护网保障概述

绿盟科技版权所有

绿盟科技

CONTENTS 目 录

绿盟科技版权所有

CONTENTS 目 录

绿盟科技版权所有

NSFOCUS

01

什么称为护网行动？

1. 护网行动背景
2. 护网行动规则
3. 护网期间技巧

绿盟科技版权所有

NSFOCUS

1.1

护网行动背景

a. 护网行动背景介绍

b. 护网行动演进历史

绿盟科技版权所有

护网行动背景

1、什么是“护网行动”？

- ✓ 指挥机构：由公安机关统一组织的“网络安全实战攻防演习”。
- ✓ 护网2019分为两级演习：公安部对总部，省厅对省级公司。

2、什么是“实战攻防演习”？

- ✓ 每支队伍3-5人组成，明确目标系统，不限制攻击路径。
- ✓ 提交漏洞不得分，获取权限、数据才能得分。

旁站攻击 暴力破解 Web渗透 操作提权

【禁止行为】

- ➢ 不能使用DDOS攻击，部分目标系统需要在非常规攻击时段进行攻击操作；
- ➢ 不能使用破坏性的物理入侵，但针对如无人值守变电站、智能电表等均在测试范围之内；
- ➢ 不能使用有感染及多进程守护功能的木马；
- ➢ 重要业务系统进行攻击操作前需要向指挥部进行请示；

绿盟科技版权所有

护网行动背景

“护网行动”的演进历史

护网2016

国家电网、国内民航系统

护网2017

国家旅游局、北京市食药监局、 北京自来水集团、北京教育考试院、中国人寿、中科院、央视网、首汽租车、安贞医院、小米科技、网宿科技...

护网2018

税务、电力、电信、银行、铁路、财政、广电、水利、教育、互联网、检察院、法院、石油、交通...

护网2019

行业更广、

范围更大、

运营商行业

“护网2018”参考：

「行动目标」：涉及税务、电力、电信、银行、铁路、财政、广电、水利、教育、互联网、检察院、 法院、石油、交通等16个行业、29家单位、45个公安部指定的目标系统，+26个中非论坛目标系统。（其中，国税总局电子发票系统、中移动的官网门户系统覆盖全国各省）

「攻击队伍」：公安、军队、科研院所、学校、信息安全企业等组成41支攻击队伍。

「行动时间」：2018年7月16日-7月27日，5月至6月为准备工作期。

绿盟科技版权所有

1.2

护网行动规则

a. 护网2018—攻守对抗规则
b. 护网2018—防守方减分规则
c. 护网2018—防守方加分规则

绿盟科技内部培训专用

护网 2018 — 攻守对抗规则

攻守对抗规则

攻击靶心由各单位自报或公安部指定，公安部一般提前3周通知各单位参演靶心，以及攻击的起始时间与结束时间，各单位可在此期间进行防御准备。

防御团队

由护网单位自行组织安全专家进行针对性防御。

护网防御

防御人员：护网单位组织安全专家进行全方位防御（针对攻击靶心）；

防御方式：不限防御方式，监控全网的攻击，及时发现并处置，避免内部系统被攻陷；

护网攻击

攻击人员：3-5人一组， 每组对一个目标进行攻击；

攻击方式：不限攻击方式，但攻击过程受到监控（在2018年护网实际开展中，对攻击未监控，因此攻击的时间地点不受控）；

攻击团队

由公安部组织包括国家信息安全队伍、军队、科研机构、测评机构、安全公司等共几十支队伍，百余人组成。

评分原则：

指挥部拟对攻防双方进行评分考核。对防守方评分的总体原则是：

1. 根据安全防护能力强弱对防守方进行排名；
2. 初始分5000分；
3. 目标系统被拿下不参加排名，即护网失败；
4. 攻击方提交报告 1 小时内，防守方发现来自攻击方的行为并上报，将不扣分；
5. 主要考核参演单位监测发现能力、应急处置能力、与公安机关配合能力。

