
# 常态化攻防演练下的金融安全解决方案及实践

北京知道创宇信息技术股份有限公司

云安全解决方案部

张亮

# 目录
CONTENTS

# “国家级攻防演练”是一个命题作文

# “国家级网络安全攻防演练”的发展

“国家级网络安全攻防演练”组织国内安全攻防专家作为攻击队伍，采用“攻防实战演习”的方式，国有重要骨干企业和中管金融企业作为防守方，攻击方通过在防守方真实信息系统上模拟黑客进行网络攻击和渗透入侵的方式，全方位的检验防守方的网络安全管理、技术防护、应急响应的能力。

## “攻防演练”目标

### 目标一

- 从黑客（攻击者）的角度出发，帮助企业（防守方）发现和整改一批网络安全深层次问题隐患，提升关键信息基础设施安全保护能力

### 目标二

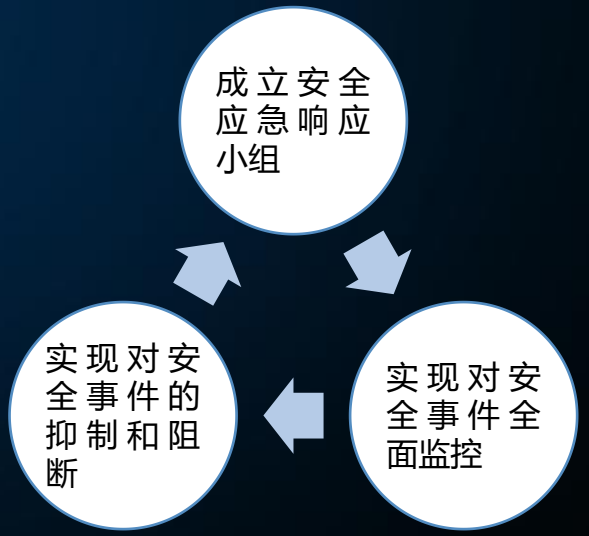
- 提升防守单位的网络安全工作协同作战、应急处置能力

### 目标三

- 提高防守单位全员的网络安全意识以及网络安全管理和执行团队的专业水平

## 对攻击方的要求


## 对防守方的要求



# 攻击特点：低烈度、受控的网络战

01

## 低烈度

1. 高级 0day 投入极少或没有（几乎不可能出现针对操作系统、通用路由设备、通用中间件和服务、密码算法等 0day）；
2. 一定量的应用和业务系统 0day，主要以 Web 系统和 APP 的 0day 为主；

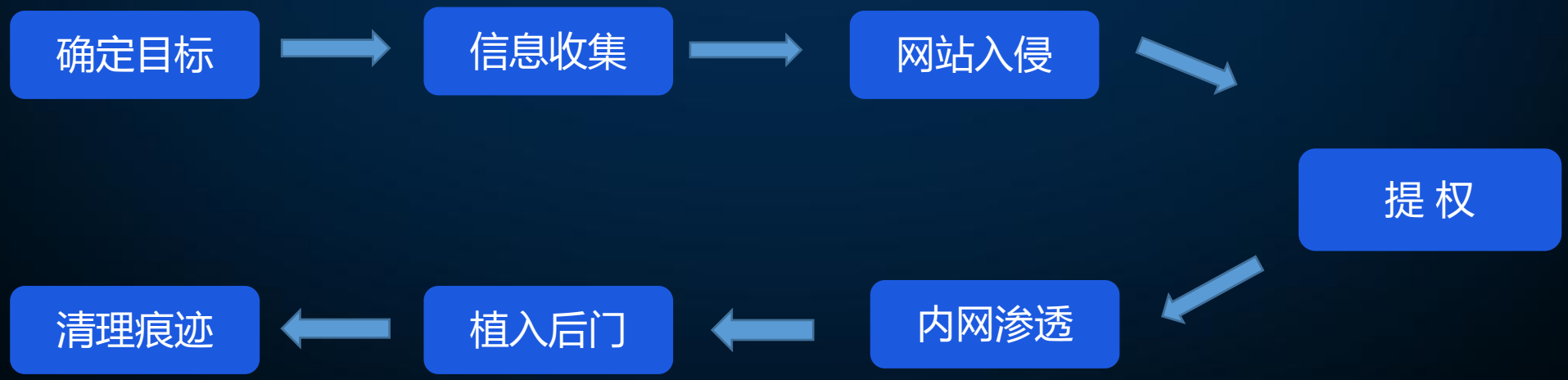
02

## 受 控

1. 不会对网络和系统进行破坏性攻击尝试（例如底层网络攻击、拒绝服务和重启等）；
2. 参与人员总数和攻击尝试时间有限；
3. 发起攻击的 IP 池有限；

# 攻击特点：具体攻击过程

目标选择→信息收集→子域名扫描→端口服务信息收集→主机漏洞扫描→ WEB漏洞扫描→漏洞利用→获取业务系统权限→业务系统getshell →服务器提权获取管理员权限→内网渗透→靶心攻击



# 1.信息收集阶段

信息收集是对目标资产的域名、IP、CDN、开放服务端口、邮箱等相关信息进行收集整理归纳，进而找到资产的暴露面。

哪些信息?

1.域名信息：whois、dns、子域名、注册人信息（邮箱、地址、电话、时间）、google hack

3.IP信息：端口、端口服务、C段、旁站

3.操作系统信息：类型（linux/windows/android/ios）、版本

4.应用信息：web、数据库、FTP、telnet、SMB等指纹信息（类型、版本、框架、中间件、程序诧言）

5.其他泄露的信息： 漏洞、github、cnvd、乌云镜像、微信/QQ、邮箱、社工库等互联网上曝光的信息

**安全风险：暴露面太广，可能存在的幽灵资产信息、泄露到互联网的信息被攻击队伍利用**

# 2.漏洞挖掘

漏洞挖掘是指通过对目标资产的暴露面进行不断的测试，找到可以利用的漏洞或脆弱点，进而入侵服务器。

安全漏洞的潜在范围：

- 操作系统安全漏洞
- 数据库安全漏洞
- Web应用系统安全漏洞
- Web框架及中间件安全漏洞
- 弱口令、信息泄露等导致的安全漏洞
- 安全防护产品安全漏洞

**安全风险：对己方安全漏洞的情况了解不足**

# 3.漏洞利用

**一般流程**

1.子域名扫描　(API/DNS/枚举三种方式，Subdomainsniper)

2.端口扫描　(1-65535 全端口扫描，Nmap/Smartscan)

3.主机漏洞扫描　(极光/Nessus)

4.弱口令扫描　(SSH/RDP/telne/ftp/redis/vnc/mysql/mssql/oracle/postgresql，Hydra)

**非常规手段**

5.Web漏洞扫描　(owasp top10 漏洞，Awvs)

6.Web弱口令爆破　(登录请求，Burpsuite)

1.RCE漏洞　(如：smb、rdp、seeyon、Weblogic、struts、cms、rmi等)

