SILENCE
INFORMATION TECHNOLOGY
无声信息

以攻助防，积极防御

为你的防护加上攻击者的眼睛

四川无声信息技术有限公司——何鹏程

自我介绍

白帽子

四川无声信息技术有限公司副总监
无声双螺旋攻防研究院院长
CNVD官方白帽子
提交CNVD漏洞100余个
提交CVE漏洞14个

研究方向：渗透测试、漏洞挖掘、APT攻击、白盒审计、追踪溯源、安全研发

S I L E N C E

I N F O R M A T I O N T E C H N O L O G Y

PART 1

关于无声

PART 2

传统防护理念

PART 3

以攻构防的理念

01
关于无声

发展历程

成立

2000年7月27日

成长

2005年，领跑西南IT安全市场

变革

2013年，信息安全服务提供商

提升

2016年，无声技术服务体系

发展

2018年

分支机构

用户分布-已覆盖

用户分布-未覆盖

四川无声	无声信息(总部)
北京无声	北京无声信息 (北京)
重庆无声	重庆无声信息(重庆)
西藏无声	无声西藏运营中心(拉萨)
西北无声	无声西北五省运营中心(西安)

人员结构

220+

员工总数

161

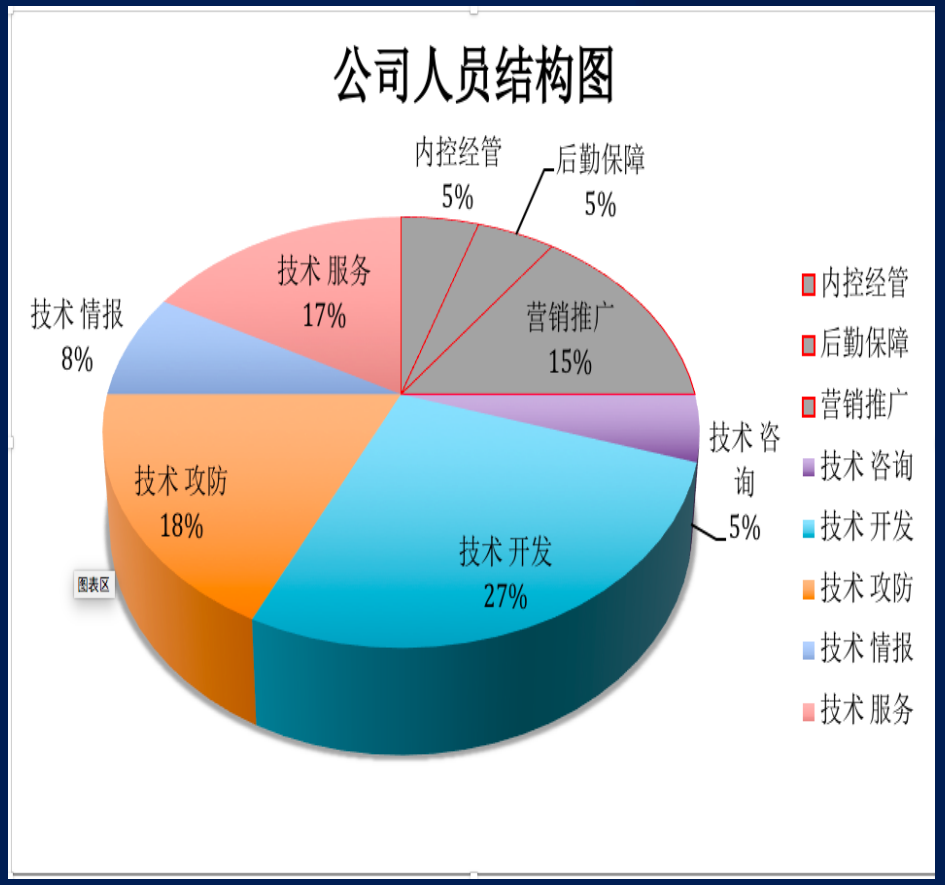
985、211 博士/硕士/本科

本科及以上学历73%

166

技术团队 75%

ISO27001/ISO20000/
CISP/SISSP/白客



服务资质

安全集成服务资质


ISCCC
信息安全服务资质认证证书
证书编号：ISCCC-2012-ISV-SI-020
兹证明
四川无声信息技术有限公司
的信息系统安全集成服务资质符合
ISCCC-SV-001:2015《信息安全服务资质认证实施规则》
二级服务资质要求。
注册地址：成都市高新区芳草东街76号
受审核地址：成都市高新区府城大道西段399号天府新谷园区5号楼802
颁证日期：2015年11月23日　证书需每年接受监审，无监审标志证书无效。
初次认证：2012年3月31日
ISCCC　CNAS C066-V　魏吴
中国信息安全认证中心
中国·北京·朝外大街甲10号（100020）　www.isccc.gov.cn

