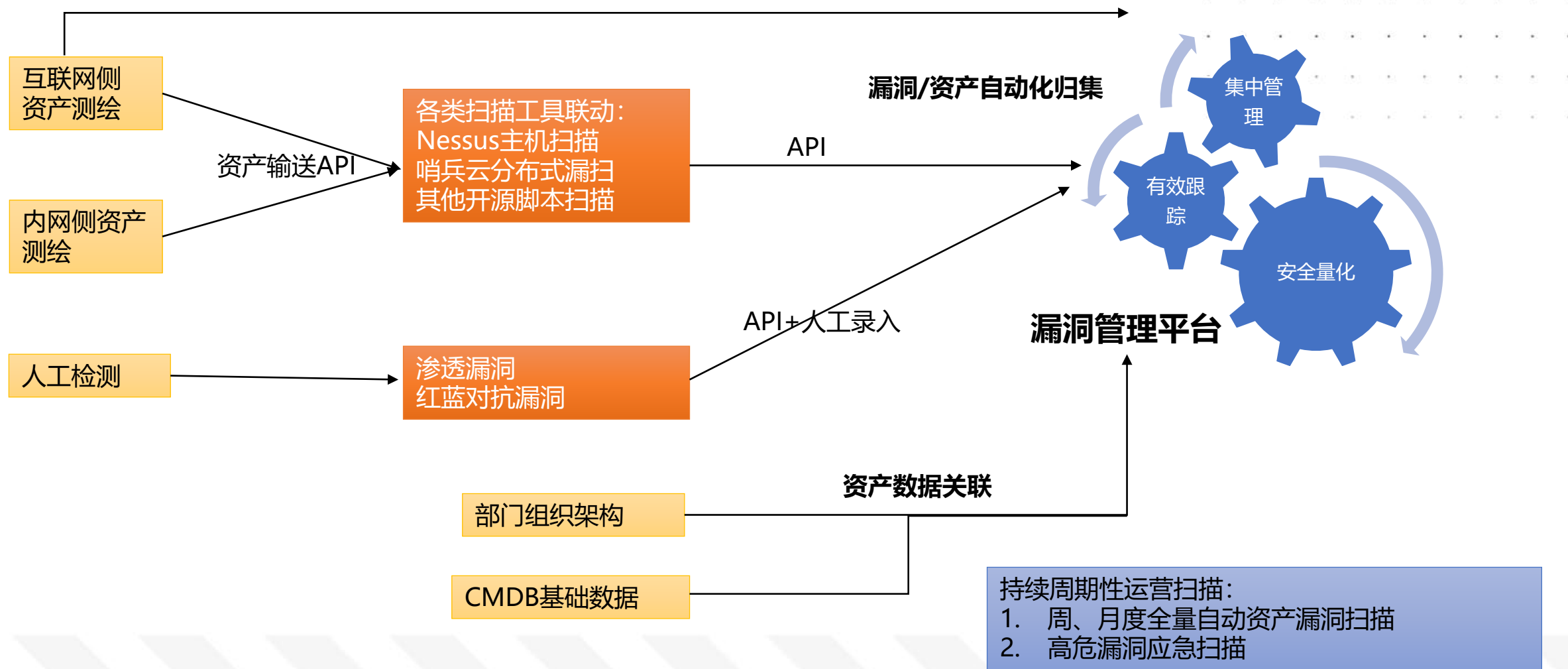
内网渗透成果扩展阶段

- 多点埋伏
- 内网横向渗透攻击
- 重要系统攻击与敏感信息获取
- 内网纵向渗透工具

攻击结束清理战场阶段

- 清理木马及后门
- 清理残留数据
- 应用系统还原
- 清理日志信息

基于攻击者视角的攻防演练思路-资产自动化梳理



攻防演练初始阶段准备-漏洞清单排查

主机漏洞	Web漏洞	通用应用漏洞
<div>未授权访问</div> <div>SNMP未授权访问漏洞</div> <div>rsync 未授权访问漏洞</div> <div>弱口令</div> <div>MySQL弱口令漏洞</div> <div>SSH弱口令漏洞</div> <div>MongoDB弱口令漏洞</div> <div>MSSQL弱口令漏洞</div> <div>RDP弱口令漏洞</div> <div>PostgreSQL弱口令漏洞</div> <div>HTTP 401认证弱口令漏洞</div> <div>MSSQLServer弱口令漏洞</div> <div>Redis弱口令漏洞</div> <div>Memcached弱口令漏洞</div> <div>SMB弱口令漏洞</div> <div>FTP弱口令漏洞</div> <div>Telnet弱口令漏洞</div> <div>Oracle弱口令漏洞</div> <div>LDAP弱口令漏洞</div> <div>DB2弱口令漏洞</div> <div>Tomcat弱口令漏洞</div> <div>phpmyadmin弱口令</div> <div>smtp弱口令漏洞</div> <div>pop3弱口令漏洞</div> <div>系统/服务器补丁不及时漏洞</div>	<div>SQL注入</div> <div>CRLF注入</div> <div>跨站脚本攻击(XSS)</div> <div>文件包含</div> <div>本地文件包含漏洞</div> <div>远程文件包含漏洞</div> <div>文件上传</div> <div>信息泄露</div> <div>权限许可和访问控制</div> <div>跨站请求伪造(CSRF)</div> <div>路径遍历</div> <div>设计错误</div> <div>配置错误</div> <div>任意文件操作</div> <div>远程命令执行</div> <div>被植入后门</div> <div>HTTP协议相关安全问题</div> <div>服务端模版注入漏洞</div> <div>逻辑漏洞</div> <div>认证缺陷</div> <div>SSRF</div> <div>XXE</div> <div>URL重定向</div> <div>条件竞争</div> <div>设计不当/逻辑错误漏洞</div>	