2.利用网络设备　(VPN) 弱口令、注入、未授权访问等控制VPN进入OA内网

**安全风险：防守方对安全漏洞潜在被利用的可能性未知**

# 4.渗透入侵

## 概念解析

在突破边界进入内网后，剩下的主要是内网渗透了。内网渗透可以简单分为**横向渗透**和**纵向渗透**。

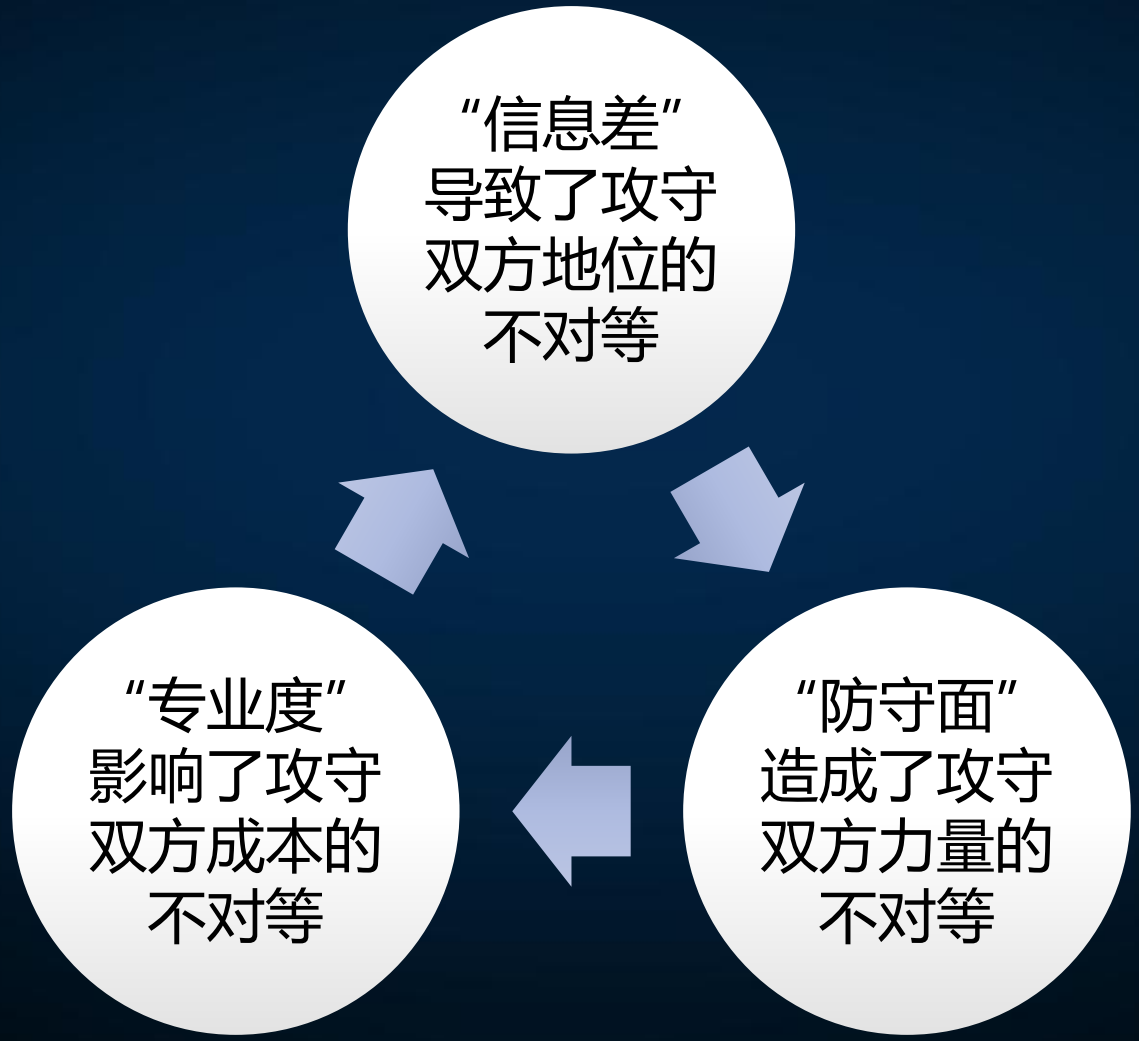
内网渗透的实质和关键是信息收集，通过不停的突破系统拿到更多的权限，而更多的权限带来更多的信息，最终在信息和权限的螺旋迭代下，拿到目标靶心的最高权限。

