2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

WebRAY 盛邦安全

威胁情报下资产测绘的关键行业分析

权小文@WebRAY

目　录

威胁情报落地方案汇报—资产治理模型

资产摸底

- 内、外网、核心资源
- 资产梳理
- 僵尸/双非系统清理

摸清家底

不走后门

- 数据中心内部备案体系
- 漏洞评估体系
- 审核体系

安全体系

- 等级保护
- 立体化防御体系

立体化

自动化运营

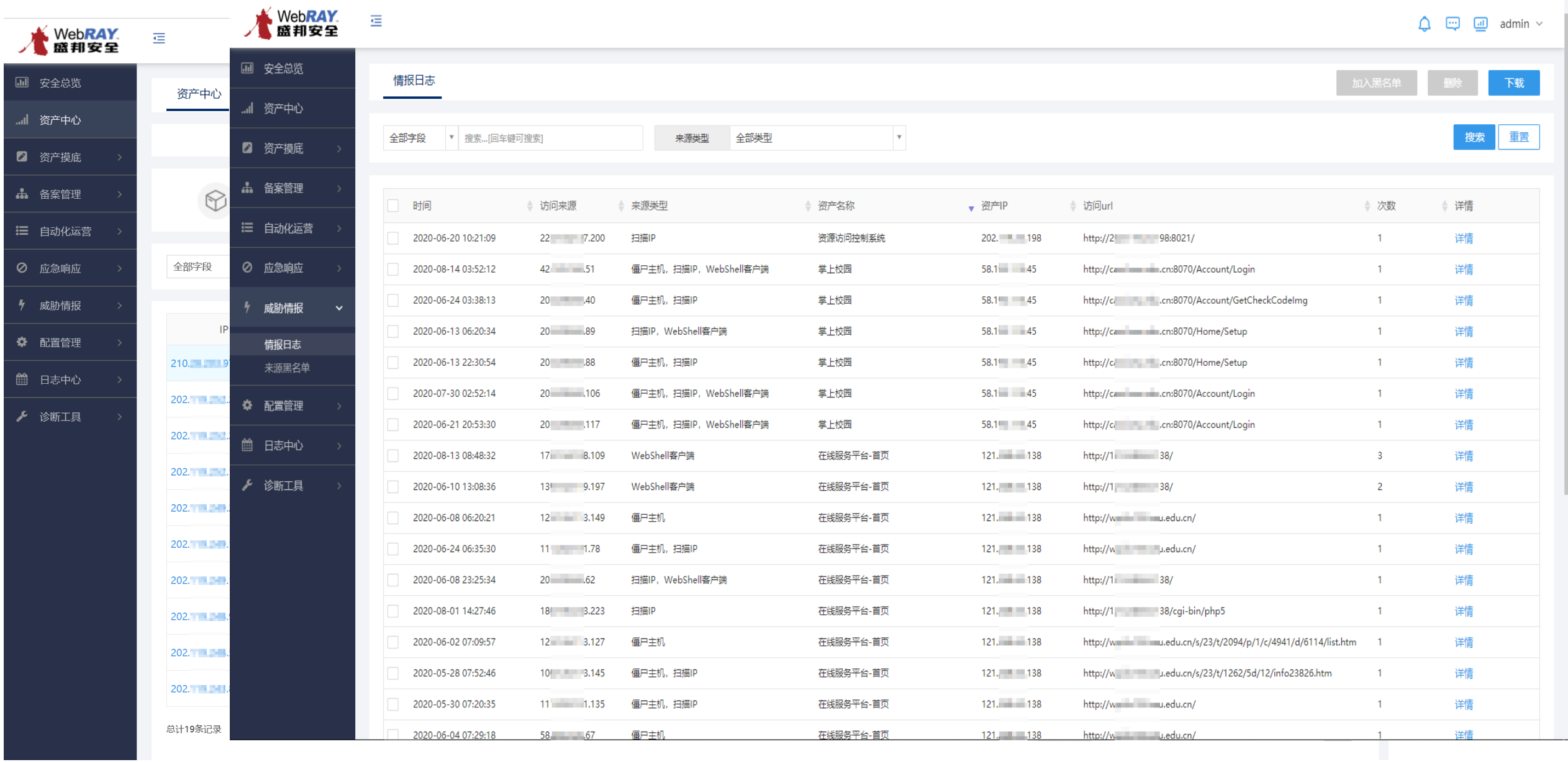
- 篡改监控
- 漏洞监控
- 流量监控（**威胁情报**）
- WebShell/弱口令

应急预案

- 一键断网
- 应急预案

紧急响应

威胁情报落地方案汇报—资产治理效果图



WebRAY 盛邦安全

admin

安全总览
资产中心
资产摸底
备案管理
自动化运营
应急响应
威胁情报
配置管理
日志中心
诊断工具

资产中心

全部字段

IP

210.
202.
202.
202.
202.
202.
202.
202.
202.
202.