<div>Discuz</div> <div>DedeCms</div> <div>PhpWind</div> <div>Ecshop</div> <div>Phpcms</div> <div>Anwsion</div> <div>ShopEx</div> <div>ShopXP</div> <div>Modoer</div> <div>AspCms</div> <div>PhpWeb</div> <div>PHP168</div> <div>KingCMS</div> <div>ASP.NET</div> <div>FCKEditor</div> <div>Joomla</div> <div>phpMyadmin</div> <div>Dvbbs</div> <div>帝国CMS</div> <div>HDWIKI</div> <div>ESPCms</div> <div>Cmseasy</div> <div>PhpYun</div> <div>Qibosoft</div> <div>EYou</div> <div>Struts2</div>

依托日常自动化的资产收集测绘，攻防演练前由驻场安全团队重复3轮进行全面的漏洞、风险检测并进行快速协作清理。

对于Fastjson、Shiro等攻防演练常被利用的Nday从项目代码库编写脚本从源代码层全部检索，对照版本全部升级。

Weblogic等常见高危中间件全覆盖检测升级加固。

攻防演练初始阶段准备-共存场景重点加固

弱口令普遍存在

互联网上泄露敏感信息

专网非法外联情况严重

内网互联网情况暴漏面过多

老旧资产成为攻击跳板

漏洞修复速度慢

漏洞存储敏感文件

服务器普遍是零防御状态

网络缺乏细颗粒度隔离

供应链安全风险巨大

互联网VPN接入问题严重

收集APP成为高排名攻击入口

日常的安全工作中和攻防演练
加固后的总结中发现该**12**类
问题仍是是需重点加固环节。

攻防演练初始阶段准备-攻防演练预演习 结果分析

VPN

- 1、启用双因子登录
- 2、VPN设备IP重点隔离

堡垒机

- 1、安装补丁加固
- 2、双因子验证
- 3、生产系统均接入

域控

- 1、域控访问隔离
- 2、部署watch AD持续监控
- 3、安装补丁加固

预防0day攻击导致的权限丢失，加紧对集权类系统做访问权限控制与加固。
安全设备均启用双因子验证登录，进一步增加集权类系统的普通用户身份验证。

分子公司网络出口

- 1、分子公司出口流量检测部署
- 2、部署开源蜜罐监测
- 3、收紧互联网出口

统一身份认证系统

- 1、业务逻辑层漏洞修复
- 2、系统日志重点监控

攻防演练初始阶段准备-安全检测加固



- 在内网私搭的互联网出口代理排查
- 排查清理了公网中泄露的有关公司相关的敏感信息例如Github、各类网盘等
- 针对堡垒机、邮件服务器、域控单独做排查

- **完成了漏洞平台中漏洞的修复和复测，在攻防演练开始前实现了严重和高危漏洞清零**
- 关闭私搭代理服务器
- 信息部邮箱备份后清空
- **全员更改密码**
- 对VPN、堡垒机等集权系统，进行了特权账户排查
- 对域控、邮件服务器进行安全加固

- **在VPN入口启用密码+企业微信验证码的双因素认证**
- **堡垒机采用双因子认证，并修改登录密码**
- 部署了全流量分析防护设备
- 收集目前攻击队常用的Nday漏洞列表
- 干扰信息发布
- 靶标系统专项加固
- 部署主机防护