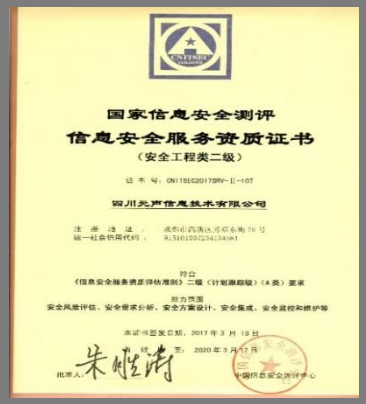
风险评估服务资质


ISCCC
信息安全服务资质认证证书
证书编号：ISCCC-2015-ISV-RA-133
兹证明
四川无声信息技术有限公司
的信息安全风险评估服务资质符合
ISCCC-SV-001:2015《信息安全服务资质认证实施规则》
二级服务资质要求。
注册地址：成都市高新区芳草东街76号
受审核地址：成都市高新区府城大道西段399号天府新谷园区5号楼802
颁证日期：2015年11月23日　证书需每年接受监审，无监审标志证书无效。
ISCCC　CNAS C066-V　魏吴
中国信息安全认证中心
中国·北京·朝外大街甲10号（100020）　www.isccc.gov.cn

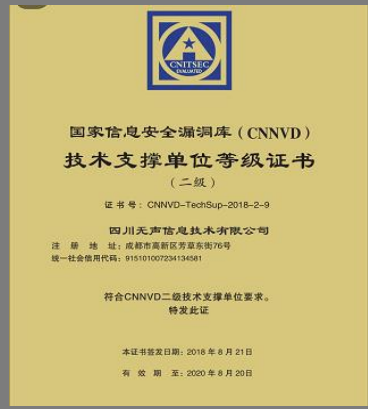
应急处理服务资质


ISCCC
信息安全服务资质认证证书
证书编号：ISCCC-2015-ISV-ER-081
兹证明
四川无声信息技术有限公司
的信息安全应急处理服务资质符合
ISCCC-SV-001:2015《信息安全服务资质认证实施规则》
二级服务资质要求。
注册地址：成都市高新区芳草东街76号
受审核地址：成都市高新区府城大道西段399号天府新谷园区5号楼802
颁证日期：2015年11月23日　证书需每年接受监审，无监审标志证书无效。
ISCCC　CNAS C066-V　魏吴
中国信息安全认证中心
中国·北京·朝外大街甲10号（100020）　www.isccc.gov.cn

安全工程资质


国家信息安全测评
信息安全服务资质证书
（安全工程类二级）
证书号：CNITSEC2017SV-E-107
四川无声信息技术有限公司
注册地址：成都市高新区芳草东街76号
统一社会信用代码：91510100723413458I
符合
《信息安全服务资质评估准则》二级（计划调整后）（A类）要求
能力范围
安全风险评估、安全需求分析、安全方案设计、安全集成、安全监控和维护等
本证书签发日期：2017年3月18日　有效期至：2020年3月17日
批准人：朱艳涛　中国信息安全测评中心

CNNVD技术支撑单位


国家信息安全漏洞库（CNNVD）
技术支撑单位等级证书
（二级）
证书号：CNNVD-TechSup-2018-2-9
四川无声信息技术有限公司
注册地址：成都市高新区芳草东街76号
统一社会信用代码：91510100723413458I
符合CNNVD二级技术支撑单位要求。
特发此证
本证书签发日期：2018年8月21日
有效期至：2020年8月20日

质量管理体系认证


CERTIFICATE
质量管理体系认证证书
四川无声信息技术有限公司
GB/T 19001-2008/ISO 9001:2008
《质量管理体系 要求》
CQM　IAF　CNAS

软件开发资质 CMMI 3


Certificate of Achievement
This is to acknowledge
四川无声信息技术有限公司
has successfully achieved
Maturity Level 3 against the CMMI® for Development (v1.3)
using the SCAMPI (v1.3) Appraisal Method
SCAMPI Appraisal System ID: 30978
CMMI Institute Partner
Issue Date: Nov 4, 2017
Expiry Date: Nov 4, 2020

涉密集成资质（甲级）


涉密信息系统集成
资质证书
（副本）
单位名称：四川无声信息技术有限公司
法定代表人：黄勇
单位地址：成都市高新区芳草东街76号
年审记录：
编号：JC2331602556
资质等级：甲级
业务种类：软件开发
通用地域：全国
有效期至：2019年09月21日
2016年09月22日

武器装备科研生产单位保密（二级）


武器装备科研生产单位
二级保密资格证书
（副本）
单位名称：四川无声信息技术有限公司
注册地址：成都市高新区芳草东街76号
法定代表人：黄勇
编号：SCH1704
有效期至：2022年8月10日

