云图-网络空间测绘平台

目录

形势背景

现状痛点

INSEC 云思华盛

摸不清网络资产

相关网络安全监管部门**缺乏有效手段**，难以全面摸清所辖区域内的网络资产，掌握资产互联网暴露面、资产类型和内容。

摸不准资产属性

资产属性**获取手段过于单一**，往往依靠手工填报，掌握资产信息少、不准确，无法快速掌握资产变化情况。

找不到资产归属

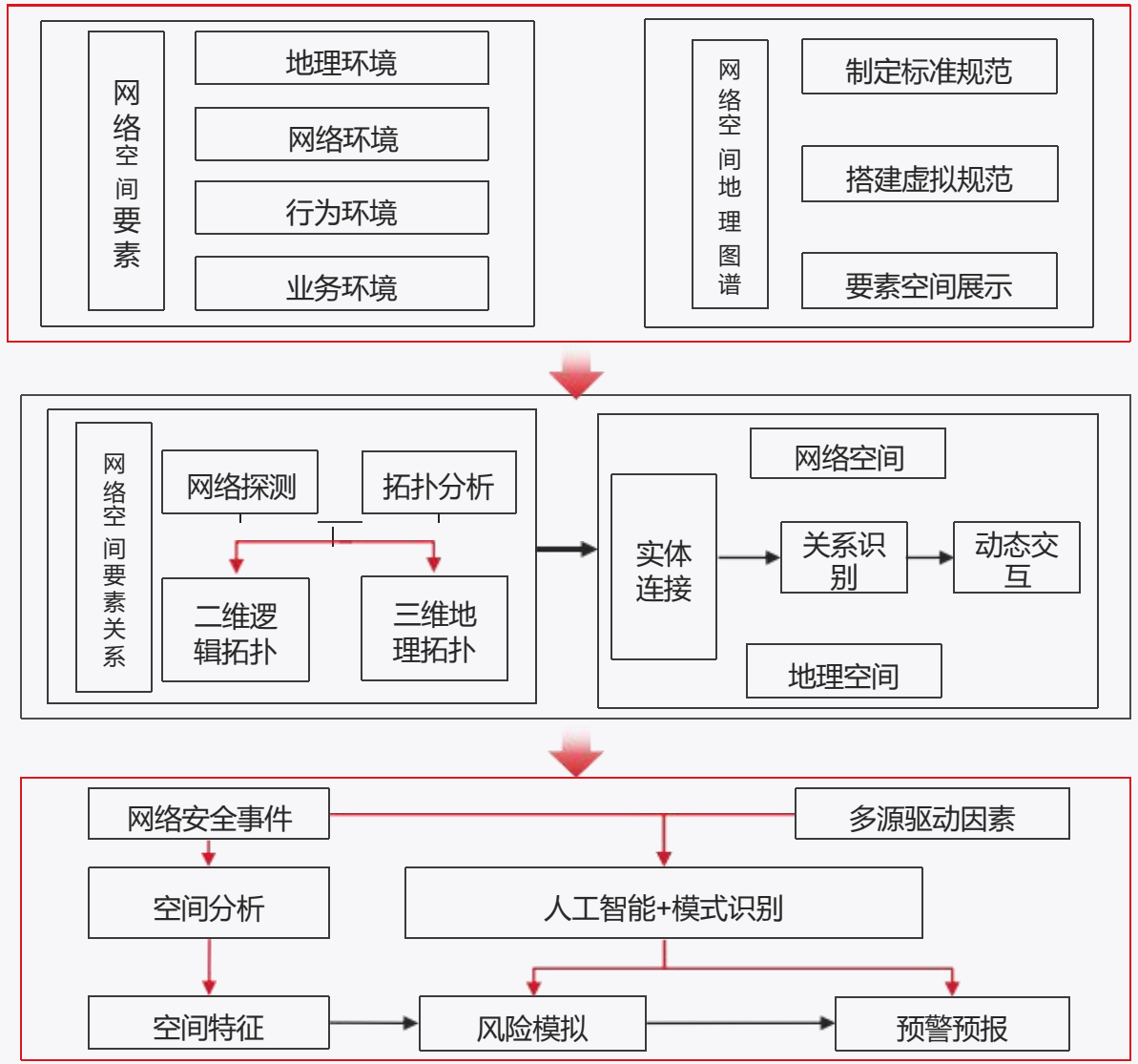
发生安全事件或通报时**无法快速定位**受影响资产，**找不到负责单位和负责人**。

挂图作战

要素可视化

关系可视化

事件可视化



应用场景

应用场景

INSEC 云思华盛

自定义的分类标志

S1： 统计党政机关类型网站数量
S2： 现需对高校开展攻防演练，需收集高校IP、网站等资产数据，进行各战队资产分配

定位资产，找到主体责任人

S1:某单位服务器被挂反共标语，及时定位该资产所属区域，IP的设备、操作系统、服务和应用；查询该单位互联网资产清单

历史回顾，动态跟踪

S1:查看某网站什么时候单位主体发生变更，网站的主要内容发生变更?