- **开展了两次邮件钓鱼演练，开展了U盘钓鱼的攻击演练**
- 整理攻防演练期间应急响应方案和小组值班分工
- 设计了应急演练脚本，持续开展应急演练

通过各部门调研和资产盘点根据公司情况制定**X**余项安全防护整改内容和工作项

基于攻击者视角的攻防演练思路

资产风险指标

- 历史漏洞评估和复测
- 资产暴露面
- 安全策略覆盖率

入侵检测效果指标

- 已知场景覆盖率
- 蓝军对抗主动发现率

攻防演练效果指标

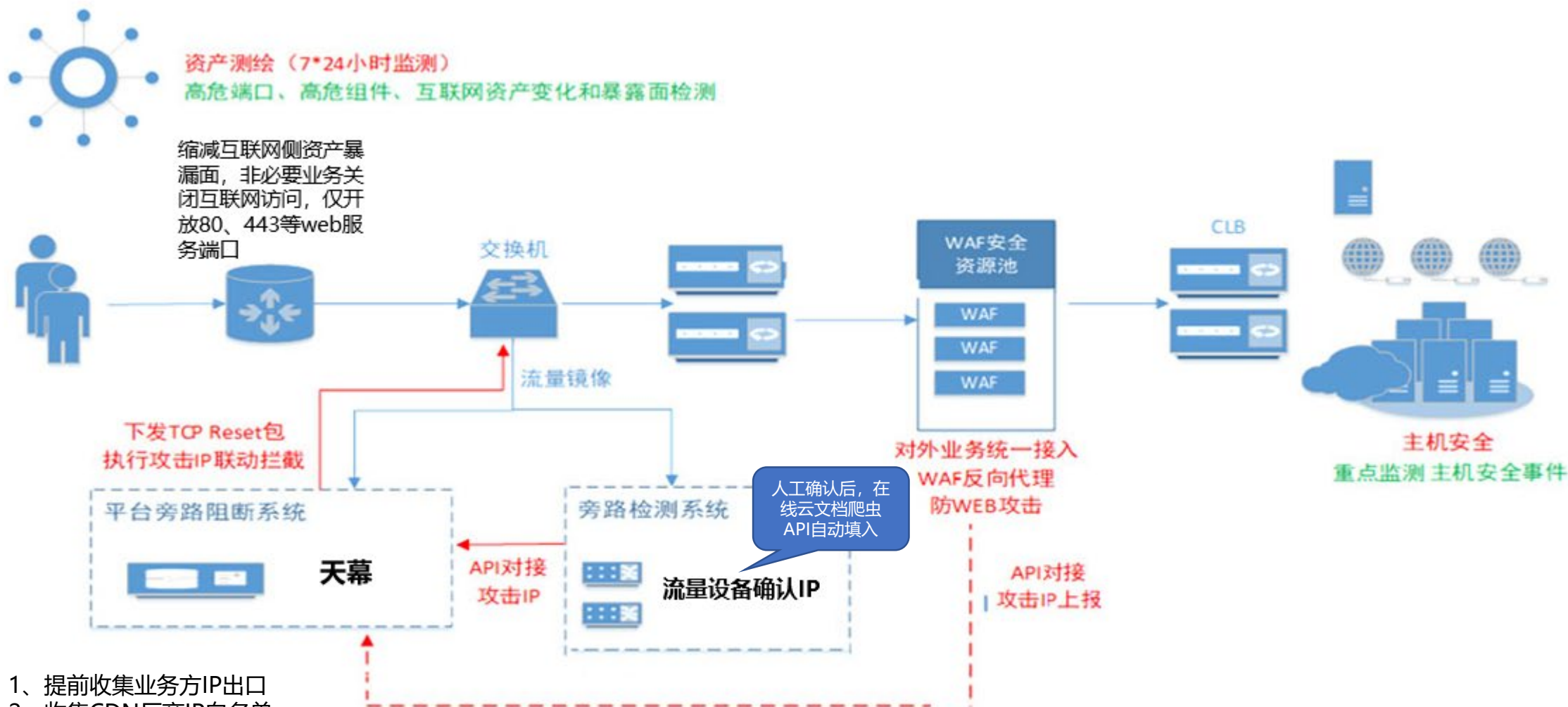
- 风险资产收敛
- 攻击事件趋势
- 攻击IP趋势



基于黑客视角攻击链多锚点检测
提升威胁发现率

联动防御攻击IP封禁
提升攻击成本

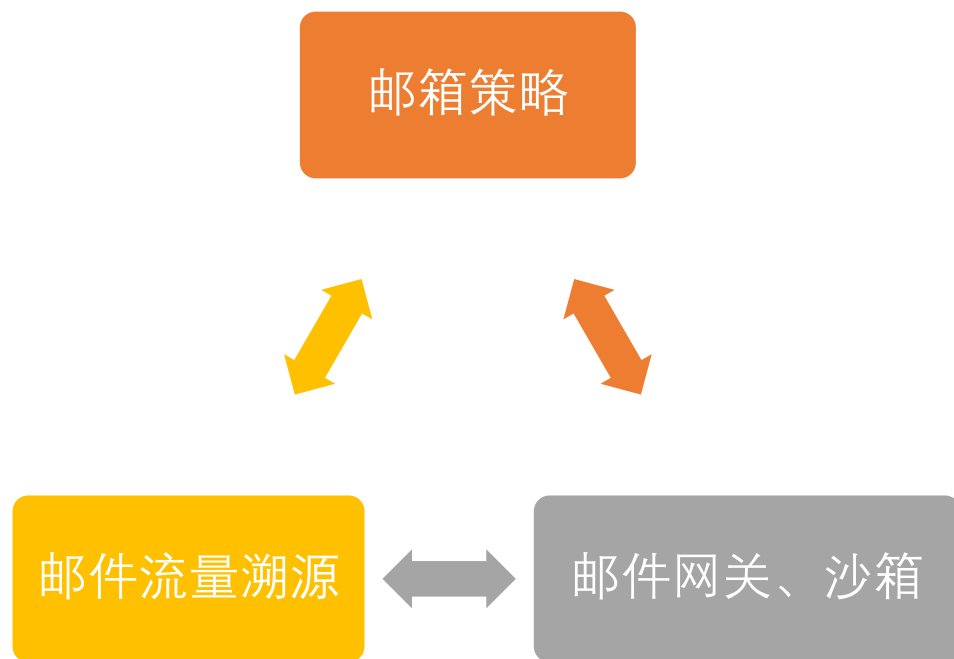
主机加固构建最后一道防线
提升响应能力



- 1、提前收集业务方IP出口
- 2、收集CDN厂商IP白名单
- 3、waf等其他安全设备规则调优

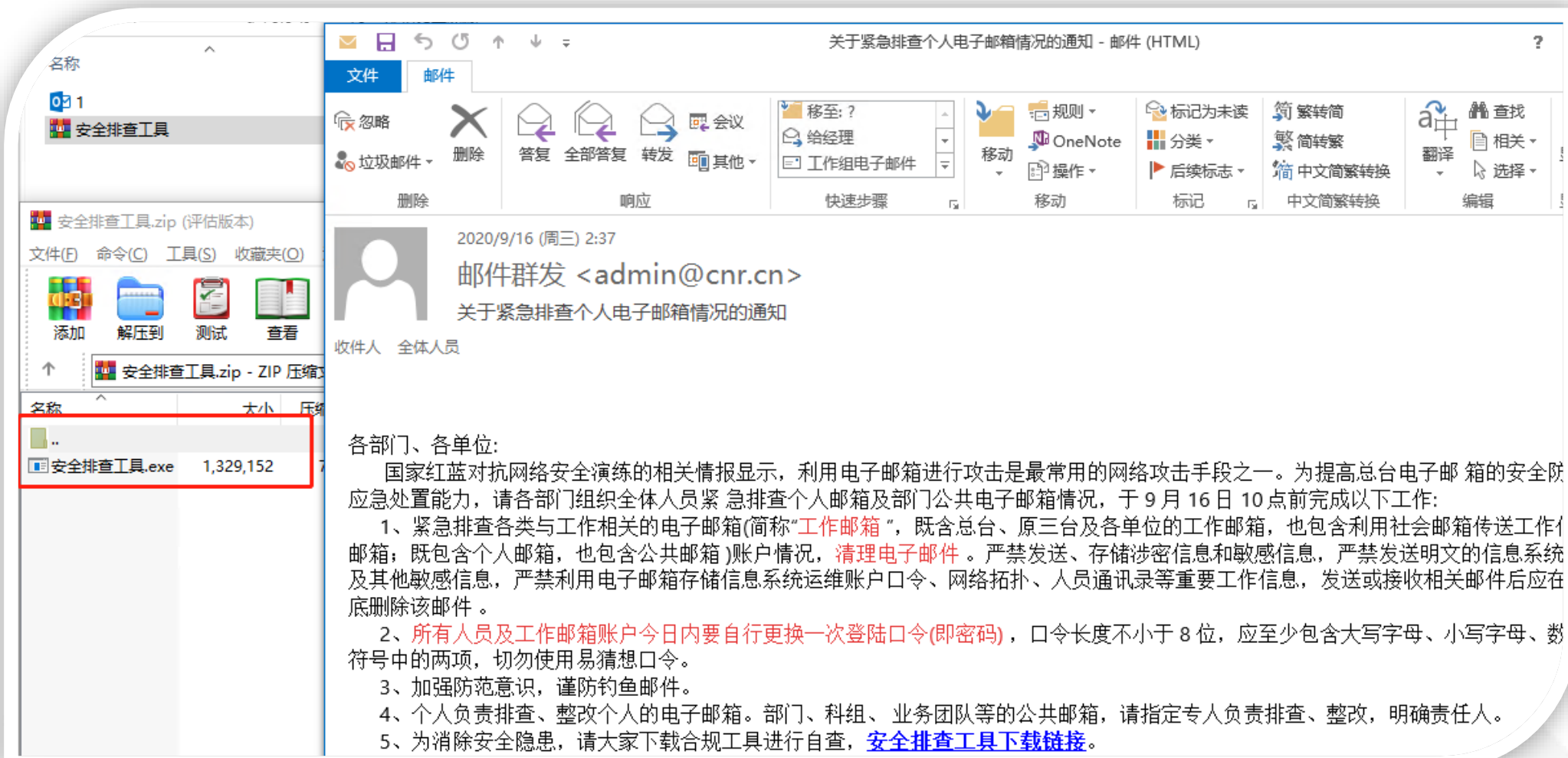
减少误报与误封IP机率, 实现自动化高效威胁自动阻断

员工10万+全员安全意识一直是一个痛点，
在攻防演练期间邮件流量分析溯源，阻断钓鱼邮件是较为重要的一项任务。