军事信息网络安全防护技术支撑单位


SILENCE
军事信息网络安全防护支撑申请书
申请单位：
申请日期：
中央军委联合参谋部信息通信局制

服务资质

省级应急支撑单位

国家信息安全通报支撑单位

成都网络安全处置中心

省信息安全重点培育企业

中国网络安全协会

中国互联网网络安全威胁治理联盟

中国通信网络安全服务资质

军民融合企业

双螺旋安全研究院

双螺旋安全研究院汇聚了来自国内多个领域的信息安全专家，是一个信息安全多向发展的团队，**是国内顶尖的攻防团队**，双螺旋攻防研究院秉承着"攻防交织，以攻构防"的理念与国内多家企业安全部门、国内安全职能部门等都有合作。该团队以渗透测试为主要核心，浏览器前端安全、代码审计、漏洞挖掘、安全软件开发等为主要研究项目，曾多次为腾讯、新浪、淘宝/支付宝、百度、360、京东、各大政务、银行、企事业单位提供安全支持服务，披露过众多有影响力的安全漏洞。

- 渗透测试
- 前端安全
- 数据挖掘
- 逆向工程
- 威胁情报
- 安全软件

双螺旋研究院

DOUBLE-HELIX INSTITUTE

30+

团队所获奖项


3000+ teams 48hours
Web-1st China-1st World-8th
0ops（0CTF）国际信息安全技术挑战赛
2016/2017贵阳大数据与网络安全攻防演练大赛
全国
安全突破奖
1st
第二届“强网杯“全国网络安全挑战赛（2018）
2600+ teams 48hours
全国 Web-1st 三等奖
CNCERT2016网络安全技术对抗赛
CNCERT
攻击总成绩 1st
2nd