## 多据点潜伏

建立后门、不死马、远控、开放服务、创建隐藏账号

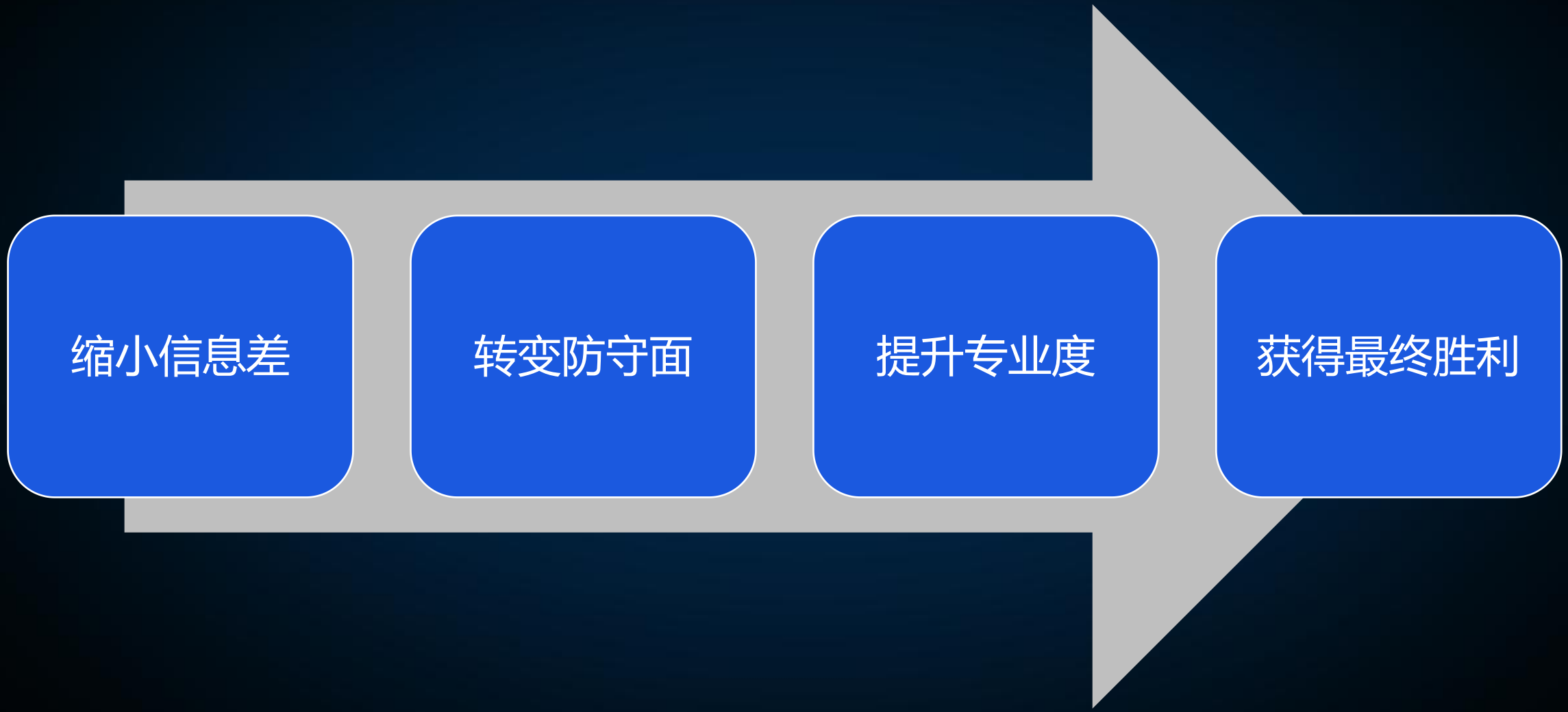
**安全风险：防守是面，渗透入侵是点，局部战场的失利威胁全局**

# “网络安全攻防演练”的本质



# 目录
CONTENTS

# 目标



# 具体思路

## 备战

- 清点资产
- 加固防线
- 埋伏防御工事
  - 第一道：云防御
  - 第二道：内网串联WAF
  - 第三道：旁路WAF、NTA、Ip封禁
  - 第四道：主机防御
- 布阵
  - 蜜网

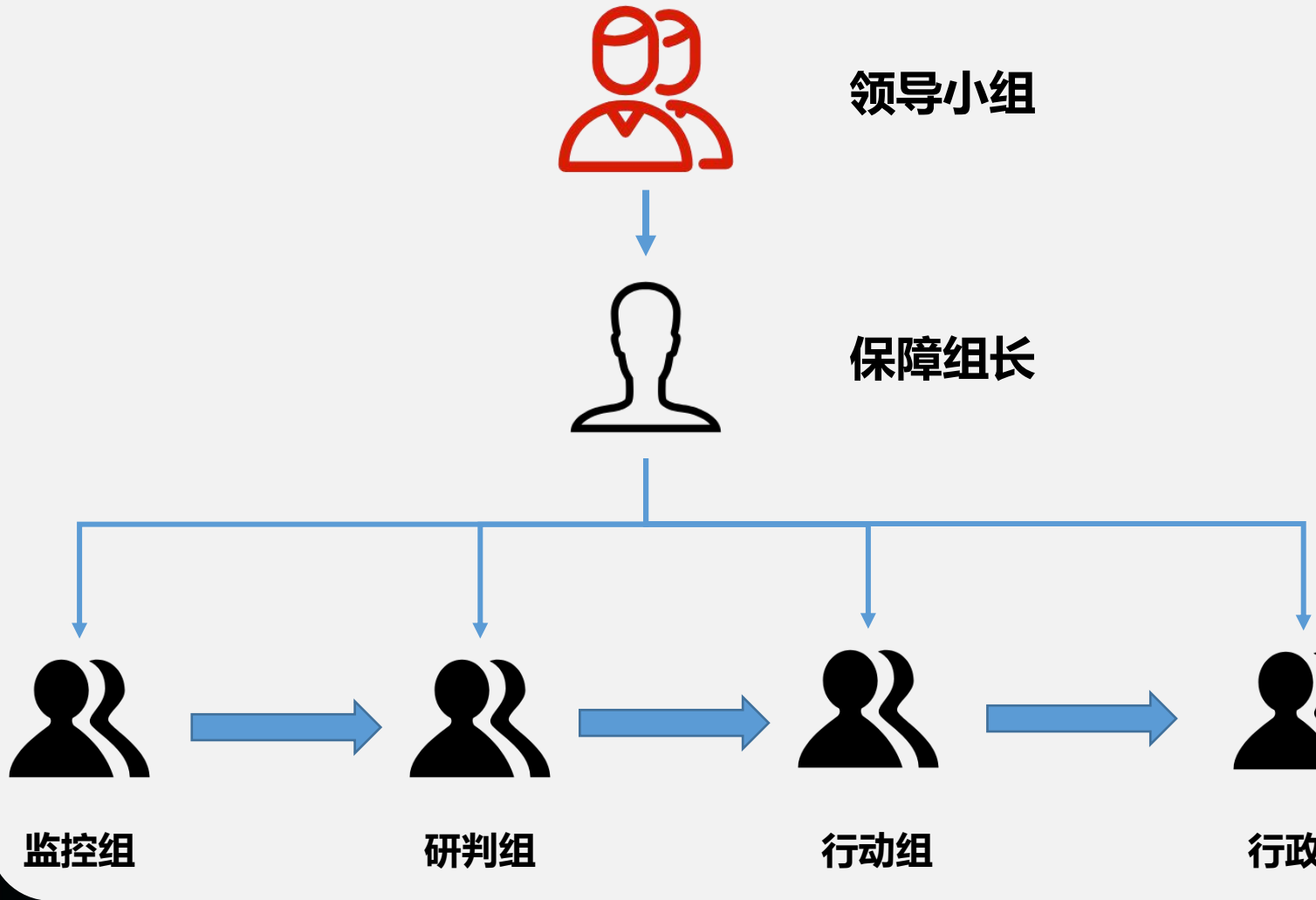
## 临战

- 模仿敌人演练
- 调整战法
- 完善战术细节
- 提升防御工事效果
  - 是否每一个攻击都可以被发现
  - 是否每一个防御设备都可以发现应该发现的攻击
- 熟练作战流程
- 应对对手心中有数

## 决战

- 设陷
  - 蜜罐
- 刺探
  - 水坑攻击
- 红衣大炮
  - IP封禁
- 应急堵漏
  - 漏洞应急
  - 漏报调整
- 战局监控
  - 态势监控
  - 战局分析
  - 溯源敌人
  - 事件报告
  - 沟通协调

# 组建团队




**领导小组：**重大事项决策、组织协调后勤、费用、法务等方面保障工作。

**行动组长：**组织落实攻防演练工作的方针政策，执行领导小组决议。组织编制攻防演练工作方案、工作计划、应急预案等相关文件。内设安全监控组、技术研判组、应急处置组、事件上报组，负责各项具体网络安全保障工作。

- 上报领导小组
- 组织内部自查

# 重要事项！！！

**内部：**

**组织全体职工召开动员会，明确“攻防演练”期间的行为守则：**

1. **警惕“钓鱼邮件”，应明确告知全员，不会在指定时间期间，要求安装或下载某些软件；收到疑似钓鱼邮件（不论是企业邮箱或个人邮箱）应及时向监控组报告；**
2. **严格管理移动存储介质及软件下载安装的行为，建议尽量提前报备或进行安全检测后使用；**
3. **警惕不明来历的电话、人员、快递等；**
4. **“攻防演练”期间，应尽可能减少系统变更行为，确需变更的话，需要提前报备并进行相应的安全检测。**
5. **在“攻防演练”期间在不影响业务正常开展的情况下，加强对外部合作伙伴的网络接入、接口接入的安全防护策略；**