绿盟科技版权所有

护网 2018 — 防守方减分规则

类型	分类	赋值	备注
获取权限	被获取终端计算机权限	10 分/台	累计不超过 200 分
	被获取Webhell权限	20 分/个，特别重要的附加 20 分	累计不超过 300 分
	被获取业务内网邮箱、FTP 应用、Web应用系统、数据库远程访问、互联网VPN接入系统的账号密码	普通权限 20 分/个 管理员 60 分/个 特别重要的，附加 60 分	同一设备两种权限扣分取高值，累计不超过 800 分
	被获取Web应用系统服务器、邮件服务器、数据库服务器等权限	普通权限 60 分/个 管理员 100 分/个 特别重要的，附加 100 分	两种权限扣分取高值，累计不超过 1200 分
	被获取域控服务器权限	管理员 300 分，特别重要的，附加 300 分	累计不超过 3000 分
	被获取路由器、交换机、防火墙等网络设备权限	接入层：50 分 汇聚层：100 分 特别重要的，附加 100-200 分	累计不超过 1000 分
	被获取其他设备权限	/	由裁判组核定

绿盟科技版权所有

护网 2018 — 防守方加分规则

工作阶段	得分标准	赋值	备注
发现攻击	发现木马攻击	50 分/个	得分累计不超过 500 分，提交拦截证据截图
	发现钓鱼邮件	20 分/个	得分累计不超过 200 分，提交分析报告和 eml 格式文件
	发现漏洞攻击	50 分/个	得分累计不超过 500 分，提交分析报告和攻击负载附件
	发现其他攻击（工控系统等）	/	由裁判组核定给分
消除威胁	处置 Webshell 木马或主机木马程序	50 分/个	得分累计不超过 500 分，提交分析报告，包括木马样本及分析报告、控制流量证据等
	处置 Web 系统、FTP 等异常新增账号，处置被爆破账号密码	20 分/个	得分累计不超过 200 分，提交分析报告，包括账号异常登陆源 IP、审计日志证据、异常登陆流量证据等。
	处置主机异常新增账号，处置被爆破账号密码	50 分/个	得分累计不超过 500 分，提交分析报告，包括账号异常登陆源 IP、系统审计日志证据、异常登陆流量证据等。
	消除其他威胁（工控系统等）	/	由裁判组核定给分
配合应急处置	积极配合应急组工作，根据线索能快速准确定位受害系统，能提供充分的日志记录，配合执法机关固定证据完成勘验	高效完成：+300 一般：+200 差：-100	最高 300 分，最低 -100 分

1.3

护网期间技巧

a. 防守方避免减分技巧

b. 防守方主动得分技巧

c. 防守方实用提示

绿盟科技内部版权所有

防守方避免减分技巧

技巧

- 非所属资产必须上诉；（合作企业资产带有单位 名称/logo，不再负责运营管理的资产等）
- 被判别为敏感数据但非数据库泄露的扣分项选择性上诉；
- 被判别为内网资产的扣分项，要求提供证明是我方资产；

要点

- 态度严谨
- 无确凿证据，拒不承认

绿盟科技版权所有

防守方主动得分技巧

- 技巧
  - ➢关注文件沙箱的告警日志，分析业务系统/邮箱流量获取的恶意样本；
  - ➢关注高危漏洞告警，如注入、命令执行、反序列化，系统提取等漏洞；
- 要点
  - ➢严格按照标准，提供充足证明

绿盟科技版权所有

防守方实用提示

- IP封禁是简单有效的防护方式；
- 内网资产监测与防护极为重要；
- 遇到国外地址进行攻击一律封禁，虽无法得分但具有真实防护效果；
- 沙箱设备能覆盖木马攻击和邮件攻击，建议设置专人专职进行样本分析；
- 提交报告需包含关键内容：源 IP，事件类型，流量分析（全流量），有样本需附上样本及分析报告，切忌只截设备告警图；
- 建立快速沟通渠道，避免耽误上报时间；

.....