攻防对抗测试

阿里红蓝对抗测试

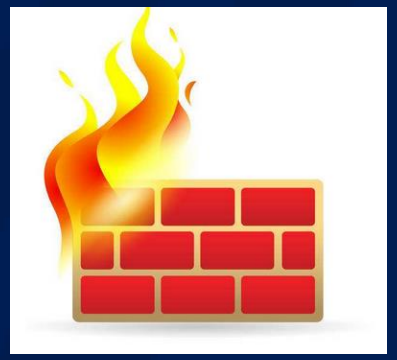
通杀阿里云

腾讯红蓝对抗测试

漫游腾讯内网

02
传统防护理念

个体单位眼中的安全防护



防火墙

+

IDS

+

IPS

WAF

+

安全审计

+

漏洞扫描器

……

监管部门眼中的安全防护

传统的安全监测


路由器


防火墙


交换机


服务器


数据库

网络设备/信息系统

网站/业务应用系统

可用性

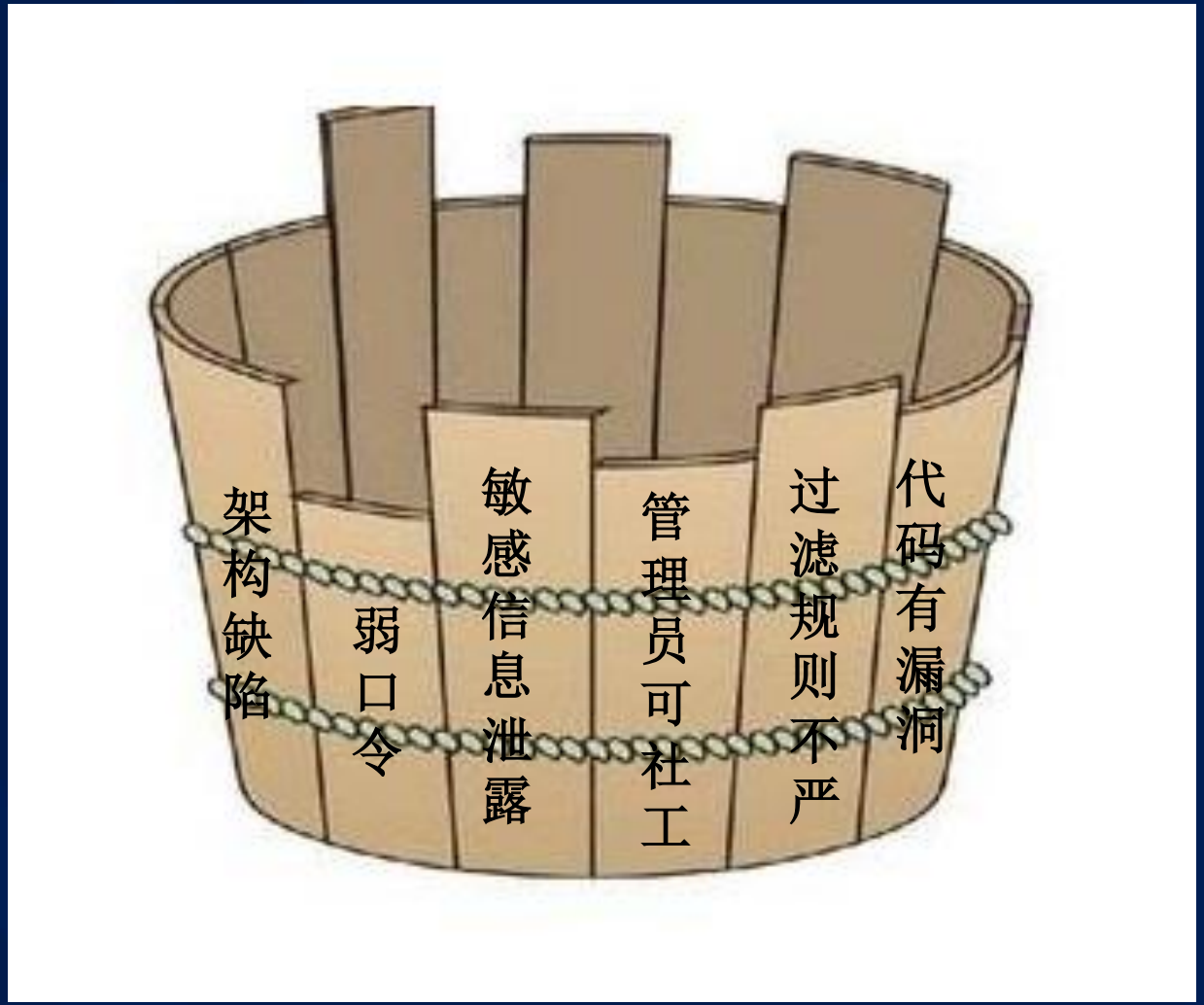
脆弱性

合规性

网络威胁

使用最先进的技术和设备，7X24小时不间断监测，为何还是有攻击事件发生？

攻击者眼中的安全防护



不求突破最强的防护

只求寻找最弱的一环

传统防护的局限

1.容错率低，监测范围无法覆盖完全