总计19条记录

WebRAY 盛邦安全

安全总览
资产中心
资产摸底
备案管理
自动化运营
应急响应
威胁情报
情报日志
来源黑名单
配置管理
日志中心
诊断工具

情报日志

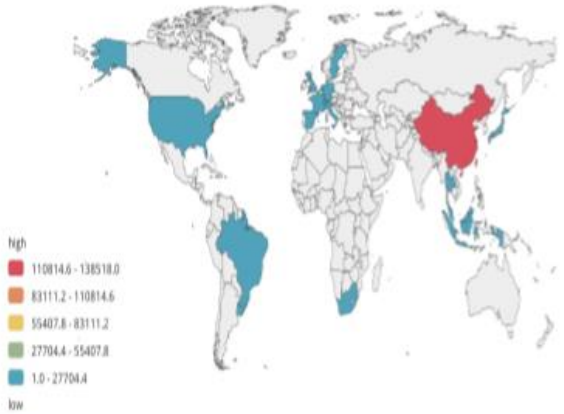
加入黑名单 删除 下载

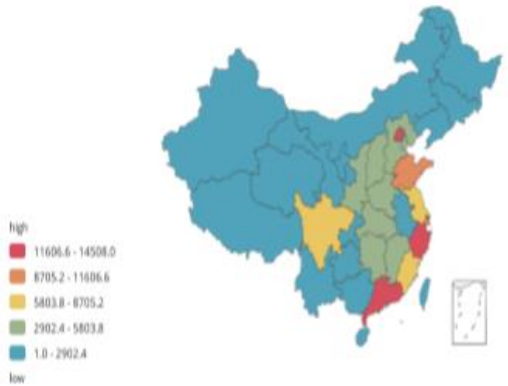
全部字段 搜索...[回车键可搜索] 来源类型 全部类型 搜索 重置

时间	访问来源	来源类型	资产名称	资产IP	访问url	次数	详情
2020-06-20 10:21:09	22 7.200	扫描IP	资源访问控制系统	202. 198	http://2 98:8021/	1	详情
2020-08-14 03:52:12	42 .51	僵尸主机，扫描IP，WebShell客户端	掌上校园	58.1 45	http://ca .cn:8070/Account/Login	1	详情
2020-06-24 03:38:13	20 .40	僵尸主机，扫描IP	掌上校园	58.1 45	http://c .cn:8070/Account/GetCheckCodeImg	1	详情
2020-06-13 06:20:34	20 .89	扫描IP，WebShell客户端	掌上校园	58.1 45	http://ca .cn:8070/Home/Setup	1	详情
2020-06-13 22:30:54	20 .88	僵尸主机，扫描IP	掌上校园	58.1 45	http://c .cn:8070/Home/Setup	1	详情
2020-07-30 02:52:14	20 .106	僵尸主机，扫描IP，WebShell客户端	掌上校园	58.1 45	http://ca .cn:8070/Account/Login	1	详情
2020-06-21 20:53:30	20 .117	僵尸主机，扫描IP，WebShell客户端	掌上校园	58.1 45	http://c .cn:8070/Account/Login	1	详情
2020-08-13 08:48:32	17 8.109	WebShell客户端	在线服务平台-首页	121. 138	http://1 38/	3	详情
2020-06-10 13:08:36	13 9.197	WebShell客户端	在线服务平台-首页	121. 138	http://1 38/	2	详情
2020-06-08 06:20:21	12 3.149	僵尸主机	在线服务平台-首页	121. 138	http://w u.edu.cn/	1	详情
2020-06-24 06:35:30	11 1.78	僵尸主机，扫描IP	在线服务平台-首页	121. 138	http://w u.edu.cn/	1	详情
2020-06-08 23:25:34	20 .62	扫描IP，WebShell客户端	在线服务平台-首页	121. 138	http://1 38/	1	详情
2020-08-01 14:27:46	18 3.223	扫描IP	在线服务平台-首页	121. 138	http://1 38/cgi-bin/php5	1	详情
2020-06-02 07:09:57	12 3.127	僵尸主机	在线服务平台-首页	121. 138	http://w u.edu.cn/s/23/t/2094/p/1/c/4941/d/6114/list.htm	1	详情
2020-05-28 07:52:46	10 3.145	僵尸主机，扫描IP	在线服务平台-首页	121. 138	http://w u.edu.cn/s/23/t/1262/5d/12/info23826.htm	1	详情
2020-05-30 07:20:35	11 1.135	僵尸主机，扫描IP	在线服务平台-首页	121. 138	http://w u.edu.cn/	1	详情
2020-06-04 07:29:18	58 .67	僵尸主机	在线服务平台-首页	121. 138	http://w u.edu.cn/	1	详情

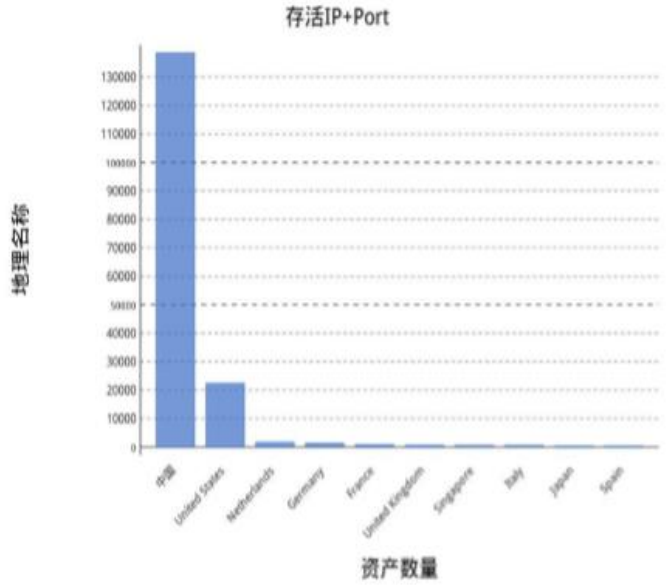
网络空间资产的关键技术点——某央企集团外网暴露面分析

170, 076 IP+Port 数量（个）		49, 842 独立 IP 数量（个）
4 行业分布（个）	200 开放端口（个）	200 开放服务（个）
12 操作系统（种）	268 组件（个）	8 设备类型（种）
475 漏洞（个）	0 弱口令数量（个）	1 PoC（⚠非常危险）