绿盟科技版权所有

CONTENTS 目 录

绿盟科技版权所有

NSFOCUS

02

如何开展 护网工作

1. 护网工作整体流程及思路
2. 护网工作-备战阶段
3. 护网工作-临战阶段
4. 护网工作-决战阶段

绿盟科技版权所有

2.1

护网工作整体流程及思路

NSFOCUS

护网工作整体流程及思路

备战阶段	临战阶段	决战阶段	总结阶段
护网前2个月	护网前1个月	持续2周	护网结束
自查	预演	保障	总结
➢ 互联网暴露资产自查 ➢ 网络安全架构分析 ➢ 安全能力现状绘制 ➢ 护网保障资产梳理 ➢ 业务系统风险分析 ➢ 护网资产安全评估 ➢ 安全能力缺陷补充 ➢ 整体安全策略优化 ➢ 发现风险整改推进 ……	➢ 护网保障团队组建 ➢ 应急场景演练开展 ➢ 应急场景预案调整 ➢ 安全意识宣贯培训 ➢ 红蓝对抗攻防演练 ➢ 保障机制调整优化 ……	➢ 通告处置 ➢ 封堵封禁 ➢ 监控预警 ➢ 分析研判 ➢ 应急响应 ➢ 事件上报 ➢ 策略优化 ➢ 安全巡检 ……	➢ 攻击事件汇总梳理 ➢ 攻击路径还原分析 ➢ 安全缺陷整改跟进 ➢ 护网保障经验总结 ……