2.基于已知的规则，对未知威胁防护能力较差

3.逻辑类漏洞和问题无法做到全面检测

4.人为和社工因素造成的威胁难以预防

既然攻击是一个需要人工干预的行为，那么防御也不可能做到完全自动化

03
以攻构防的理念

“以攻构防”的核心理念

- 防火墙
- 入侵检测
- 防病毒
- 安全审计

传统安全防御体系模式固化

以攻助防
以攻促防
以攻验防

“以攻构防”思想的雏形——渗透测试

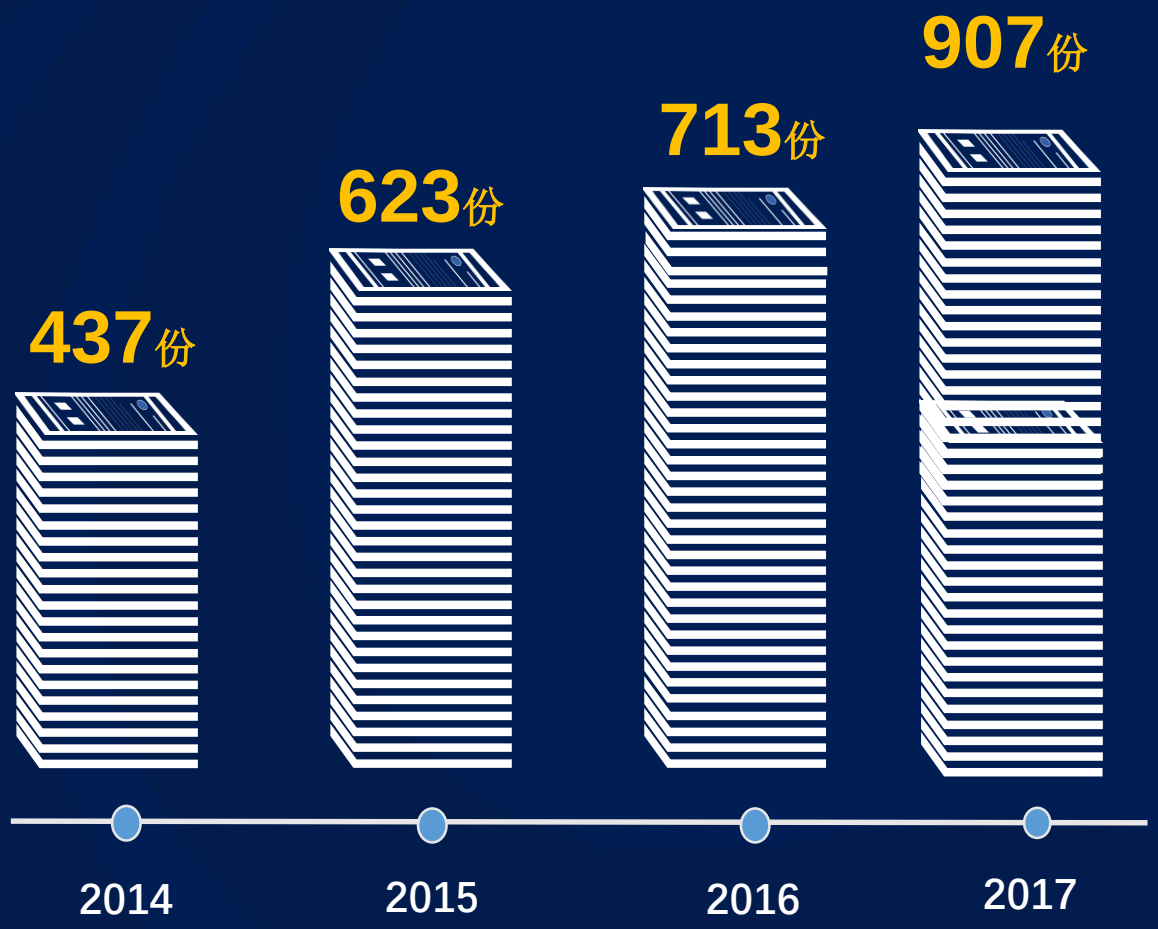
渗透测试是通过**模拟恶意黑客**的攻击方法，来评估计算机网络系统安全的一种评估方法，渗透人员在不同的位置（比如从内网、从外网等位置）利用各种手段对某个特定网络进行测试，以期**发现和挖掘系统中存在的漏洞**，然后输出渗透测试报告，并提交给网络所有者。网络所有者根据渗透人员提供的渗透测试报告，可以清晰知晓系统中存在的**安全隐患和问题**。