- 存活 IP+Port 资产 170076 条，分布前 10 区域分别为中国，United States，Netherlands，Germany，France，United Kingdom，Singapore，Italy，Japan，Spain；
- 独立 IP 资产 49842 条，分布前 10 区域分别为中国，United States，Netherlands，Germany，France，United Kingdom，Singapore，Italy，Japan，Spain；
- 开放端口 200 个，TOP10 为：443，80，8080，8443，8081，1935，8888，5666，9090，9000；
- 开放服务 200 个，TOP10 为：http，https，tcpwrapped，http-proxy，jetdirect，rpcbind，irc，rtmp，https-alt，smtp；



地理位置	数量	比例
中国	138518	81.44477
United States	22339	13.13472%
Netherlands	1676	0.98544%
Germany	1251	0.73555%
France	830	0.48802%
United Kingdom	619	0.36395%
Singapore	535	0.31457%
Italy	511	0.30045%
Japan	340	0.19991%
Spain	314	0.18462%

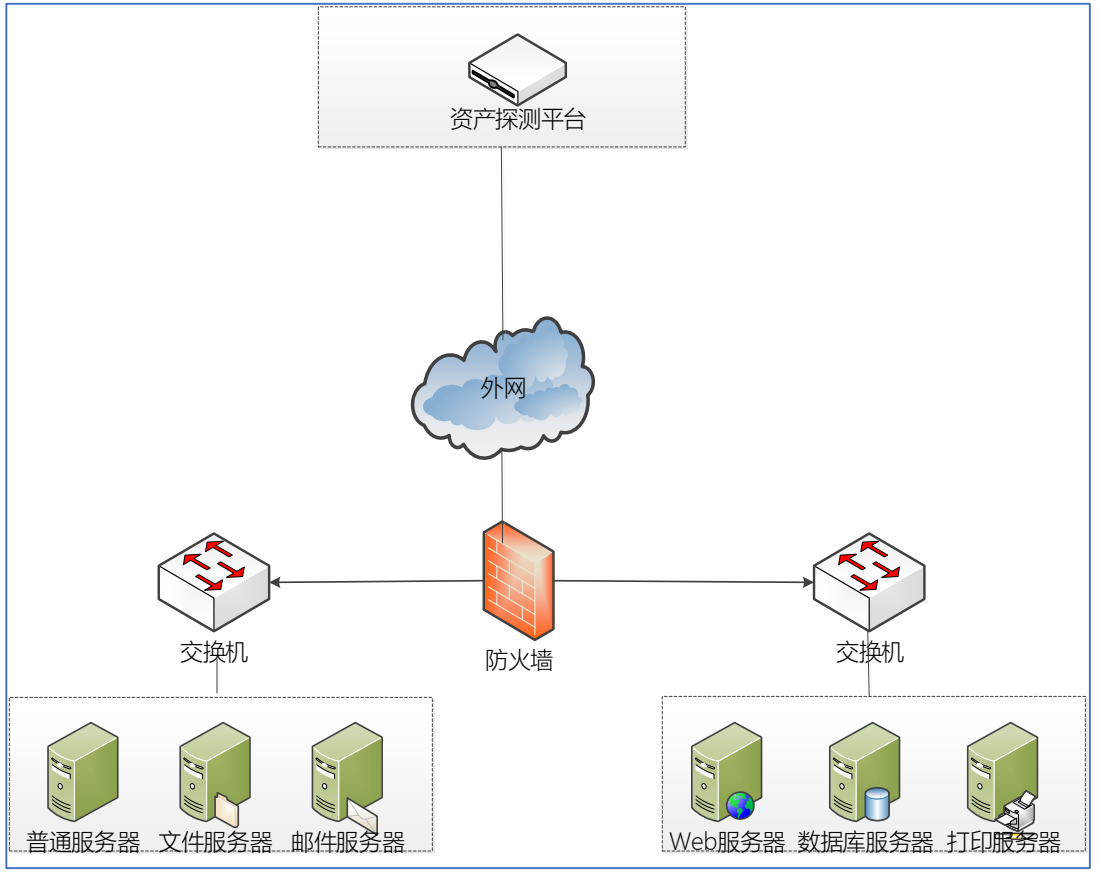
特点：网络空间的国家边界属性不清晰，你中有我，我中有你，相互交错

网络空间资产的关键技术点——某央企集团外网暴露面分析

统计周期内， 设备类型 8 种， 设备类型数量 TOP8 分别为：

1) 设备类型： 云服务资源 数量： 9550 占比： 46.27386%；
2) 设备类型： 负载均衡设备 数量： 8093 占比： 39.21407%；
3) 设备类型： 安全防护设备 数量： 2875 占比： 13.93061%；
4) 设备类型： 其它网络设备 数量： 94 占比： 0.45547%；
5) 设备类型： 路由交换设备 数量： 12 占比： 0.05815%；
6) 设备类型： 智能移动终端 数量： 8 占比： 0.03876%；
7) 设备类型： 运维管理 数量： 5 占比： 0.02423%；
8) 设备类型： 网络摄像头 数量： 1 占比： 0.00485%；

网络安全设备子类	厂商	数量
waf	F5 Networks	2817
access gateway	Citrix Systems, Inc	38
vpn	Cisco Systems Inc.	14
access security	Juniper Networks, Inc.	6