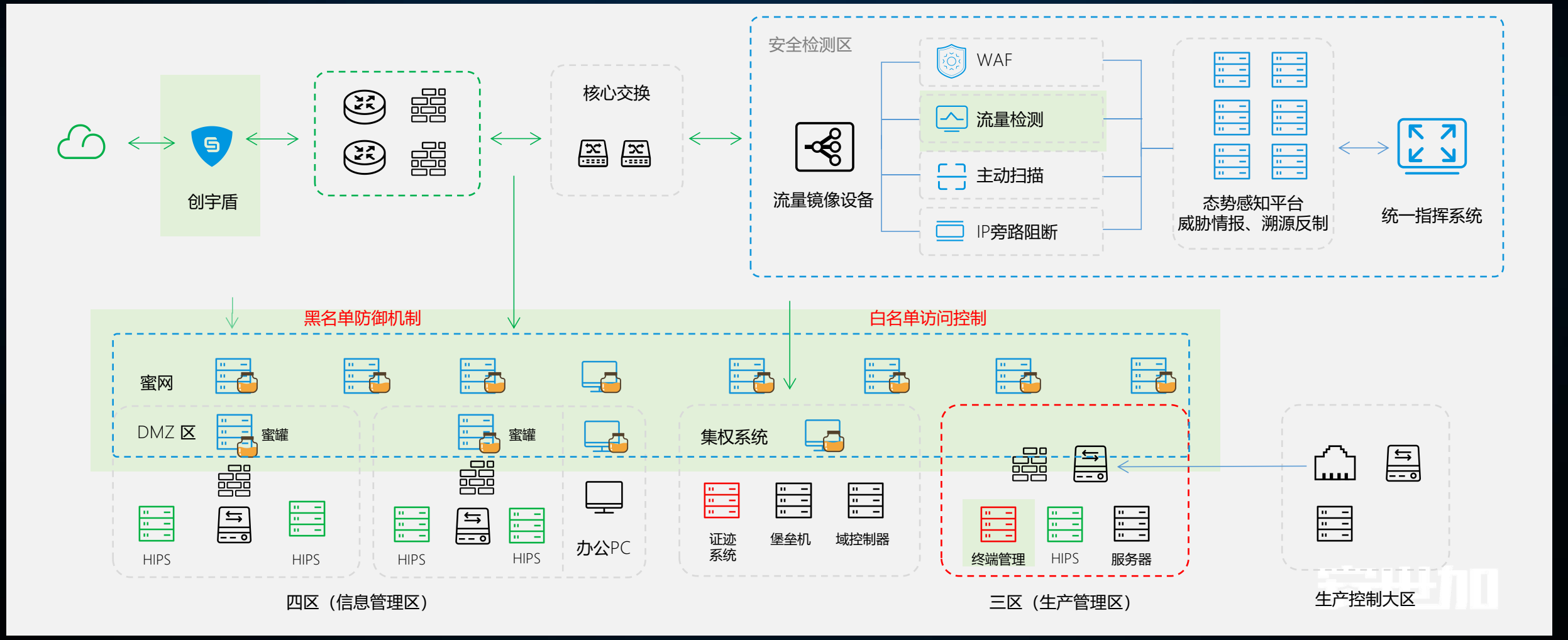
**外部：**

**告知相关利益方（如信息系统合作第三方、数据合作第三方或其他第三方供应商）：**

1. **在“攻防演练”期间，应做好自身的防护工作，应与安全部门的安全要求保持一致；**
2. **遇到可疑问题，应及时通知安全部门**

# 战前准备：构建纵深防御体系

构建多重交叉式防御体系，选择真正实战有效的能力，并不断优化，提高检出率和增强互补性，最终达到整体的安全防护保障。



# 备战阶段：资产及风险梳理（缩小信息差）

ZoomEye BE

**端口探测**

探测开放的端口和端口上运行的服务

**资产权重分配**

可根据资产重要性对资产划分等级

**可用性监测**

探测服务器运行状态是否活跃

| 安全状态 | 可用性 | 地址 | 站点名称 | 管理员 | 端口 | 权重 | 指纹信息 | 操作 |
|---|---|---|---|---|---|---|---|---|
| 高危 | 运行 | http://118.89.58.28 | 1day测试 | zhumengya | 2个端口 | 2 | 未知waf general purpose Linux | 查看 编辑 检测 |

