锦行科技
Jeeseen Technologies

诱

欺骗防御与威胁感知平台

幻云释义：“幻”-迷惑性、欺骗性；“云”-云与天齐，辐射范围大，由气及微小颗粒组成，无实质性。

锦行科技 Jeeseen Technologies

幻云

目　录

CONTENTS

01 网络安全现状

- 安全现状
- 事件原因分析

1.1-安全现状

欧洲能源巨头EDP遭网络攻击，被勒索近**1000万欧元**

- **美国**

国内最大燃油管道遭遇勒索软件攻击后，美国政府宣布进入**国家紧急状态**，以应对石油供应危机。

- **德国**

政府遭冠状病毒主题钓鱼攻击**损失数千万欧元。**

- **意大利**

跨国能源公司被攻击。

- **委内瑞拉**

国家电网干线遭攻击，**全国大面积停电。**

- **以色列**

供水部门工控设施遭到网络攻击。

- **阿塞拜疆**

政府和能源部门遭受黑客攻击。

- **伊朗**

纳坦兹核设施的配电系统遭受网络攻击，停电导致**离心机严重损坏**。

- **本田汽车** 遭受工业型勒索软件攻击，部分**生产系统中断。**

- **中国台湾**

两大炼油厂遭受勒索软件攻击，**加油站混乱。**

1.2-事件原因分析

缺乏内网威胁感知手段

IT系统安全建设**局限于边界防御体系**，内网防护脆弱不堪，缺乏有效的内网威胁感知手段。

难以应对新型高级威胁

高等级攻击隐蔽性强、攻击手段不断变化，使得**传统安全防御手段容易失效**，无法及时发现及有效应对。

各类安全手段作用范围存在局限

现有安全防护手段**只能作用于一定范围和过程**，缺少有效的数据融合和协同管理机制，无法预判系统安全漏洞并提前做好防御措施。

02 幻云介绍

- 幻云简介
- 产品架构
- 工作原理
- 产品优势
- 应用价值

2.1-幻云简介

幻云通过搭建高度仿真的业务系统诱引攻击者进入幻云蜜网，一旦发现攻击，将第一时间通知用户，让用户第一时间发现攻击，为用户争取宝贵的应急响应时间。同时，幻云将全面采集攻击数据，进行关联分析，预测攻击意图，协助用户重点防御核心资产，消除安全隐患。这些基于语境的威胁数据还可转化为标准的威胁情报输出，与您现有的的安全产品形成联动，增强协同防御的能力，共同抵御攻击者入侵。

幻云能检测和捕获勒索病毒、肉鸡挖矿、APT攻击等攻击事件数据，有效识别暴力破解、窃取数据、内网渗透等攻击手段，即使攻击者突破边界防御体系，幻云仍可持续作用，保护核心资产。

主要应用场景：

欺骗防御　数据安全　应急响应　威胁情报

重保特护　供应链安全　病毒勒索　资产保护

2.2-产品资质


首款获得公安部安全专用产品销售许可证的欺骗防御类产品
ISCCC信息安全产品认证
资质
围绕该产品已申请50余项发明专利，授权近30项
国内首款欺骗防御技术的网络安全产品