1. 针对全体邮箱限制普通用户发送数量限制
2. 邮件沙箱、网关自动阻断策略，大量外部域名批量无法发送。
3. 流量层邮件溯源分析，制定密码、下载、安全、更新等钓鱼邮件常见关键字，攻防演练期间专人值守对邮件内容进行溯源分析。
4. 邮箱管理员轮流值守，如流量溯源组发现高危邮件则批量直接后台批量清除。

攻防演练中工作部署-钓鱼邮件案例



The image shows a phishing email interface on the right and a Windows File Explorer on the left. The email, titled '关于紧急排查个人电子邮箱情况的通知 - 邮件 (HTML)', is from '邮件群发 <admin@cnr.cn>' and dated '2020/9/16 (周三) 2:37'. The subject is '关于紧急排查个人电子邮箱情况的通知'. The email body contains instructions for a security drill, mentioning the need to check personal email accounts and change passwords. It lists five tasks: 1. Check all work-related email accounts (including personal and public ones) and clean up old emails. 2. All staff must change their login passwords today, with requirements for length and complexity. 3. Strengthen防范意识 (awareness) and prevent phishing. 4. Individuals responsible for checking and整改 (rectification) of their own email accounts. 5. Download the '安全排查工具' (Security Check Tool) for self-inspection. The File Explorer on the left shows the downloaded file '安全排查工具.exe' (1,329,152 bytes) in a folder named '安全排查工具.zip - ZIP 压缩包'.

关于紧急排查个人电子邮箱情况的通知 - 邮件 (HTML)