渗透测试的两大特点：

1.渗透测试是一个**渐进的并且逐步深入**的过程

2.渗透测试是选择**不影响业务系统正常运行**的攻击方法进行的测试

无声提供的渗透测试服务



渗透测试报告

自2014年1月至2017年12月双螺旋团队共为用户单位测试出具各类网站/系统/应用的【渗透测试报告】**2680**份。

“以攻构防”思想的进阶——网络靶场

网络靶场是指通过虚拟环境与真实设备相结合，**模拟仿真**出真实网络空间攻防作战环境，能够支撑网络空间作战能力研究和网络空间武器装备验证试验平台。

V1.0 ——CTF解题模式　　V2.0——AWD攻防模式
V3.0——仿真城市靶场

核心问题没有得到解决：
1.网络空间对抗不止是人与关键基础设施的对抗，更是**人与人**之间的对抗，真正的攻击夹杂着很多**社工和情报分析元素**，仿真效果再好也跟真实环境有很大的出入。
2.面对**未知架构和未知威胁**，无法模拟和仿真。

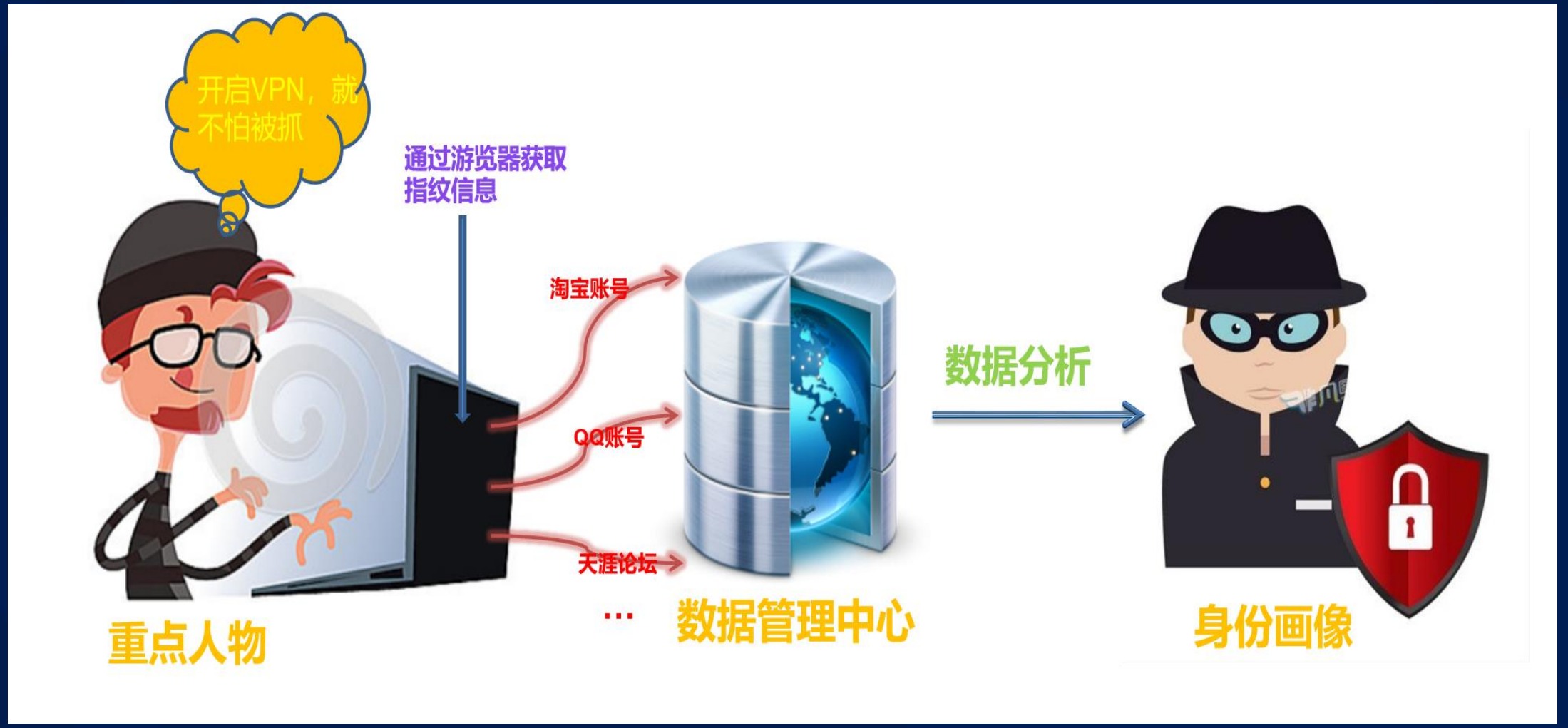
“以攻构防”思想的实战——APT攻击

高价值
目标

高价值
情报

APT攻击

“以攻构防”思想的应用——攻击溯源



常规攻击思路

需要解决的问题

1.无论是攻是防，监管部门自身需要掌握渗透攻击相关知识，如何做体系化的建设和培训

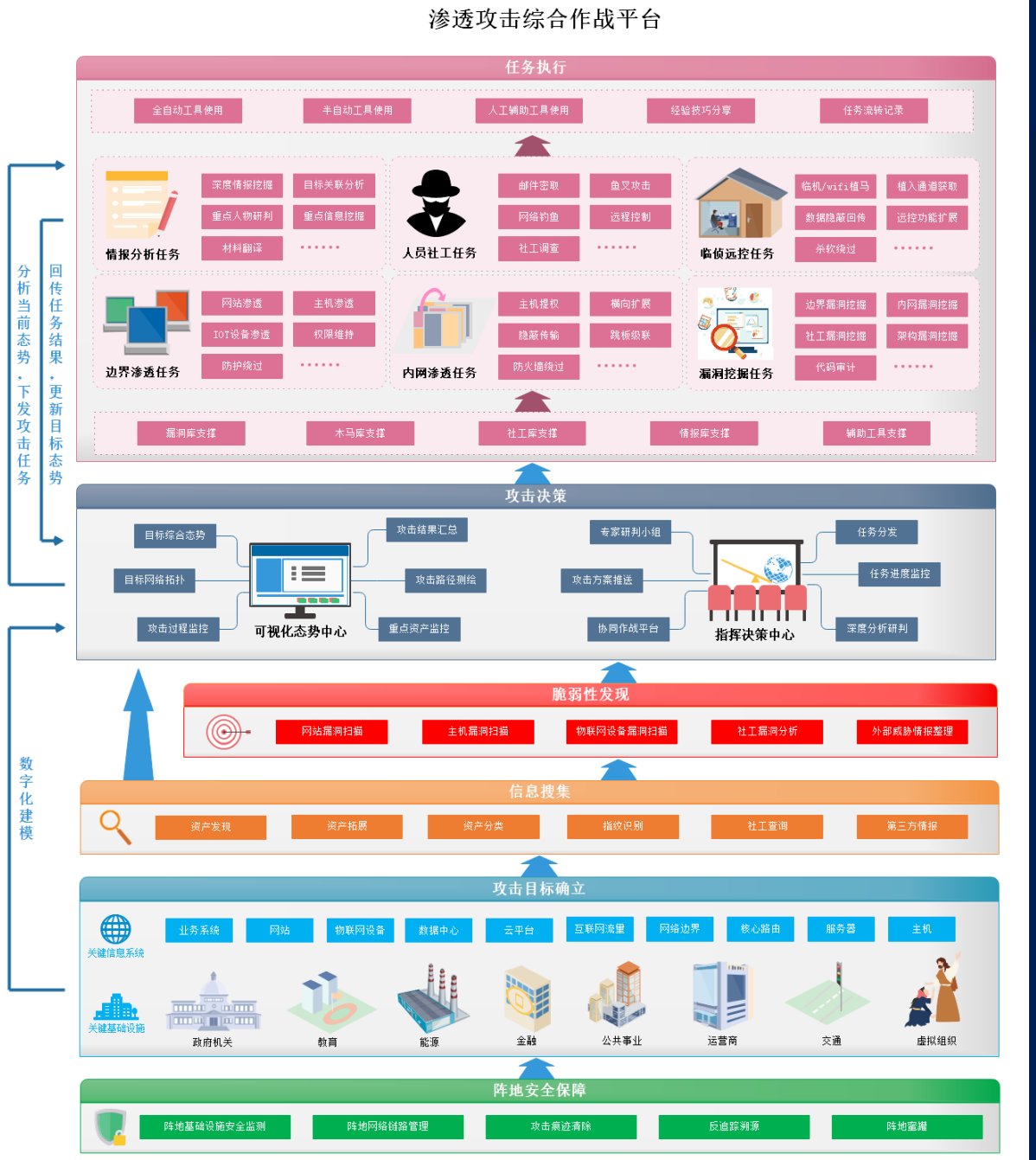
2.渗透攻击是一个流程化的过程，如何能够将攻击过程串联起来，实现尽可能的自动化和简单化