2.3-产品优势

蜜罐模板丰富

蜜罐模版全面覆盖常见windows、**Linux操作系统**，上百种业务应用，十余种常见工控规约，支持蜜罐定制化

可搭建漏洞利用环境

支持搭建丰富的漏洞利用环境，构建漏洞利用攻击链和预设攻击路径，提供给攻击者持续渗透的纵深空间

蜜罐交互多层次

幻云利用多种虚拟化技术构建多层次交互蜜罐，**可灵活构建丰富类型的仿真场景**

高集成、智能化平台

高度集成和智能化的管理平台，提供**全自动化**一键部署、全图形化的管理操作界面，简单易用，部署快捷

可构建真实网络环境

支持构建真实的政企单位网络环境，通过多种类型的蜜罐组网、多层次蜜网架构划分、丰富的虚假业务数据线索，构建**可承载复杂业务环境的沉浸式诱捕蜜网**

强大数据采集能力

强大的数据采集能力，可**全面捕获**网络层、系统层、内核层、应用层的攻击数据，提供基于攻击者视角的攻击回放、攻击关联分析等功能

2.4-客户应用

公安部第三研究所

首次蜜罐系统在国家部委运营系统成功应用案例（2017）

中信建投证券 CHINA SECURITIES

18年初首次建设落地。知名大型券商首个蜜罐落地案例

深圳证券交易所 SHENZHEN STOCK EXCHANGE

20年交易所5年框架采购，覆盖深交所以及旗下多个专业子公司

中国农业银行 AGRICULTURAL BANK OF CHINA

业界首个国有大行全行全覆盖案例，部署范围本部数据北京、上海数据中心及全国37家一级分行。目前业界装机数量最多的蜜罐项目（2020）

国家电网公司 STATE GRID CORPORATION OF CHINA

覆盖北京、山东、福建、甘肃、陕西、青海、湖南、四川等多个省份。并首次在国家大型攻防演练活动中通过蜜罐系统捕获境外攻击者获得单份报告加分3000的记录

中国工商银行 INDUSTRIAL AND COMMERCIAL BANK OF CHINA

业界首个国有大行蜜罐应用案例（2019）
蜜罐攻击反制技术首次应用

中国南方电网 CHINA SOUTHERN POWER GRID

21年南网总部集中采购，覆盖南网全部5省公司、总部、广州局、深圳局、双调、超高压

中泰证券 ZHONGTAI SECURITIES

18年首次建设落地。20年、21年多次扩容

招商银行 CHINA MERCHANTS BANK

中国民生银行 CHINA MINSHENG BANK

业界首个saas云蜜罐+高仿真场景定制搭建案例，适合大型攻防演练等场景

中国电信 CHINA TELECOM

业界首个5G蜜罐成功创新应用案例

中国平安 PING AN 金融·科技

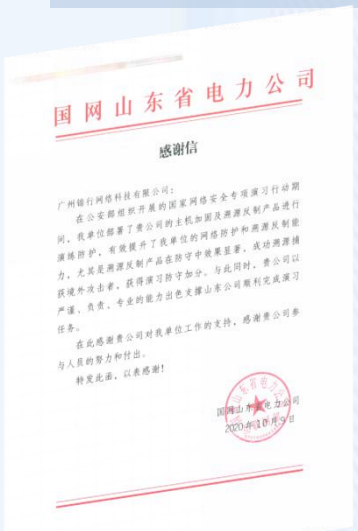
平安银行

18年首次落地，20年集团三年框架扩容采购，覆盖平安科技及集团旗下多个专业子公司

具有影响力的行业应用案例

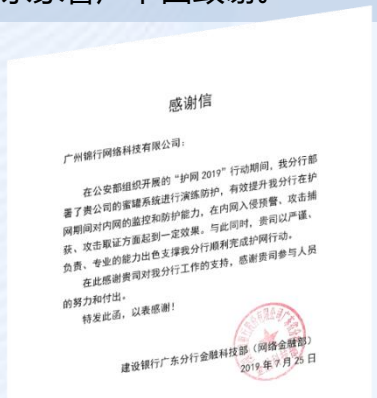
2.4-客户应用

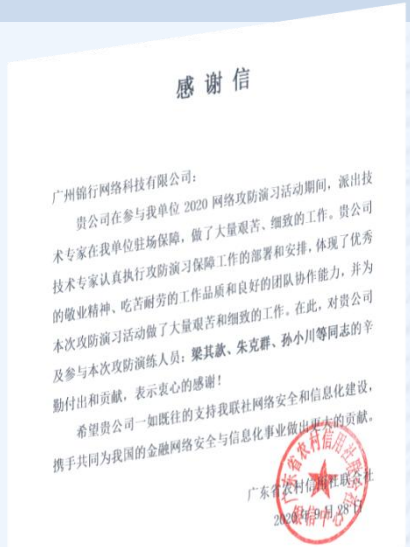
锦行科技蜜罐产品和专业的技术服务，多次在国家和各级政府组织的重大活动保障、攻防演练活动中帮助用户创造了价值、取得了出色的成绩，获得了包括深交所、民生银行、南方电网、建设银行在内的近30余家客户书面致谢。