内容不明

落地不易

摸清家底 → **识别应用** → **违规排查** → **联合破案** → **重点盯防** → **安全朔源** → **网络空间可视化**

资产不清

全面灵活的资产探测

S1:ADSL统计
S2:网络摄像头统计
S3:某区县现存或IP数量

犯罪不晓

查处整改，规避风险

S1:执法整改：帮助统计未进行公安未备案的网站，辅助基层网安民警工作，行程执法整改任务

重点不分

场景化盯防、个性化设置

S1： 统计cop15重保单位的资产数据，且将资产标记为重点监控对象，保证有影响力的单位不产生安全事件。

多维可视化表达

全息挂图作战地图

S1:攻防演练

产品介绍

推广价值


网络空间可视化
网络空间要素
可视化表达
网络空间关系
可视化描述
网络安全事件
可视化分析
三化一体平台建设
网络空间
地理空间
社会空间
绘制网络空间地图

应用价值

INSEC 云思华盛

应用价值

提高资产统计汇报准确能力

完善攻防大赛基础数据收集能力

提升安全事故应急处理能力

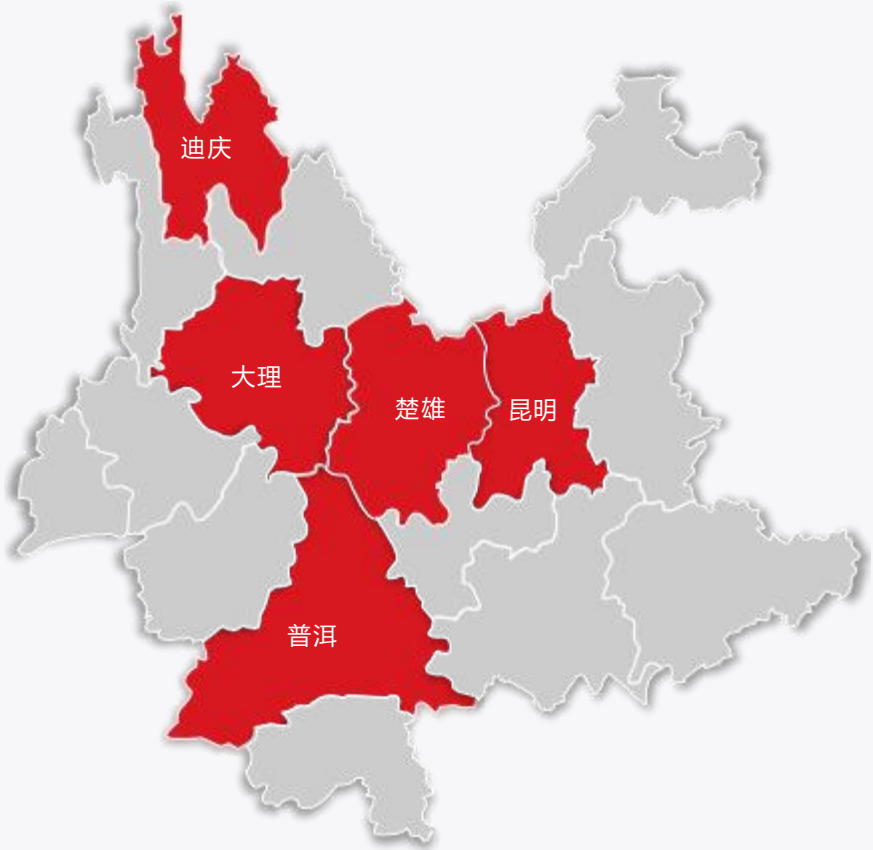
进一步加固区域网络安全治理能力

抓手

网络空间测绘平台

基石

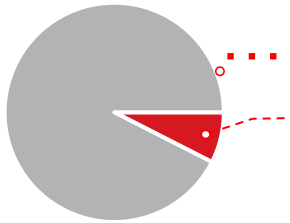
网络空间资产数据



已搭建

应用价值

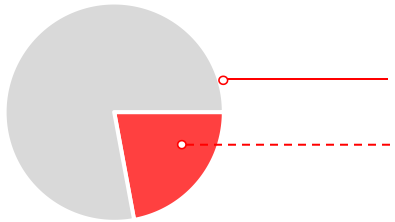
梳理网络空间资产数据，帮助监管单位在网络安全事件中精准定位相关主体单位。 已采集部分数据如下：