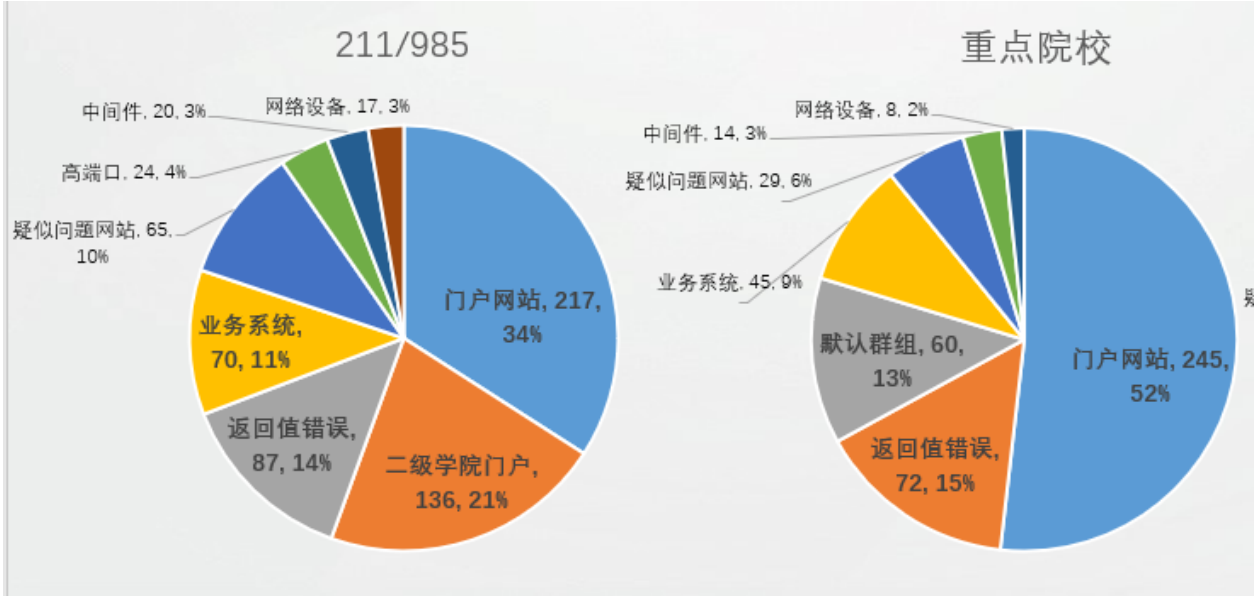


拓扑部署：基于扫描的主动资产摸底

网络空间资产的关键技术点——教育类行信息化普查

域名	行政部门	学校	总计
.com	316	16524	16840
.cn	268	7681	7949
.edu.cn	29	1499	1528
.com.cn	48	1101	1149
.net.cn	32	295	327

类别	公司	产品	占比
迎新系统	浙江正方	迎新管理系统	12%
财务系统	复旦天翼	天翼财务管理系统	8%
学生系统	浙江正方	学生工作管理系统	16%
邮件系统	Coremail	Coremail	54%
教务系统	湖南青果	青果教务管理系统	37%



教育行业网络空间测绘：

1）教育行业域名使用情况；
2）教育行业软件使用情况、漏洞情况、运维情况、整体运维风险情况；
3）教育行业网络空间信息化资产情况和设备分配情况；
4）IPv6普及情况等。