**指纹识别**

识别资产的特征信息

## 资产梳理

结合实际环境，协助用户梳理企业资产，并将资产信息录入管理平台，进行统一管理。

## 指纹定制

根据用户实际资产情况，识别并记录企业资产特有指纹，使指纹信息与企业业务场景紧密贴合，更好的记录资产信息，丰富资产画像。

# 备战阶段：构建互联网统一防护体系（转变防守面）

**创宇盾：** **“防守利器”** Web应用安全攻击统一云防护平台。60S急速接入、隐藏源站IP、全球攻击行为快速识别及拦截，独创虚拟补丁技术，4小时内完成0day漏洞防御。安全运营服务团队7X24小时实时响应。

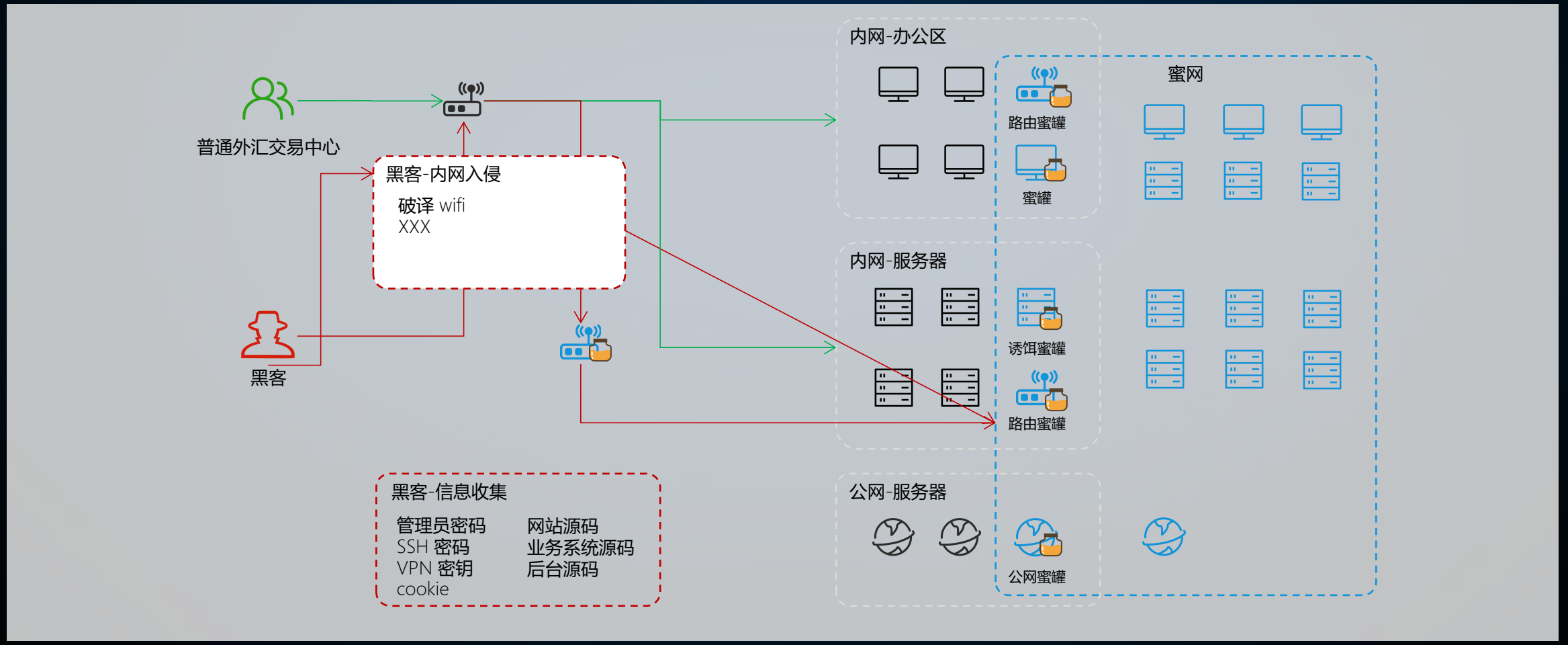

**军工级防护能力**
云端Web防护，安全、高效。

**异构兼容**
无需改动现有系统架构、无需修改源码。

**随需随用**
满足灵活的使用需求。

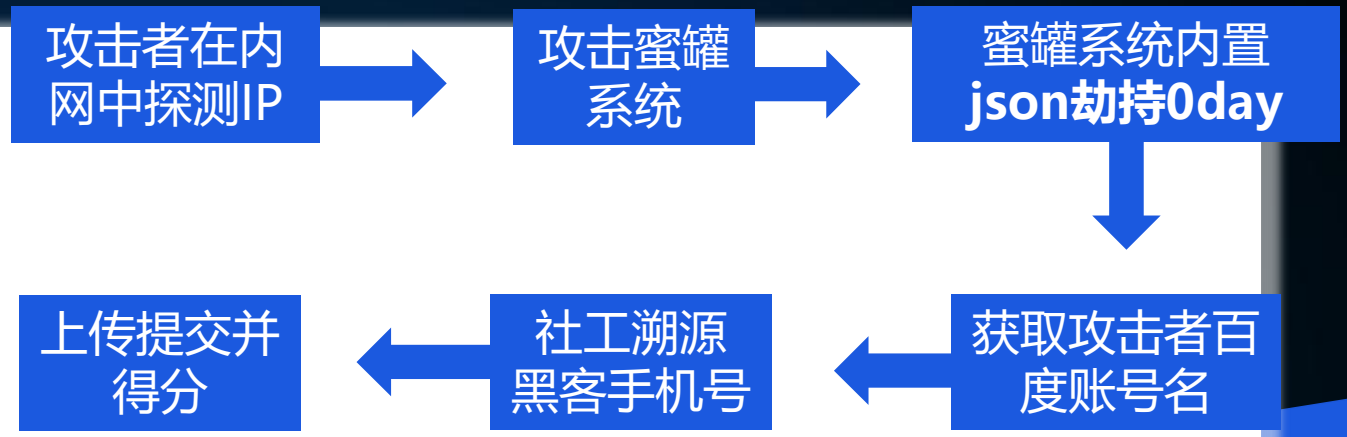
# 备战阶段：构建仿真网络（转变防守面）

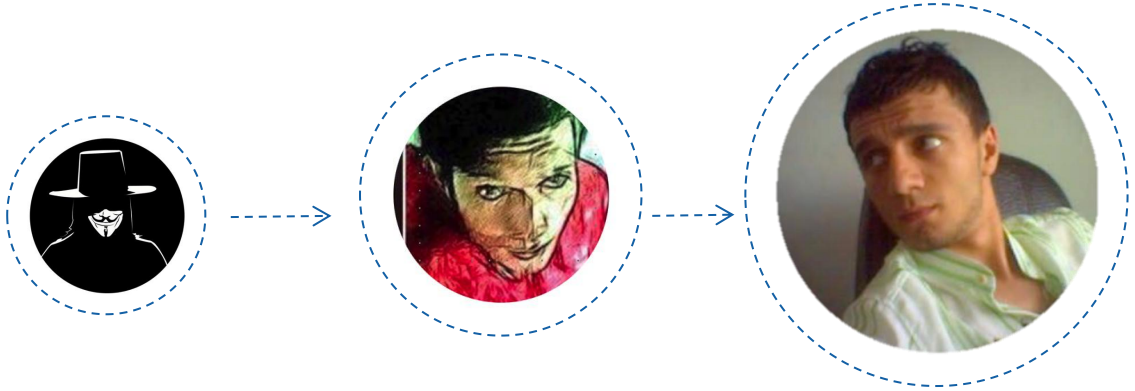
**猎风蜜罐**：基于“攻击欺骗”&“伪装欺骗”技术，在实际网络结构中通过部署大量伪装真实业务的蜜罐节点构建“蜜网”，诱导攻击队伍攻击蜜罐节点，并将攻击队伍流量和行为限制在蜜网中，从而快速准确发现攻击行为，并延缓攻击过程。



# 设陷案例：构建仿真网络（转变防守面）

在攻防演练中，攻击方的攻击路径和攻击手段变化莫测。此次攻击者在该金融机构的内网中探测IP时，被诱导进了蜜罐系统，猎风内置**国内最大搜索引擎json劫持0day**。在攻击者实施攻击的过程中我们获取到其百度账号用户名，并通过社工手段溯源其手机号，快速响应处置，解决攻击事件。