文件 邮件

忽略 删除 回复 全部回复 转发 会议 其他

移至: ? 给经理 工作组电子邮件

快速步骤

规则 OneNote 移动 操作 移动

标记为未读 分类 后续标志 标记

简繁转简 繁简转繁 中文简繁转换 中文简繁转换

查找 翻译 相关 选择 编辑

2020/9/16 (周三) 2:37

邮件群发 <admin@cnr.cn>

关于紧急排查个人电子邮箱情况的通知

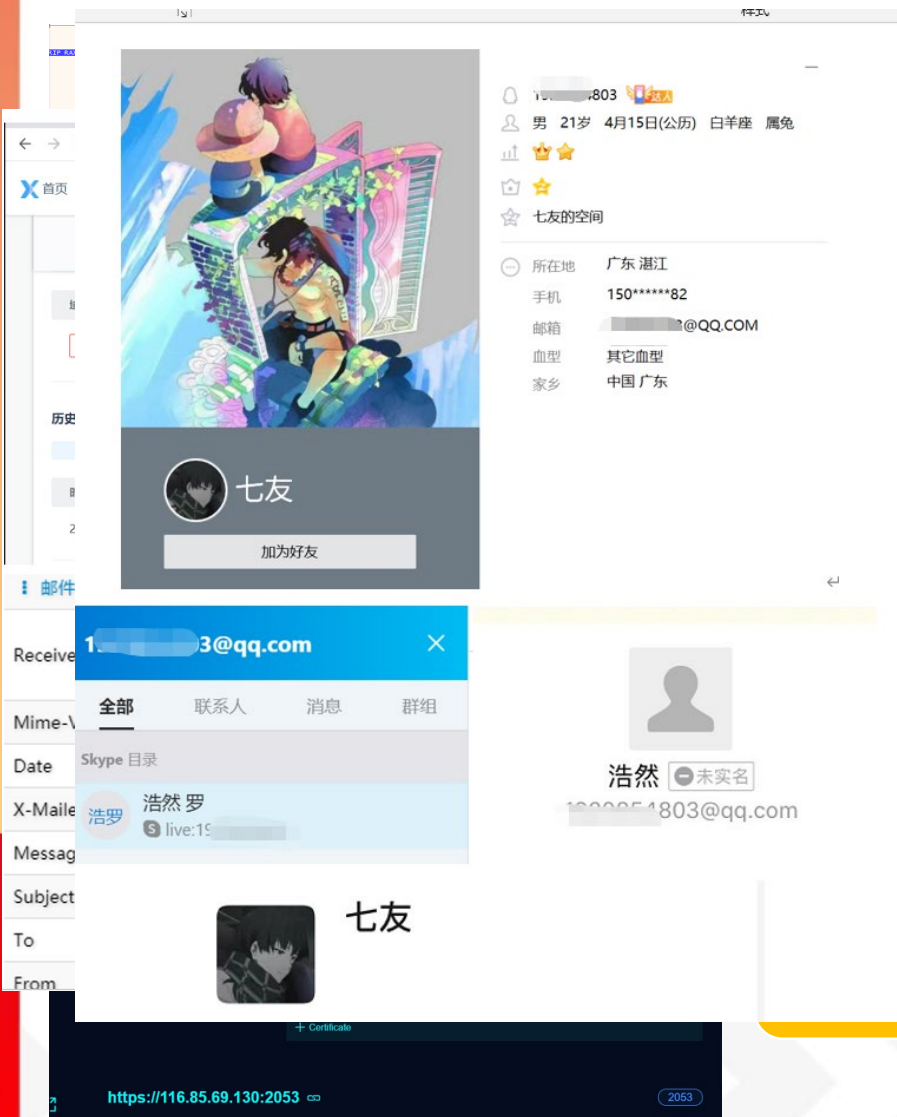
收件人 全体人员

各部门、各单位:

国家红蓝对抗网络安全演练的相关情报显示,利用电子邮箱进行攻击是最常用的网络攻击手段之一。为提高总台电子邮箱的安全应急处置能力,请各部门组织全体人员紧急排查个人邮箱及部门公共电子邮箱情况,于9月16日10点前完成以下工作:

- 1、紧急排查各类与工作相关的电子邮箱(简称“工作邮箱”,既含总台、原三台及各单位的工作邮箱,也包含利用社会邮箱传送工作电子邮箱;既包含个人邮箱,也包含公共邮箱)账户情况,清理电子邮件。严禁发送、存储涉密信息和敏感信息,严禁发送明文的信息系统及其他敏感信息,严禁利用电子邮箱存储信息系统运维账户口令、网络拓扑、人员通讯录等重要工作信息,发送或接收相关邮件后应在底删除该邮件。
- 2、所有人员及工作邮箱账户今日内要自行更换一次登陆口令(即密码),口令长度不小于8位,应至少包含大写字母、小写字母、数字符号中的两项,切勿使用易猜想口令。
- 3、加强防范意识,谨防钓鱼邮件。
- 4、个人负责排查、整改个人的电子邮箱。部门、科组、业务团队等的公共邮箱,请指定专人负责排查、整改,明确责任人。
- 5、为消除安全隐患,请大家下载合规工具进行自查, [安全排查工具下载链接](#)。

攻防演练中工作部署-钓鱼邮件案例



非查工具.exe

加密载荷

mbcweb.com:2
CTae

远控木马上线

www.cmbcweb.com

116.85.xxx.xx0历史解析
bty.cloud该域名也曾在针对我
公司的钓鱼邮件中出现

Fofa查询cmbcweb.com相关证
书还出现在另一国内
IP116.85.xxx130(滴滴云)

仿冒民生银行
www.cmbcweb.com
2020.7.6在Godaddy注册

根据木马中编译路径
C:/Users/qiyou/

对比微步威胁情报沙箱hash检
索分析攻防演练期间这批样本
曾解析到119.23.xx.230 (阿里
云)