如果信息资产进入网络空间，那么这个资产可以称为网络空间资产，否则仍然为信息资产。举例：

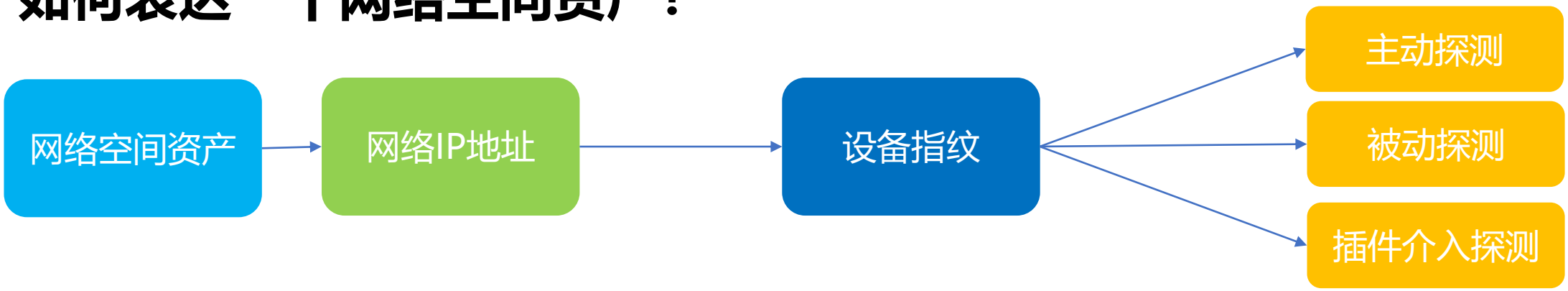
1）软件Office 2019，算信息资产-软件资产；

2）软件Office 356，具备联网属性并且以IP地址表达，因此算网络空间资产。

MS Office 2019

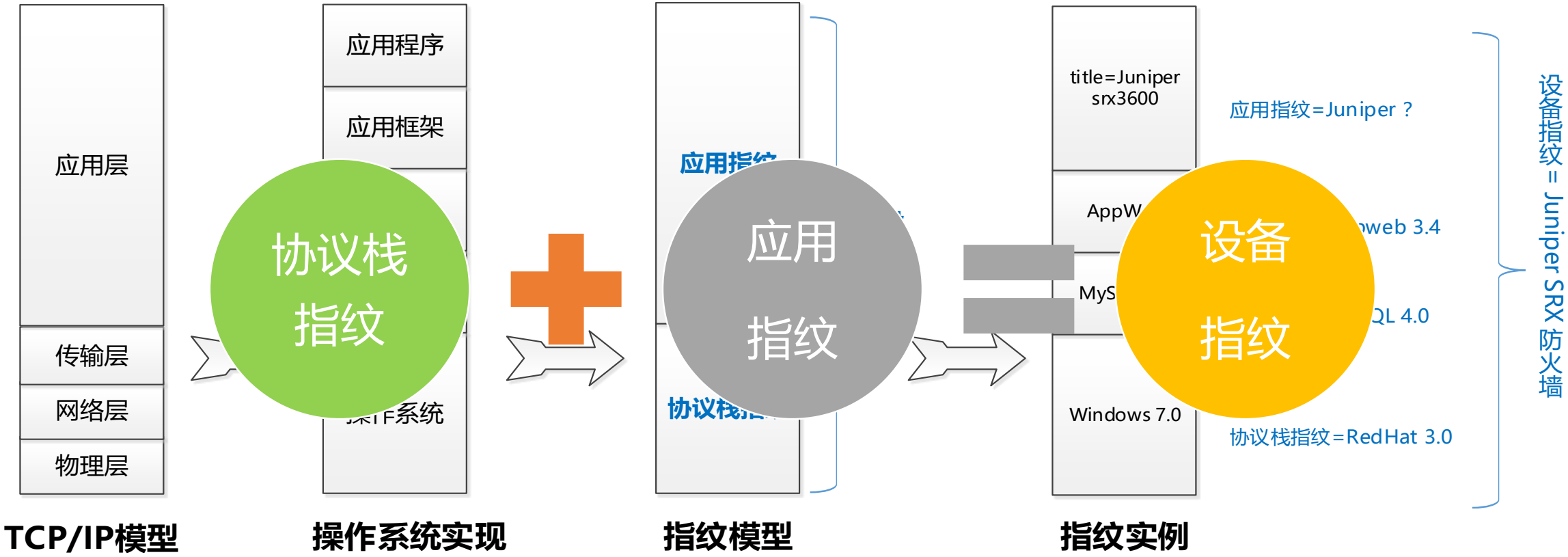
MS Office 365

如何表达一个网络空间资产？



设备指纹是网络空间资产的表达唯一因素

网络空间资产的关键技术点——网络空间的网络测绘模型



网络空间资产的关键技术点——网络空间探测模型

轻量级探测

1

- 存活性
- IPV4
- IPV6

全栈探测

2

- 交换路由
- 安防设备
- IoT设备
- 云平台
- 服务类
- 工控类
- 网络打印机
- 暗网软件

协议栈指纹

- Banner识别
- 带外识别
- 响应顺序
- ALG协议识别安防
- 逆向行为

指纹信息获取

- IP属性信息
- 应用信息
- OS信息
- 厂商信息

漏洞检测

3

- 紧急漏洞（POC）
- 常规漏洞
  - 系统扫描
  - Web扫描
  - 工控扫描
  - 数据库扫描
- 漏洞快速普查（24h）

漏洞信息获取

行业属性分析

5

机构信息获取

- WhoIS
- DNS库
- 行业机构
- ...