# 备战阶段：加强流量未知威胁分析能力（转变防守面）

**创宇云图**：多维度流量未知威胁检测能力，实时分析网络全流量，结合网络行为分析技术及威胁情报数据，深度检测所有可疑活动，分析文件行为，识别出未知威胁，构建针对攻击链的交叉检测交叉验证体系

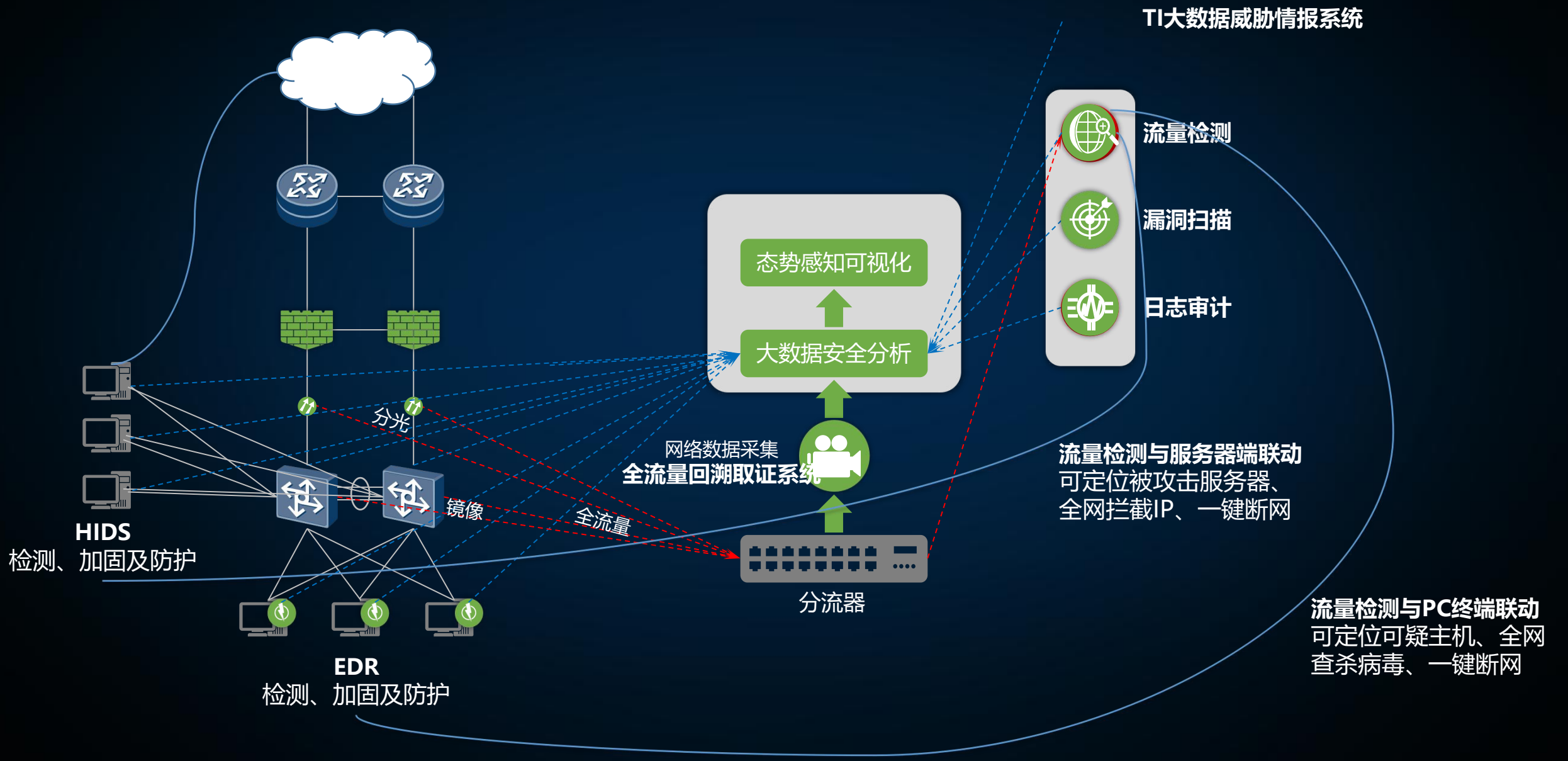
| | Kill Chain | 扫描探测 | 网络钓鱼 | 漏洞利用 | 木马下载 | 远程控制 | 横向渗透 | 行动收割 |
|---|---|---|---|---|---|---|---|---|
| 探针 | IDS | ✓ 网络特征检测 | | ✓ 网络特征检测 | | ✓ 网络特征检测 | ✓ 网络特征检测 | |
| | AV | | ✓ 已知威胁特征检测 | | ✓ 已知威胁特征检测 | | | |
| | NTA | ✓ 网络流量分析 | ✓ 网络流量分析 | ✓ 网络流量分析 | ✓ 网络流量分析 | ✓ 网络流量分析 | ✓ 网络流量分析 | ✓ 网络流量分析 |
| | NDR | ✓ 网络行为检测 | | ✓ 网络行为检测 | | ✓ 网络行为检测 | ✓ 网络行为检测 | ✓ 网络行为检测 |
| | Sand box | | ✓ 未知威胁行为检测 | | ✓ 未知威胁行为检测 | | | |
| | IOC | ✓ 入侵指标确认 | ✓ 入侵指标确认 | | ✓ 入侵指标确认 | ✓ 入侵指标确认 | | ✓ 入侵指标确认 |
| 平台 | TI | ✓ 威胁情报检测 | ✓ 威胁情报检测 | | ✓ 威胁情报检测 | ✓ 威胁情报检测 | | ✓ 威胁情报检测 |
| | Big Data | ✓ 大数据关联分析 | ✓ 大数据关联分析 | ✓ 大数据关联分析 | ✓ 大数据关联分析 | ✓ 大数据关联分析 | ✓ 大数据关联分析 | ✓ 大数据关联分析 |
| | AI | ✓ 人工智能检测分析 | ✓ 人工智能检测分析 | ✓ 人工智能检测分析 | ✓ 人工智能检测分析 | ✓ 人工智能检测分析 | ✓ 人工智能检测分析 | ✓ 人工智能检测分析 |