绿盟科技版权所有

NSFOCUS

2.2

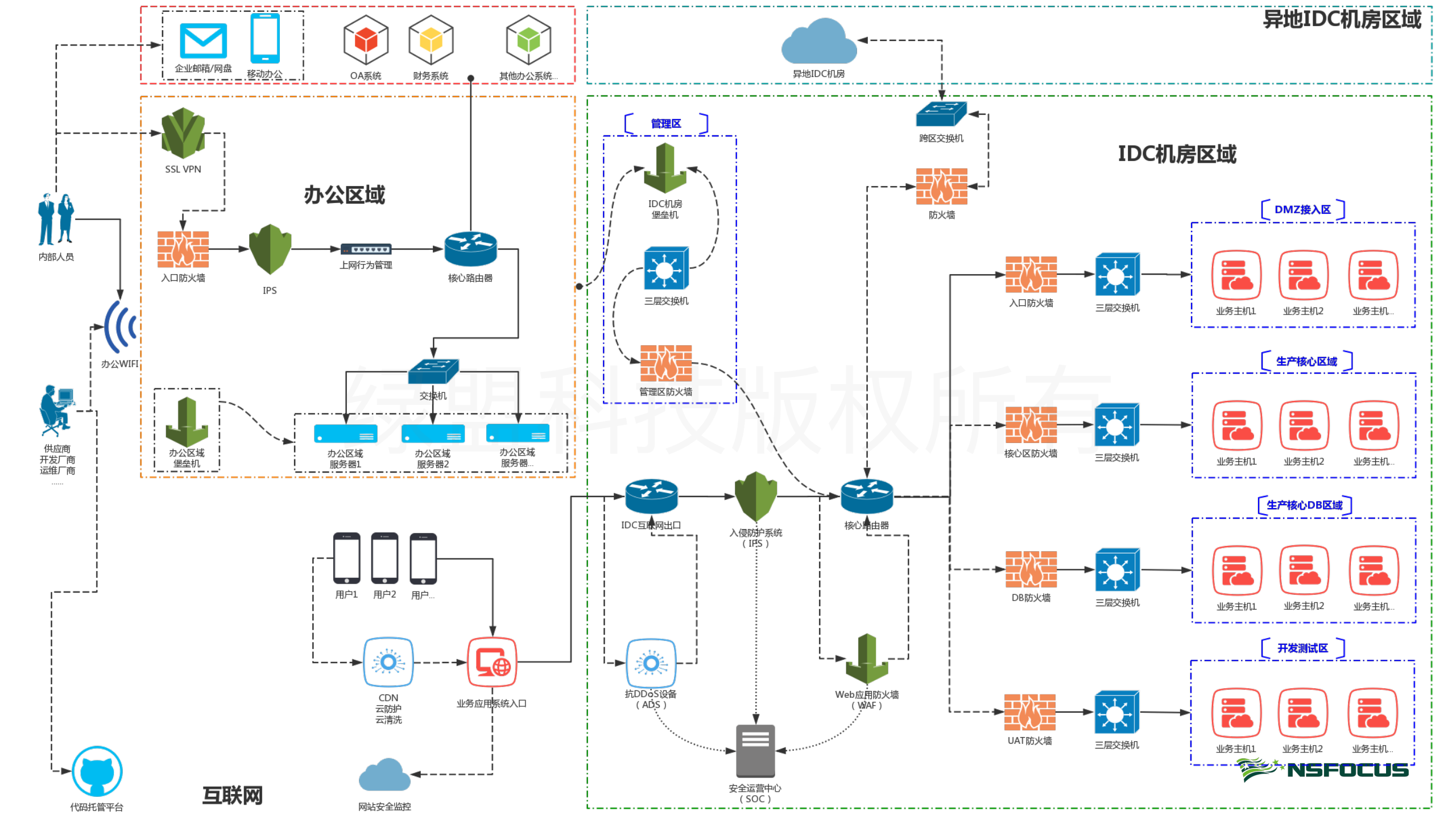
护网工作-备战阶段

NSFOCUS

护网工作-备战阶段

- 目的
  - 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
  - ……

绿盟科技版权所有


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机房区域
异地IDC机房
SSL VPN
办公区域
内部人员
入口防火墙
IPS
上网行为管理
核心路由器
办公WIFI
交换机
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...
供应商
开发厂商
运维厂商
.....
管理区
IDC机房
堡垒机
三层交换机
管理区防火墙
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
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
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
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
抗DDoS设备
（ADS）
Web应用防火墙
（WAF）
安全运营中心
（SOC）
用户1
用户2
用户...
CDN
云防护
云清洗
业务应用系统入口
网站安全监控
代码托管平台
互联网
NSFOCUS

2.3

护网工作-临战阶段

NSFOCUS

护网工作-临战阶段

- 目的
  - ➢建立护网保障机制
  - ➢熟悉应急响应流程
  - ➢提高内部安全意识
  - ➢检验护网保障能力
  - ➢磨合护网保障团队
  - ➢主动改进自身不足
  - ……