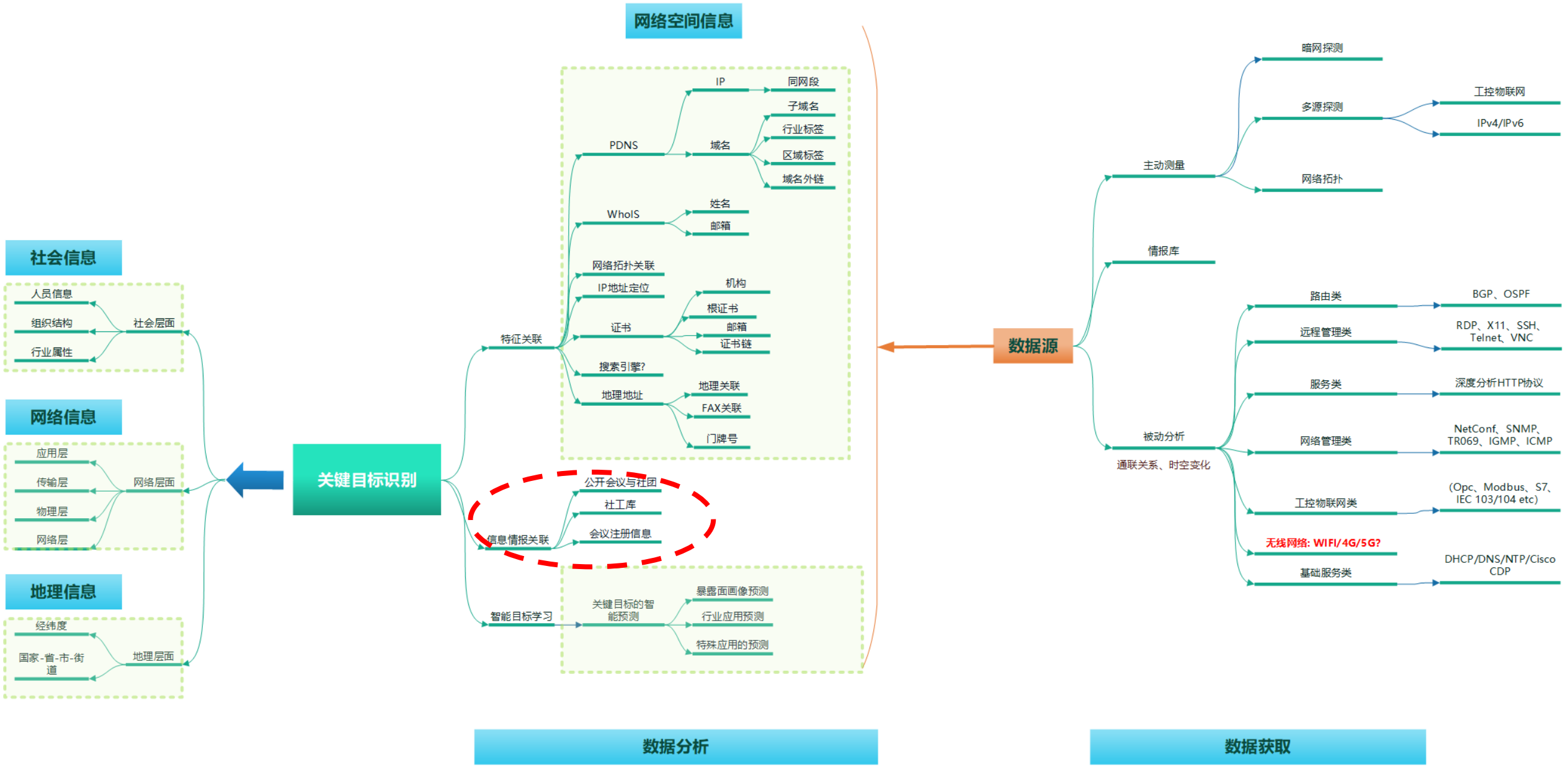
情报关联

4

威胁情报关联

- 攻击库
- IP画像
- ...

网络空间资产的关键技术点——网络空间->社会空间



网络空间资产的关键技术点——网络空间资产测绘效果展示

135.26.240.214 查看源数据(键值对)

基本信息

更新时间	2019-12-02
国家地区	United States,Kansas,Shawnee
经度，纬度	-94.7202,39.0417
运营商	consolidated.com
主机名称	135-26-240-214.static.everestkc.net
ASN	AS18712
网关	64.126.2.162
组织	SureWest Kansas Operations, LLC

IP定位，融合算法

端口开放

端口服务

Open: 22/ssh 80/http 443/https

漏洞概述

漏洞统计

高危(2) 中危(5) 低危(0) POC(1)

专家模式

标签分类

可视化展示

业务/产品	
支撑层	
服务层	
系统层	
硬件层	Dell Sonicwall NSA 220 Firewall
其它	

资产详情

服务详情

22 tcp ssh

组件名称: OpenSSH
系统名称: embedded
系统类型: embedded
设备名称: Dell Sonicwall NSA 220 firewall
设备类型: 安全防护设备
厂商名称: Dell Technologies
更新时间: 2019-12-02
品牌: Dell
设备型号: Sonicwall NSA 220

Dell Sonicwall NSA 220 Firewall

产品标签，可以全局检索

资产指纹拓扑

指纹拓扑

端口变化

端口变化

```
info: Remote protocol version 2.0, remote software version OpenSSH_6.2 PKIX
compression_algorithms: none,zlib
encryption_algorithms: aes128-gcm@openssh.com,aes256-gcm@openssh.com,aes128-ctr,aes256-ctr,arcfour128,des,3des,arcfour
server_host_key_algorithms: ssh-rsa
kex_algorithms: diffie-hellman-group-exchange-sha1
mac_algorithms: hmac-sha1
```

profession

80 tcp http

网站标题: Document Moved
组件名称: SonicWALL firewall http config
系统名称: embedded
系统类型: embedded
设备名称: Dell Sonicwall NSA 220 firewall
设备类型: 安全防护设备
厂商名称: Dell Technologies
更新时间: 2019-03-17
品牌: Dell
设备型号: Sonicwall NSA 220

Dell Sonicwall NSA 220 Firewall SonicWALL公司产品

端口变化 跳转访问

profession

```
<head><meta http-equiv="Content-Type" content="text/html; charset=utf-8">

<meta http-equiv="Content-Type" content="text/html">
<title>Document Moved</title>
<meta name="id" content="docJump" >
<link rel=stylesheet href="swl_styles-5.0.0-233648838.css" TYPE="text/css">
<script type="text/JavaScript">
var resetSecureFlag = false;
```