205+万 全市IP总数

15+万 存活IP数

30+万 存活网站



86+万 全市工商注册单位

19+万 已建设网站应用单位

未备案网站	涉黄网站	暗链网站	涉赌网站	被篡改网站
40000+	400+	90+	10+	30+

核心支撑保证系统

100+

广播电视台
自来水务
电网
……

20+单位

社会重要信息系统

500+

省级党政机关
市级党政机关
高校
……

95+单位

其他系统

300+

医院
区县级机关单位
国有企业
中小学
……

30+单位

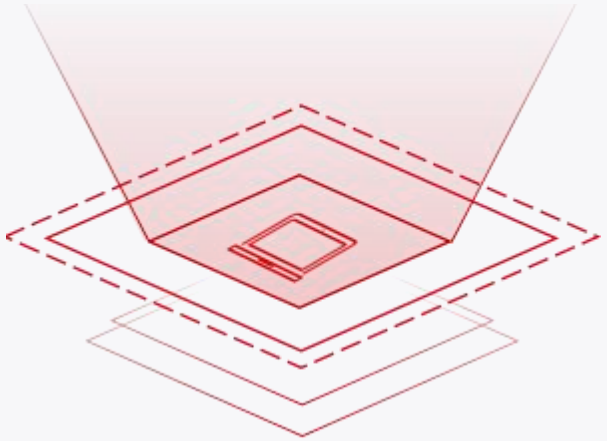
解决思路

INSEC 云思华盛

01

扫描探测

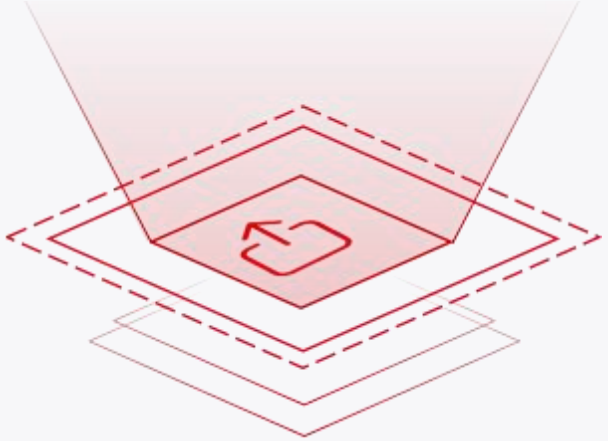
对区域范围内使用的网络资产中的IP和网站分别进行**扫描和爬虫**，实现网络空间资源的**自动探测和资源可视化**。



02

自动化分析

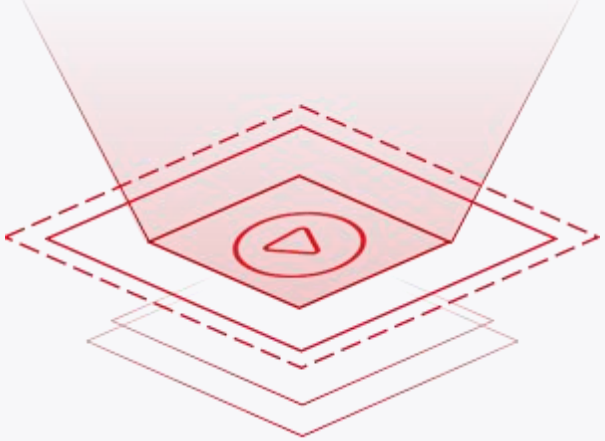
采用**机器学习**方式对网络资产探测内容进行**自动化分析**；
采用**聚类算法**进行**内容精细化分类**，实现持续内容监控。