绿盟科技版权所有

2.4

护网工作-决战阶段

NSFOCUS

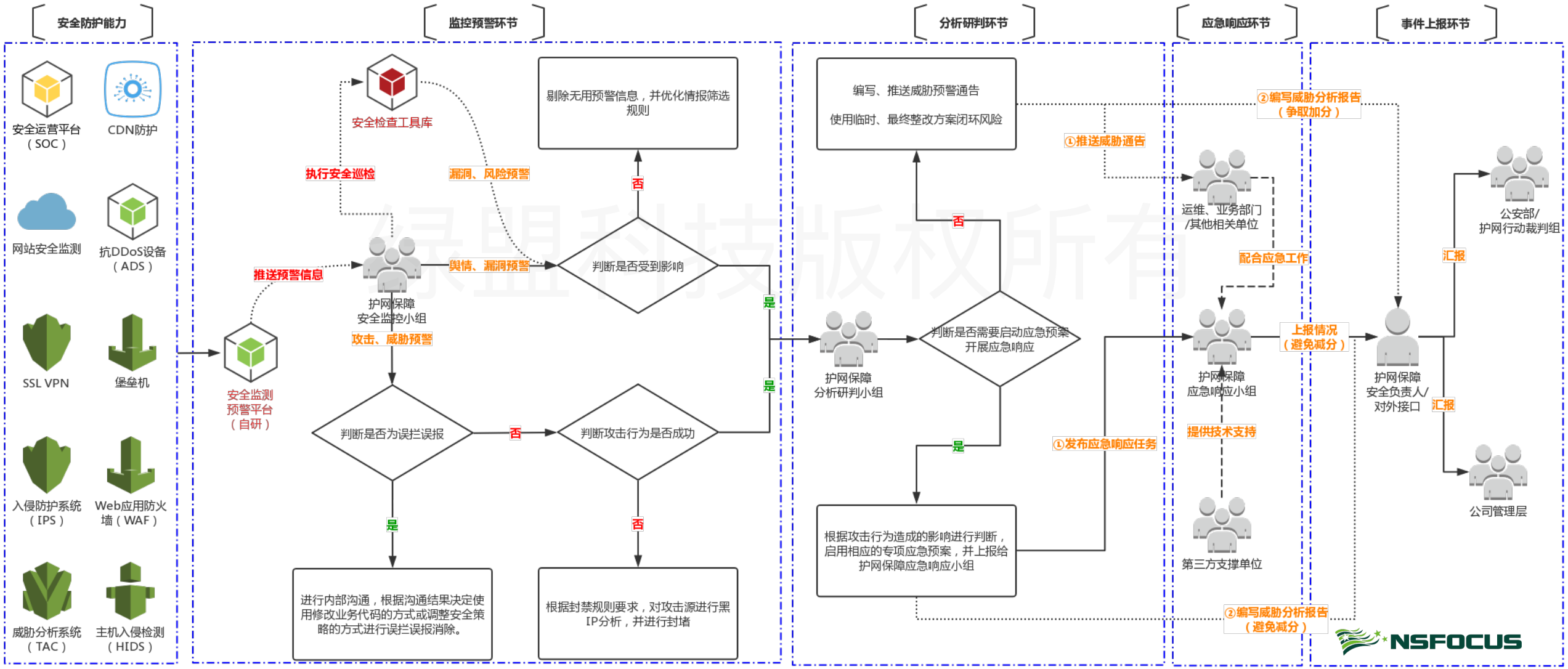
护网工作-决战阶段

- 目的
  - 避免非必要减分情况
  - 提前进行攻击拦截
  - 主动获取各项加分项
  - 及时控制安全风险

……

绿盟科技版权所有

护网工作-决战阶段


安全防护能力
监控预警环节
分析研判环节
应急响应环节
事件上报环节
安全运营平台（SOC）
CDN防护
网站安全监测
抗DDoS设备（ADS）
SSL VPN
堡垒机
入侵防护系统（IPS）
Web应用防火墙（WAF）
威胁分析系统（TAC）
主机入侵检测（HIDS）
安全检查工具库
执行安全巡检
漏洞、风险预警
剔除无用预警信息，并优化情报筛选规则
否
推送预警信息
舆情、漏洞预警
判断是否受到影响
是
护网保障安全监控小组
攻击、威胁预警
安全监测预警平台（自研）
判断是否为误拦误报
否
判断攻击行为是否成功
是
否
进行内部沟通，根据沟通结果决定使用修改业务代码的方式或调整安全策略的方式进行误拦误报消除。
根据封禁规则要求，对攻击源进行黑IP分析，并进行封堵
编写、推送威胁预警通告
使用临时、最终整改方案闭环风险
否
①推送威胁通告
护网保障分析研判小组
判断是否需要启动应急预案开展应急响应
是
①发布应急响应任务
根据攻击行为造成的影响进行判断，启用相应的专项应急预案，并上报给护网保障应急响应小组
②编写威胁分析报告（争取加分）
运维、业务部门/其他相关单位
配合应急工作
护网保障应急响应小组
提供技术支持
第三方支撑单位
上报情况（避免减分）
护网保障安全负责人/对外接口
汇报
公安部/护网行动裁判组
汇报
公司管理层
②编写威胁分析报告（避免减分）
NSFOCUS