已确认POC

确认PoC

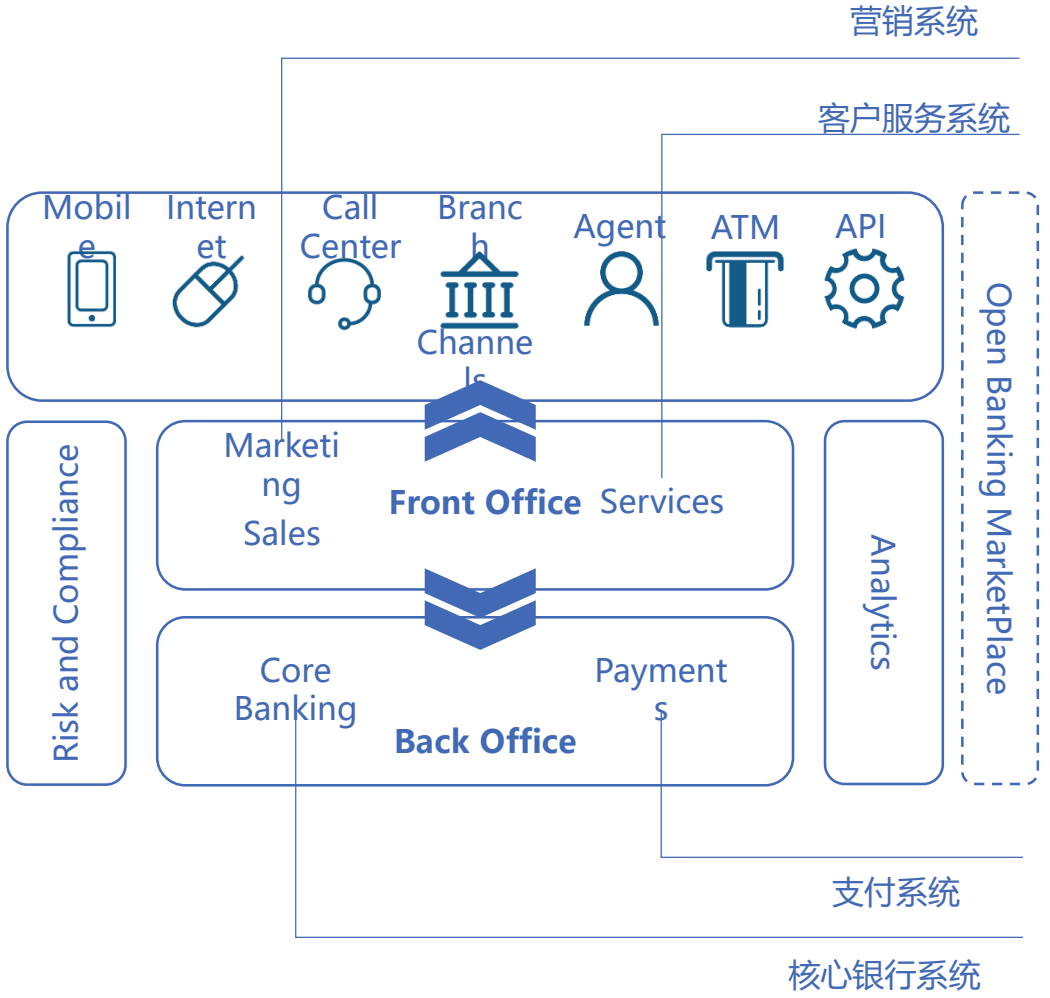
OpenSSH-用户枚举漏洞

【漏洞对象】OpenSSH
【涉及版本】openssh版本<=7.7
【漏洞描述】
OpenSSH 7.7及之前版本中存在安全漏洞，该漏洞源于程序会对有效的和无效的身份验证请求发出不同的响应。攻击者可通过发送特制的请求利用该漏洞枚举用户名称。,攻击者可以通过向目标系统发送身份验证请求数据包来利用此漏洞，成功的利用可能允许攻击者访问敏感信息，例如系统上的有效用户名。