# 备战阶段：加强流量未知威胁分析能力（转变防守面）

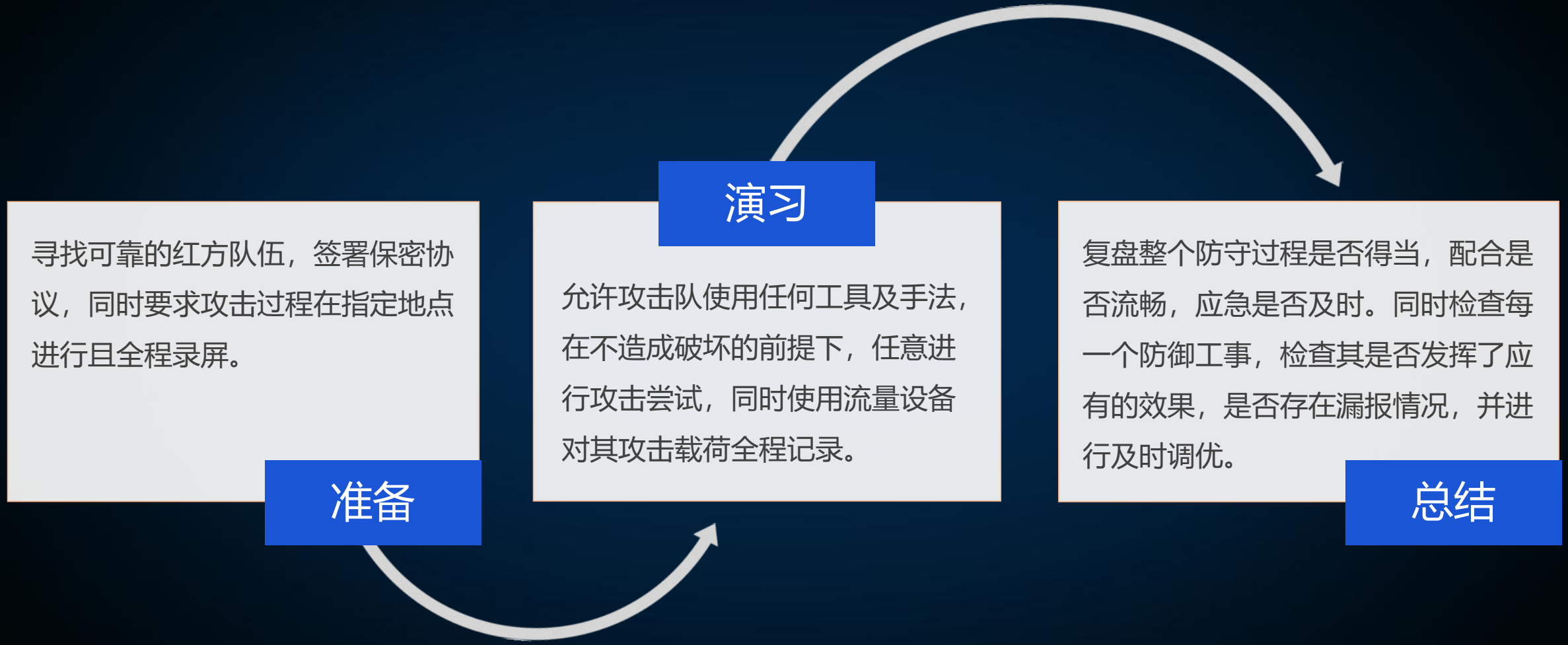
**创宇云图**：多维度流量未知威胁检测能力，实时分析网络全流量，结合网络行为分析技术及威胁情报数据，深度检测所有可疑活动，分析文件行为，识别出未知威胁，构建针对攻击链的交叉检测交叉验证体系

| 序号 | AI技术 | 应用 | 交叉验证准确率（%） |
|---|---|---|---|
| 1 | 文件基因图谱检测 | 采用基因图谱及深度学习模型检测恶意代码变种 | 97.77% |
| 2 | 流量基因图谱检测 | 采用基因图谱及深度学习模型检测未知协议恶意流量 | 98.12% |
| 3 | 加密流量检测 | 采用机器学习模型检测恶意程序加密通信行为 | 98.23% |
| 4 | 暗网流量检测 | 采用步态指纹及深度学习模型检测暗网（Tor）通信行为 | 99.12% |
| 5 | Shadow socks流量检测 | 采用步态指纹及深度学习模型检测Shadowsocks流量 | 96.54% |
| 6 | VPN流量检测 | 采用步态指纹及深度学习模型检测VPN流量 | 96.33% |
| 7 | DNS隐蔽隧道检测 | 采用机器学习模型检测DNS隐蔽隧道外发数据的行为 | 99.83% |
| 8 | ICMP隐蔽隧道检测 | 采用机器学习模型检测ICMP隐蔽隧道外发数据的行为 | 97.45% |
| 9 | HTTP隐蔽隧道检测 | 采用机器学习模型检测HTTP隐蔽隧道外发数据的行为 | 96.18% |
| 10 | HTTPS隐蔽隧道检测 | 采用机器学习模型检测HTTPS隐蔽隧道外发数据的行为 | 95.21% |
| 11 | 沙箱恶意行为模式库构建 | 采用频繁项集挖掘算法构建沙箱恶意行为模式库 | 不涉及 |
| 12 | DGA域名检测 | 采用多个深度学习模型交叉检测Fast-Flux僵尸主机 | 98.94% |
| 13 | WebShell网站后门检测 | 采用深度学习及强化学习模型检测WebShell | 96.20% |
| 14 | SQL注入攻击检测 | 采用深度学习及强化学习模型检测SQL注入攻击 | 96.89% |
| 15 | XSS跨站脚本攻击检测 | 采用深度学习及强化学习模型检测XSS攻击 | 96.11% |