2.4

护网工作-总结阶段

NSFOCUS

护网工作-总结阶段

- 目的
  - ➢闭环护网安全风险
  - ➢吸取护网经验教训
  - ➢备战后续护网保障
  - ……

绿盟科技版权所有

CONTENTS 目 录

绿盟科技版权所有

03

怎么进行护网保障

1. 护网保障经典案例

绿盟科技版权所有

3.1

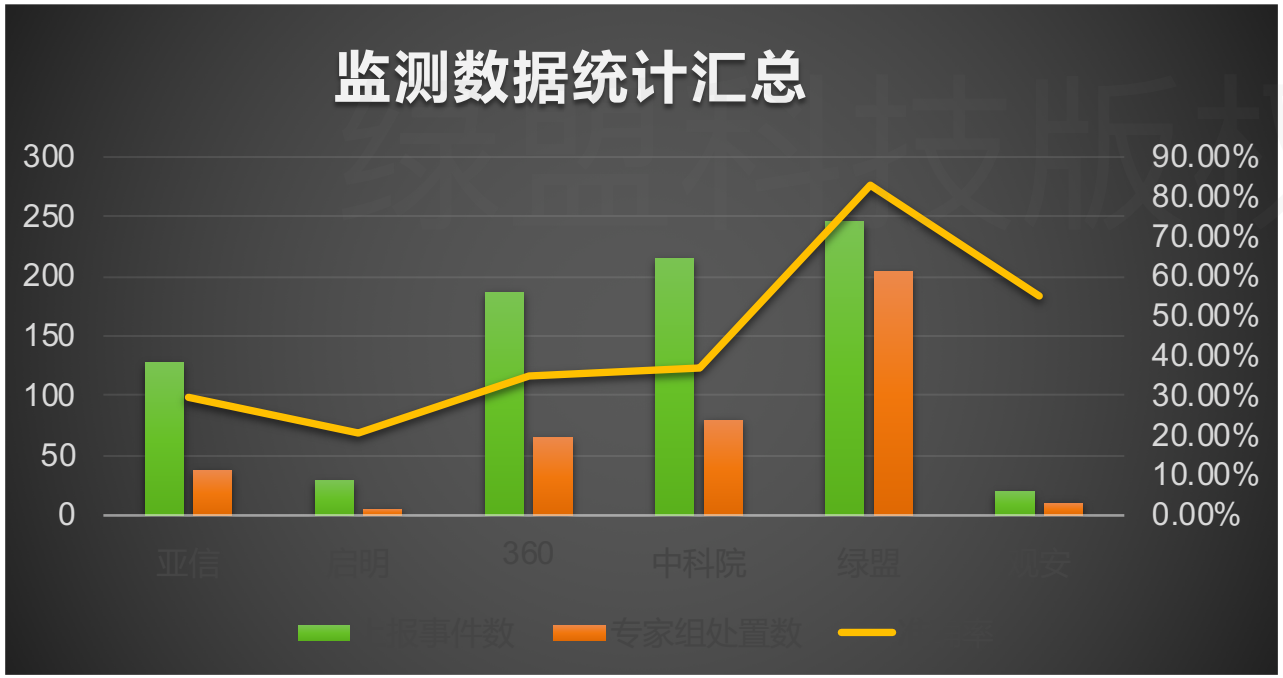
护网保障经典案例

绿盟科技版权所有

案例1：中国移动集团护网2018保障

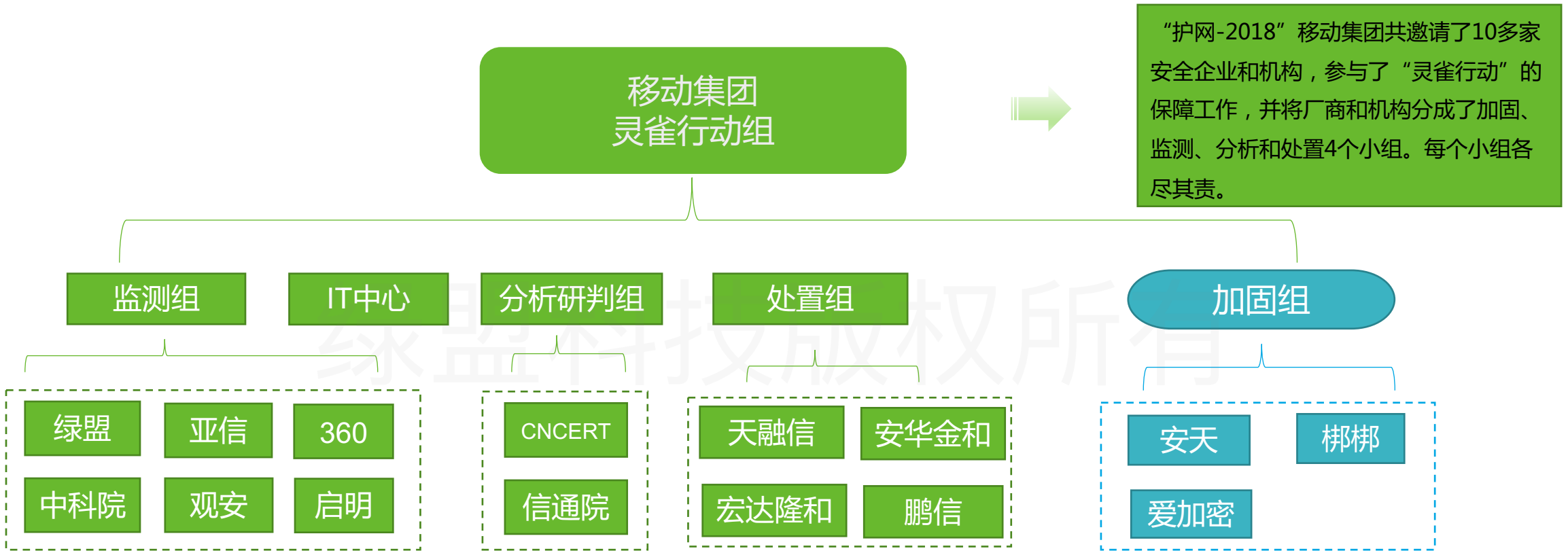
时间：2018年7 月 16 日至 27 日的**工作日**时间，9:00 到 17:00