03

关联匹配

通过多渠道单位数据采集、梳理、分析；
采用**关联分析算法**以及**人工交叉验证**的方式将单位主体与网络资产进行**关联匹配**。



实现过程-扫描探测

对区域范围内IP进行全端口或常用端口扫描探测

对区域范围内访问过的网站、存在http/https协议的IP进行网站爬虫

实现过程-自动化分析

采用**机器学习**方式对网站进行**分类鉴别**，**识别应用**情况；

在全网范围内**搜索样本网站**，爬取网站的标题、关键字、描述等短文本信息；

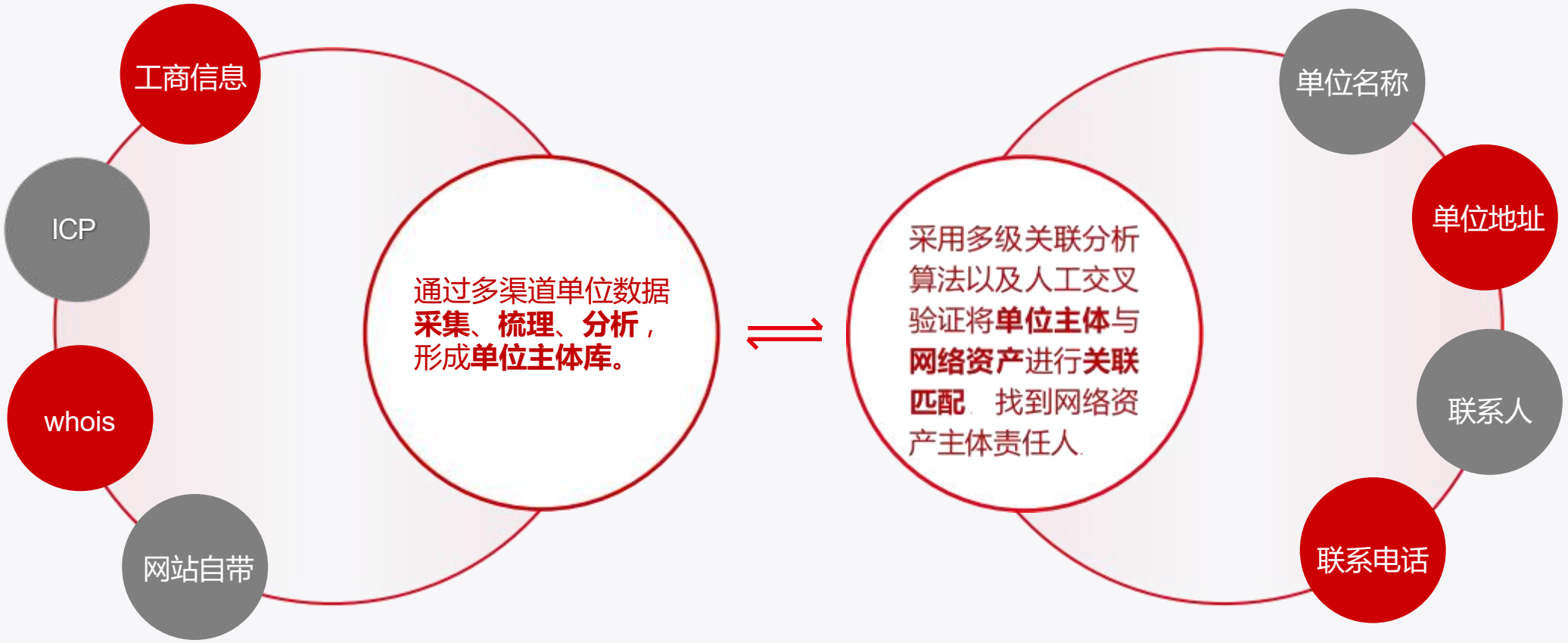
根据监管部门需求**创建主题库**，抽取满足主题规则的样本数据，人工训练样本标签后提交至系统模型；

采用**svm支持向量机**的算法，对网站标题、关键字、描述等进行分词，剔除标题符号、助词等得到词语向量作为特征值；

建立二维坐标轴，x/y（分类/特征值），采用多分类的监督学习算法，在坐标上得到一个最优集，通过朴素贝叶斯等算法优化进一步获取到非线性分类回归方程式；

该数据方程式作为**数据模型**对爬虫扫描到的网站进行**分类分析**，提高识别应用准确率。

实现过程-关联匹配


工商信息
ICP
whois
网站自带
通过多渠道单位数据**采集**、**梳理**、**分析**，形成**单位主体库**。
采用多级关联分析算法以及人工交叉验证将**单位主体**与**网络资产**进行**关联匹配**，找到网络资产主体责任人
单位名称
单位地址
联系人
联系电话