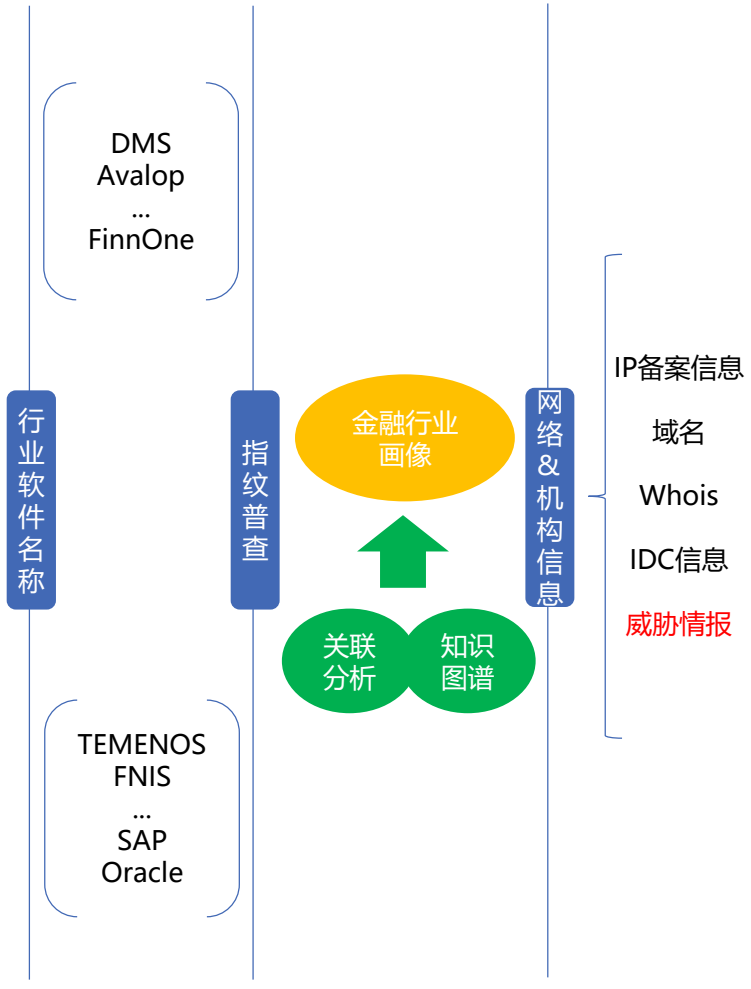
CVE漏洞列表

关联漏洞

威胁情报下资产测绘的行业分析——社会组织识别与分析

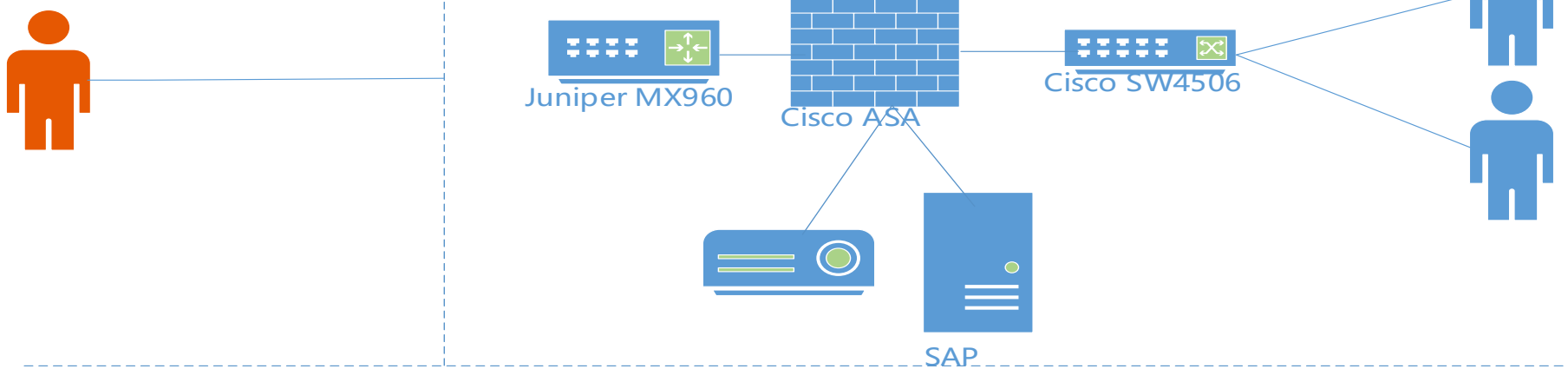


银行系统典型部署图

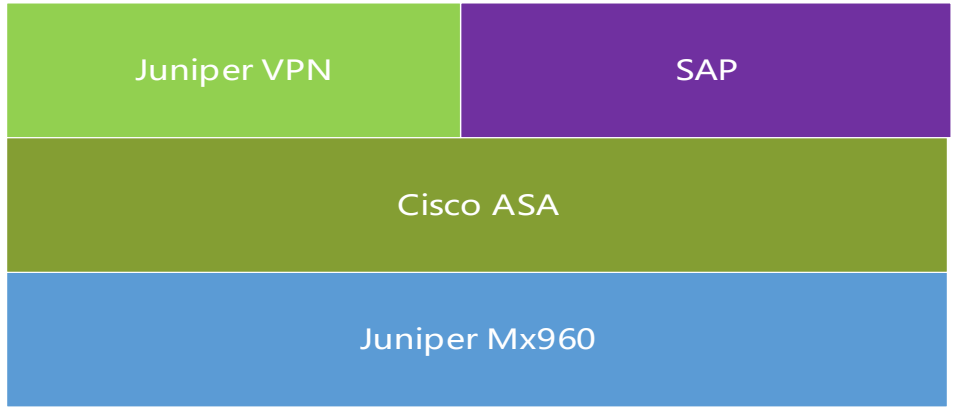


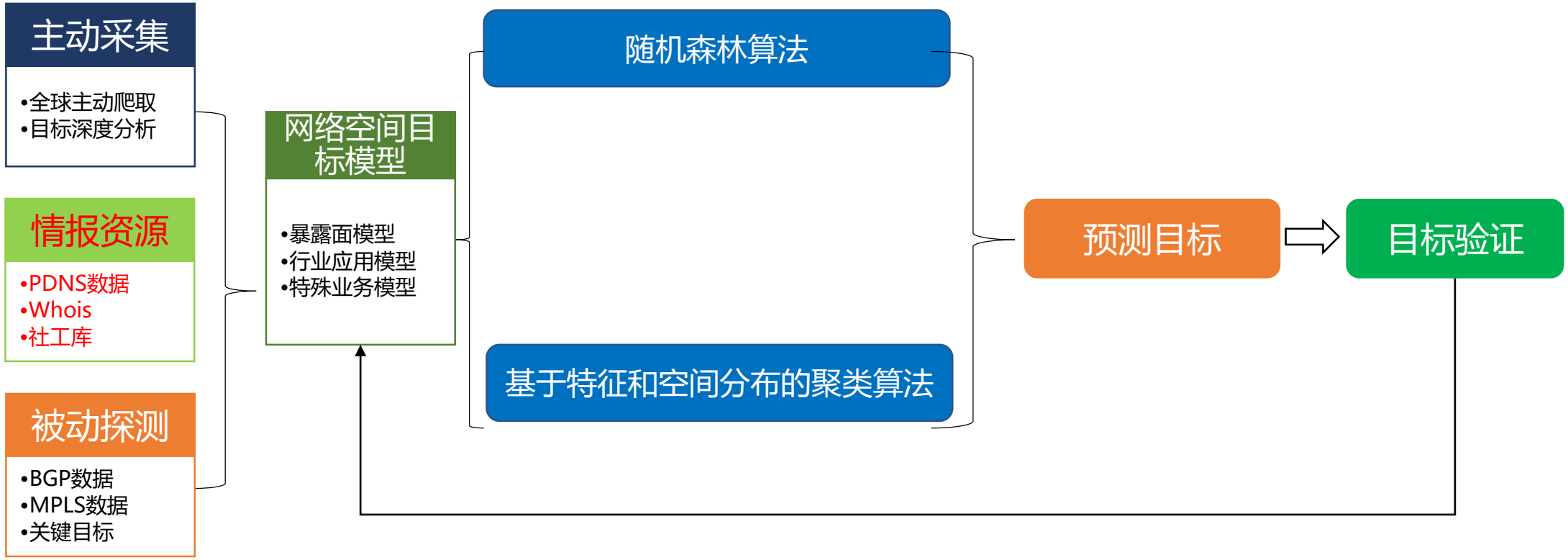
北美前10大银行软件

基本网络信息


Juniper SSL VPN
Juniper MX960
Cisco ASA
Cisco SW4506
SAP

暴露面模型


Juniper VPN
SAP
Cisco ASA
Juniper Mx960


主动采集
•全球主动爬取
•目标深度分析
情报资源
•PDNS数据
•Whois
•社工库
被动探测
•BGP数据
•MPLS数据
•关键目标
网络空间目标模型
•暴露面模型
•行业应用模型
•特殊业务模型
随机森林算法
基于特征和空间分布的聚类算法
预测目标
目标验证

2020北京网络安全大会

2020 BEIJING CYBER SECURITY CONFERENCE

THANKS

全球网络安全 倾听北京声音