在2018年公安部组织开展代号为 “护网-2018”的网络攻防演习中，中国移动代表通信行业第一次参加。绿盟做为支撑单位参加了移动集团的安全保障工作，得到了中国移动的高度认可。



事中阶段：提供7*24小时值守监控；告警事件的分析确认；提供处置建议
绿盟在监护期间，上报攻击事件数246个，被客户专家处置80个

移动集团护网参与厂商及角色分工



- 加固组做行动前的系统脆弱性检查，安全加固。
- 厂商监控组发现安全事件，按模板填写事件单，并按要求在规定时间上报至外部专家组进行研判。
- 外部专家组中获取事件单后，进行攻击行为判断,并向处置组下达处置任务。
- 厂商处置组根据专家组的判断结果实施IP封堵。

绿盟科技版权所有

移动集团护网2018分组职责

□ 加固组（系统脆弱性检查，安全加固）

安天、梆梆安全、爱加密对集团互联网暴露资产进行WEB安全漏洞、弱口令检测、APP安全加固。

□ 监测组（通过设备平台对攻击事件进行监测、并上报至分析研判组）：

绿盟：IPS、WAF、ESPC（企业安全管理平台）

启明：IPS、WAF；亚信：IPS、WAF

360：天眼；中科院：沙箱；观安：蜜罐

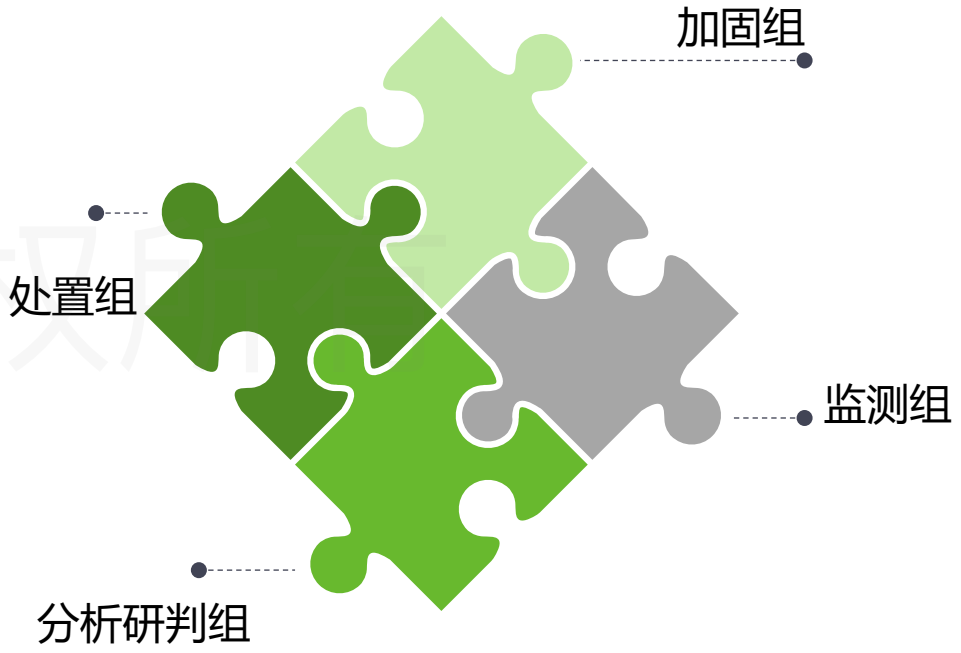
□ 分析研判组（攻击事件的分析研判，下达处置命令）

信通院、 CNCERT安全专家驻场，对集团、省公司监测发现的攻击事件进行研判，并将确认的攻击IP下发有处置组进行封堵。

□ 处置组（封堵IP）

鹏信：一键封堵（与防火墙联动）

天融信\宏达隆和\安华金和：防火墙IP封堵



绿盟科技版权所有

FAQ

绿盟科技版权所有

谢谢！

绿盟科技版权所有

NSFOCUS