# 备战阶段：联防联控（转变防守面）



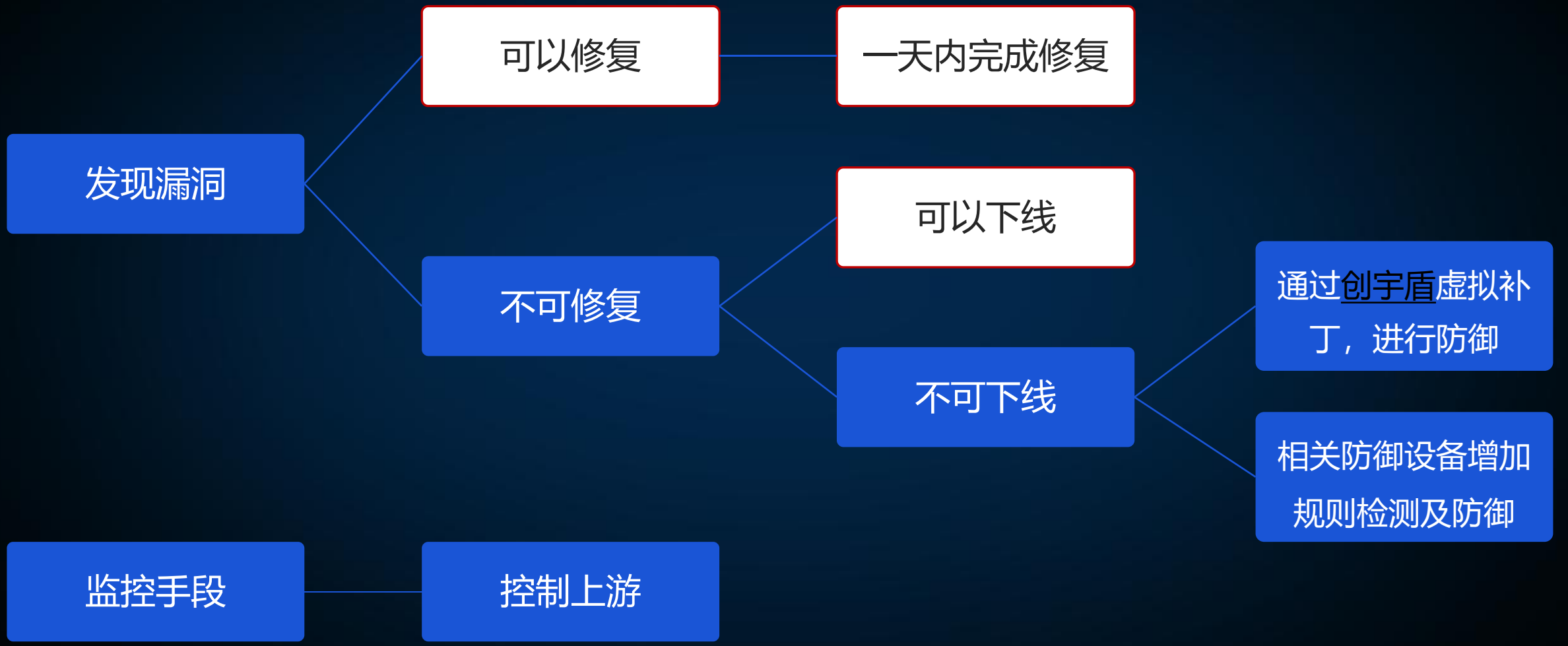
# 临战阶段：安全攻防演练（提升专业度）



# 决战阶段：实时防御（提升专业度）

| | |
|---|---|
| 防御思路 | 攻击 IP 是核心资源，大多数攻击者使用VPS （基本在美国和东南亚），资源更加有限。将攻击 IP 尽可能消耗殆尽后，逼迫攻击者更换攻击目标或者使用真实 IP。 |
| 措施 | 1. 通过云防御系统、互联网漏洞平台、内网蜜罐系统、水坑攻击系统等收集攻击者IP并形成攻击者档案库。<br>2. 将攻击者档案库收集的攻击者 IP（百万级别）放到各网关防御系统进行直接封禁。<br>3. 通过流量检测设备发现的攻击者 IP 直接进行旁路阻断。<br>4. 成立专门的黑名单管理组，动态将黑名单 IP 同步到各防御系统。 |

# 决战阶段：应急响应（提升专业度）



# 决战阶段：全面监控（提升专业度）

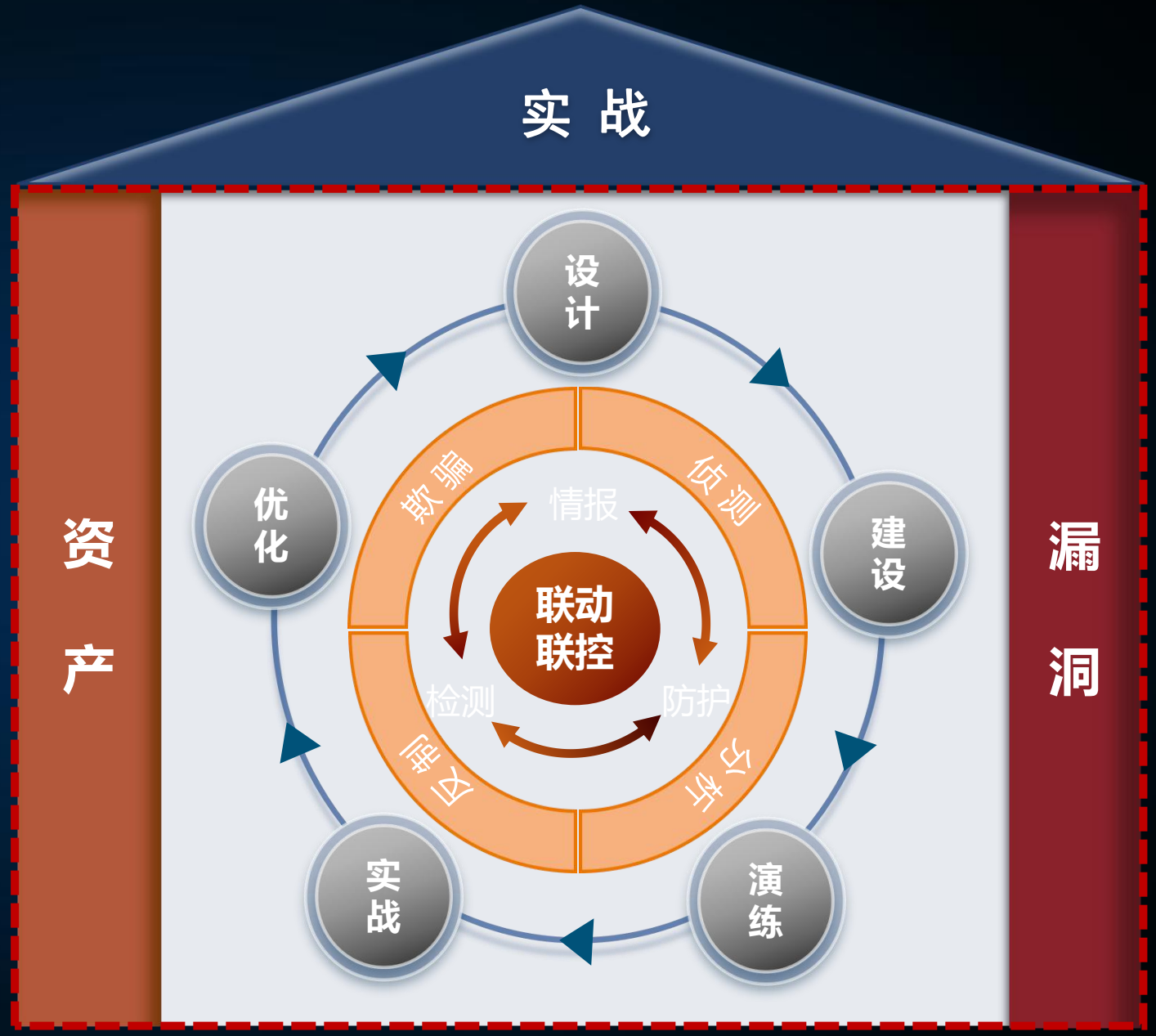
**通过**ZoomEye BE**完成内网和互联网资产的发现、安全漏洞识别等风险的识别**

# 战后：总结反思（提升专业度）

总结本次“攻防演练”专项行动的成果与较好做法，将相关工作固化至规章制度中，形成常态化、制度化成果。根据演习中发现的相关问题，举一反三，做好后续相应防范工作，形成总结报告。


# 实战化服务体系架构

- 基于一个目标：实战；
- 盯紧两个核心要素：资产和漏洞；
- 构建三位一体的协同联动：情报、 检测、防护；
- 依托四核心能力打造新时代安全观：侦测、欺骗、分析、反制；
- 通过五步走构建常态化防御体系： 设计、建设、演练、实战、优化。



# 目录
CONTENTS

# 典型案例

中国建设银行
China Construction Bank

UnionPay 银联 中国银联
China UnionPay

中信建投证券股份有限公司
CHINA SECURITIES CO., LTD.

中国交建
CHINA COMMUNICATIONS CONSTRUCTION

中国南方电网
CHINA SOUTHERN POWER GRID

中国一汽

知道创宇

# 安全，是我们不变的信仰

【邮　箱】：jjfa@knownsec.com
【网　址】：https://www.yunaq.com
【地　址】：北京市朝阳区望京SOHOT3 A座15层