产品亮点

完成网站发现、网站数据采集、DNS解析、ICP调取、TLS爬取、Whois解析，单位主体关联等资产管理，采用机器学习对网站资产进行自动精细化管理。

完成资产探测、端口探测、服务和版本探测、系统探测、应用服务等资产自动发现。

支持单位主体数据的多源获取，完成单位主体信息和网站数据、地理位置的关联映射，实现单位主体的变更跟踪信息。

支持网站涉黄、赌、毒、恐、反动违规内容的监测和告警、取证，以及网站备案信息、篡改、暗链的安全管理和监控警告。

支持对单位主体、行业自动生成相关数据分析报告，包括变更情况，网站安全运营情况、执法跟踪情况。

针对问题网站的单位主体进行闭环执法检查、实现告警和业务场景的结合，完成网站监督检查。

架构介绍

功能结构图

INSEC 云思华盛

单位主体

- 单位录入
- 分类标签管理
- 单位资产查询

挂图作战

- 网络空间
- 社会空间
- 物理空间

执法检查

- 执法流程管理
- 执法用户管理

网站告警

- 涉黄告警
- 涉毒告警
- 反动告警
- 涉赌告警
- 涉恐告警
- 网站暗链
- 网站篡改
- 备案告警

工具箱

- 行业资产报告
- 单位资产报告
- 地理资产报告
- 正则解析库
- 白名单管理
- 样本库管理
- 分类主题管理

网站管理

- 网站截图
- 网站录入
- Whois爬取
- DNS
- TLS爬取
- ICP调取
- 重点标记
- 网站爬虫
- 版本管理
- 爬虫器管理
- 单位映射
- 公安备案
- 网络拓扑
- 内容分类
- 自定义爬虫

IP管理

- IP扫描
- 端口探测
- 服务探测
- 协议探测
- 应用探测
- 设备探测
- 操作系统探测
- 运营商探测
- Tcp路由
- 静态IP识别
- 历史版本管理

平台架构


数据应用层
区域网络资产展示
资产搜索与分析
资产主体信息维护
资产持续监控
涉黄、赌、暴、恐、政识别
报表分析中心
执法检查
数据处理层
Banner指纹库
网页快照
机器学习
多分类/多标签模型
语义分析
敏感词库
网络拓扑
应用框架识别
搜索引擎
图像/视频智能识别
关联分析
手机应用识别
数据探测层
IP扫描
IP扫描探测器
Tcp路由数据
网站扫描
Whois数据
网站爬虫器
DNS数据
TLS证书数据
API接口
ICP数据
IP地址

市场分析

市场定位

系统	客户画像	价值	单点	功能
云图 网络空间测绘系统	地州网安、网信 区县网安、网信	全面的区域资产测绘、风险发现、执法支撑 成为网络安全监督、执法的核心业务系统	更多类型资产测绘 （小程序、户外大屏、应急广播、摄像头）	区域资产测绘、应用识别、风险排查、破案支撑、重点盯防、安全溯源、挂图作战
云图 网络安全自监管系统	垂直行业省级单位。 卫健委、能源、国土、交通等	比监管更早发现自身问题、整改问题	更快、更全面发现安全风险	行业资产测绘、应用识别、风险排查、风险通报、整改验证、挂图作战

竞争分析

INSEC 云思华盛

本地化服务

- 研发周期：2019年前
- 市场：公安

安恒-sumap

- 研发周期：2019年前
- 市场：公安
- *报价：高校、公安口与友商合作，如烽火*

远江盛邦-rayspace

- 研发周期：2019年前
- 市场：山东网安
- 产品：山东资产探测

潮汐-Tide

相似度：50-70%

互联网式数据服务

360-测绘

华信顺安-fofa

知道创宇-zoomeye

shodan

市场定价

硬件费用（预估）	
服务器	硬件（万元）
扫描器	0.5-1
爬虫器	1-3
应用端	3-6
数据服务器	3-6

终端价格		
客户等级	平台软件（万元）	说明
区县客户	39（一体化硬件）	2年免费升级，2年后20%升级费
地州客户 行业客户	59	
省会客户	79	

运营治理费用		
运营服务	职责	费用
定制开发	按需进行功能开发	1000人/天
现场运维	测绘技术咨询服务，解决数据查询、数据统计、数据治理、数据运营与运维工作	20-30W（人/年）

INSEC
云思华盛

谢谢

云思华盛

网络安全创新领航者