3.渗透攻击需要大量的人工干预工作，如何将人工干预降到最低

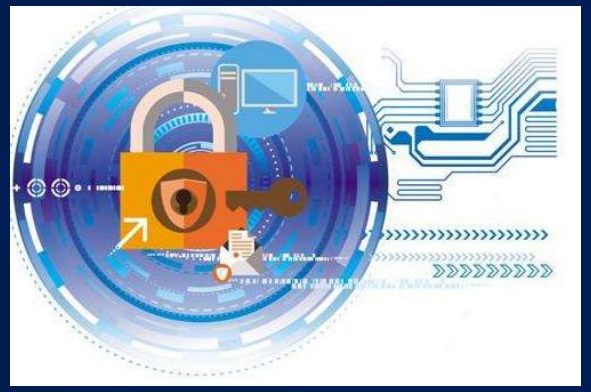
4.监管部门进行渗透攻击时需要借助外部专家团队力量，如何维持敏感性、增强适应性

渗透攻击综合作战平台


阵地防护
攻击任务执行
信息搜集
综合作战平台
攻击决策
脆弱性发现
攻击方案推送


渗透攻击综合作战平台
任务执行
全自动工具使用
半自动工具使用
人工辅助工具使用
经验技巧分享
任务流转记录
情报分析任务
深度情报挖掘
目标关联分析
重点人物研判
重点信息挖掘
材料翻译
人员社工任务
邮件密取
鱼叉攻击
网络钓鱼
远程控制
社工调查
临侦远控任务
临机/wifi植马
植入通道获取
数据隐蔽回传
远控功能扩展
杀软绕过
边界渗透任务
网站渗透
主机渗透
IOT设备渗透
权限维持
防护绕过
内网渗透任务
主机提权
横向扩展
隐蔽传输
跳板级联
防火墙绕过
漏洞挖掘任务
边界漏洞挖掘
内网漏洞挖掘
社工漏洞挖掘
架构漏洞挖掘
代码审计
漏洞库支撑
木马库支撑
社工库支撑
情报库支撑
辅助工具支撑
分析当前态势，下发攻击任务
回传任务结果，更新目标态势
攻击决策
目标综合态势
目标网络拓扑
攻击过程监控
攻击结果汇总
攻击路径测绘
重点资产监控
可视化态势中心
专家研判小组
攻击方案推送
协同作战平台
任务分发
任务进度监控
深度分析研判
指挥决策中心
数字化建模
脆弱性发现
网站漏洞扫描
主机漏洞扫描
物联网设备漏洞扫描
社工漏洞分析
外部威胁情报整理
信息搜集
资产发现
资产拓展
资产分类
指纹识别
社工查询
第三方情报
攻击目标确立
关键信息系统
业务系统
网站
物联网设备
数据中心
云平台
互联网流量
网络边界
核心路由
服务器
主机
关键基础设施
政府机关
教育
能源
金融
公共事业
运营商
交通
虚拟组织
阵地安全保障
阵地基础设施安全监测
阵地网络链路管理
攻击痕迹清除
反追踪溯源
阵地蜜罐