7月18日出现样本回连的C&C
地址为119.23.xx.230 (阿里
云), 关联的域名7xxu.site

进一步针对该红队人员进行溯
源得到身份画像: 手机号、qq、
微信、支付宝等信息

攻防演练中工作部署-攻防演练原则和关键点

招募同盟军



与部分参演甲乙方形成同盟，实现信息共享、协同作战

保卫边境线



重点保证互联网出口、广域网等堡垒防线不被突破

装备预警机

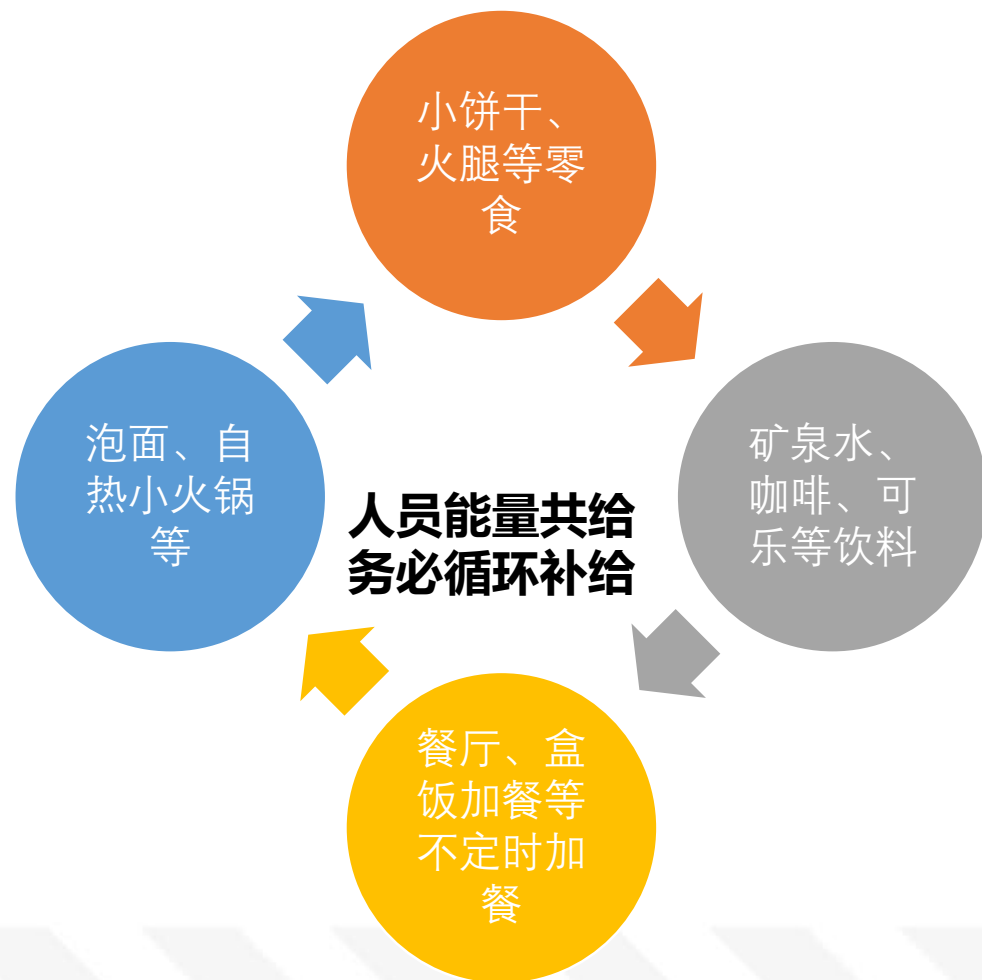


各渠道威胁情报收集共享：0day预警、威胁ip等等

穿上隐身衣



靶标系统重点加固后，形成有效在线时间机制



现场值守人员，吃得好、休息的好才能有精力持续的完成各项保障工作，对参与攻防演练期间值守的甲乙双方同事表示衷心的感谢！

攻防演练结束复盘问题与总结

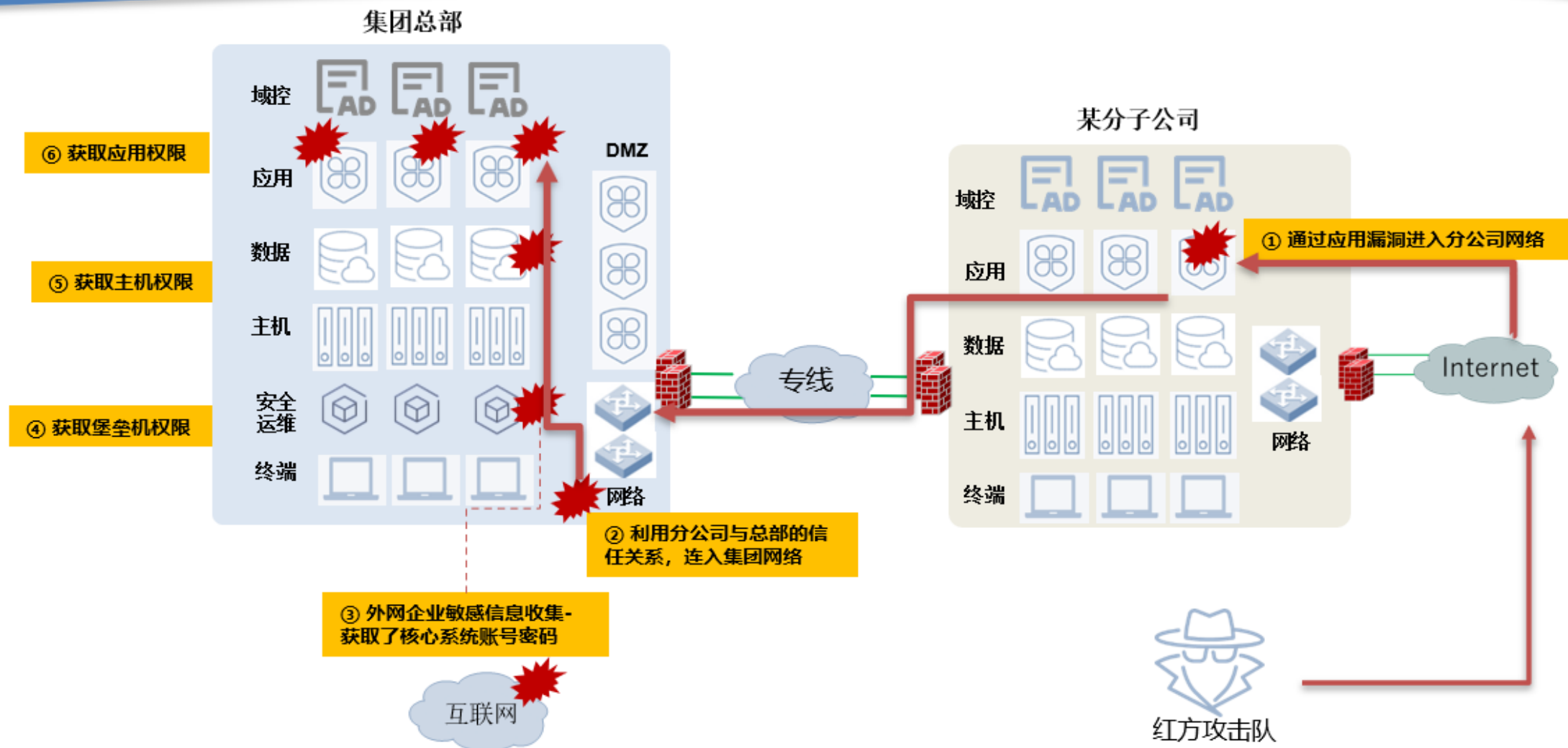
安全自查和准备

安全测试演练和服务商选择

安全加固和整改

实战驻场战役

整体复盘总结



安全自查和准备

安全测试演练和服务商选择

安全加固和整改

实战驻场战役

整体复盘总结

复盘护网过程，总结实战防守经验

- 护网结束后，汇总、复盘、分析所有攻击数据和我方的防守措施，并总结经验教训，对现存问题提出合理整改建议。
- 对于好的防守流程经验、应急措施、防护设备等，后续进行沉淀固化

全视角梳理，提供体系化安全建设优化建议

梳理在护网中被突破的各个核心点，整理出公司在后续需要进行深度整改的措施，推进整体信息化安全建设

提升公司常态化防守能力

推动公司安全体系建设

收到了公安部发来的攻防演练报告，评价是：取得了较好的成绩！

2000万次

值守团队每天抵御近2000万次互联网攻击。截止到攻防演练结束，安全设备中共封禁互联网IP地址。

316起

研判各类内网安全告警316起

12份

攻防演练中攻击溯源组共提交溯源报告12份，溯源到疑似攻击者画像3人。

实战检验防护能力

发现隐藏的安全问题

优化安全运维管理流程

提升团队协作



棉花

上海 长宁



扫一扫上面的二维码图案，加我微信



网络安全创新大会
Cyber Security Innovation Summit

THANKS