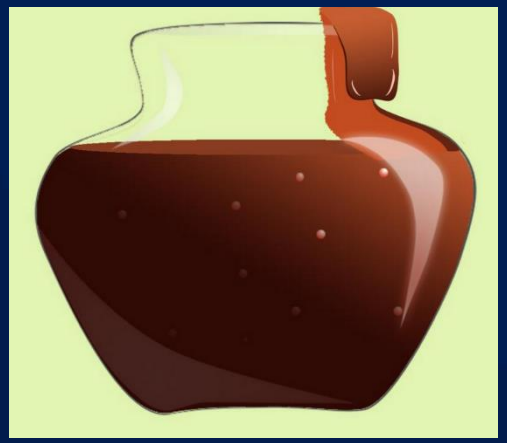
阵地防护



阵地基础设施安全监测

阵地链路管理

阵地流量监测审计



阵地蜜罐

阵地内网安全监测

……

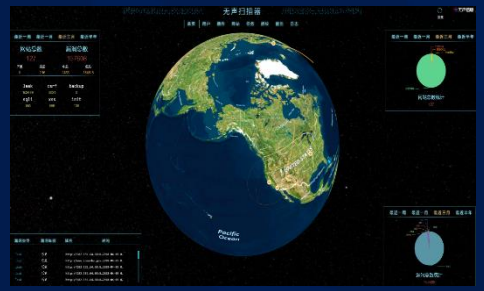
信息搜集与脆弱性分析

资产发现

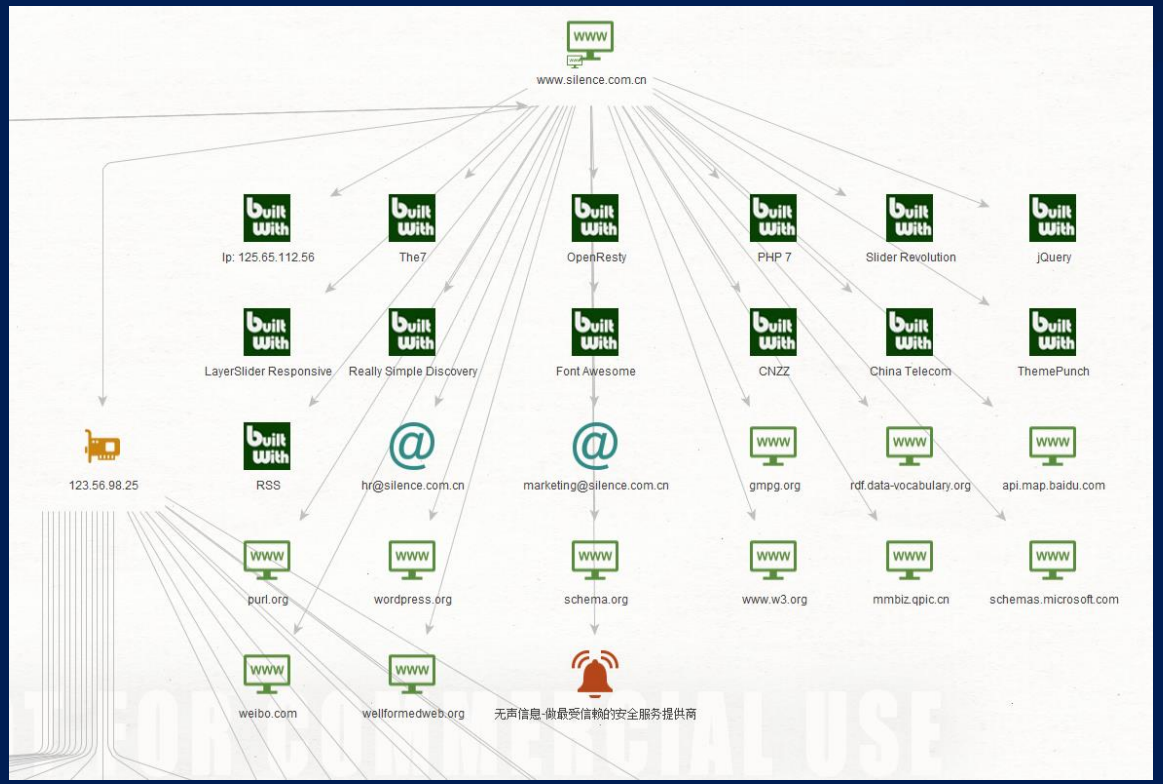
资产拓展

资产分类

外部威胁情报



脆弱性分析



攻击决策

攻击方案推送
依据目标信息探测和脆弱性发现的结果，生成推荐的攻击方案和攻击路径供决策者参考

攻击任务派发
依据当前攻击方案下发不同的攻击任务供各攻击小队执行

攻击任务更新
依据各类任务的完成和反馈情况，更新攻击方案，重新下发新的任务

攻击效果评估
对目标攻击结果进行汇总，评估渗透攻击效果。

攻击任务执行


任务执行
全自动工具使用
半自动工具使用
人工辅助工具使用
经验技巧分享
任务流转记录
情报分析任务
深度情报挖掘
目标关联分析
重点人物研判
重点信息挖掘
材料翻译
人员社工任务
邮件密取
鱼叉攻击
网络钓鱼
远程控制
社工调查
临侦远控任务
临机/wifi植马
植入通道获取
数据隐蔽回传
远控功能扩展
杀软绕过
边界渗透任务
网站渗透
主机渗透
IOT设备渗透
权限维持
防护绕过
内网渗透任务
主机提权
横向扩展
隐蔽传输
跳板级联
防火墙绕过
漏洞挖掘任务
边界漏洞挖掘
内网漏洞挖掘
社工漏洞挖掘
架构漏洞挖掘
代码审计
漏洞库支撑
木马库支撑
社工库支撑
情报库支撑
辅助工具支撑

态势展示

阵地安全态势
呈现当前阵地基础设施安全情况、阵地链路接入情况、阵地流量分析情况、阵地内网脆弱性发现情况和阵地蜜罐捕获情况等阵地自身的安全态势情况

攻击目标态势
呈现当前目标设备信息、应用信息、目标网络结构、目标侦查结果、目标相关人员信息、目标脆弱性等攻击目标态势信息

任务执行态势
呈现当前信息搜集任务完成情况、攻击任务完成情况、攻击路径、攻击进度、攻击结果、失败原因等任务执行态势信息

综合态势
呈现渗透攻击作战平台的综合态势信息，包括攻击目标统计、攻击工具统计、历史攻击任务统计、最新攻击任务信息等


感谢您的观看!