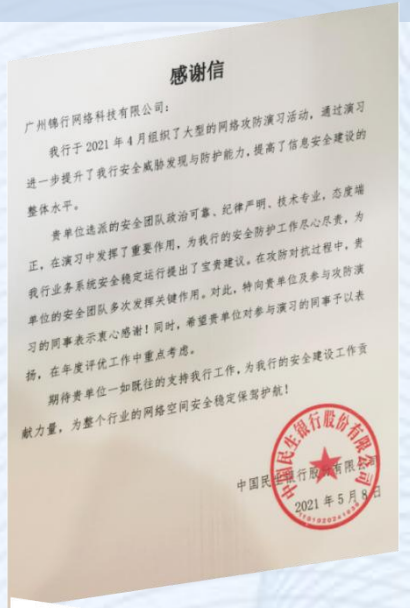

国网山东省电力公司

感谢信


感谢信

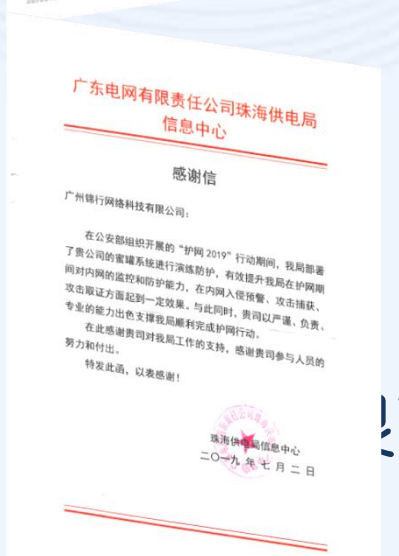

感谢信


感谢信

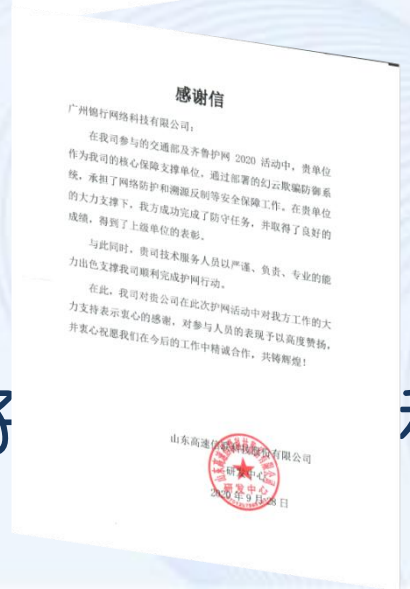

感谢信

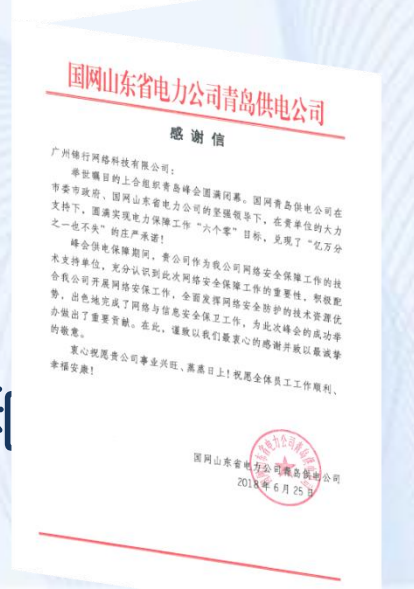

国网青海省电力公司
信息通信公司

感谢信

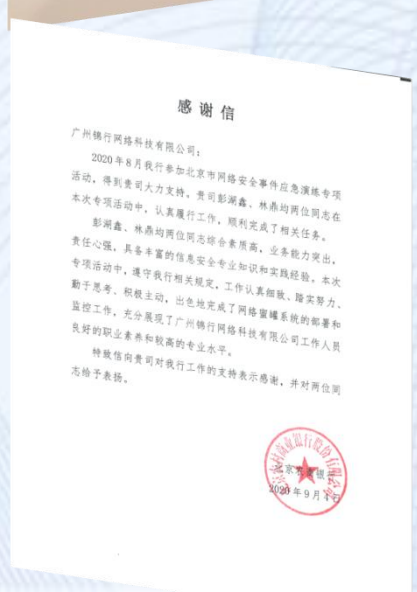

广东电网有限责任公司珠海供电局
信息中心

感谢信


感谢信


国网山东省电力公司青岛供电公司

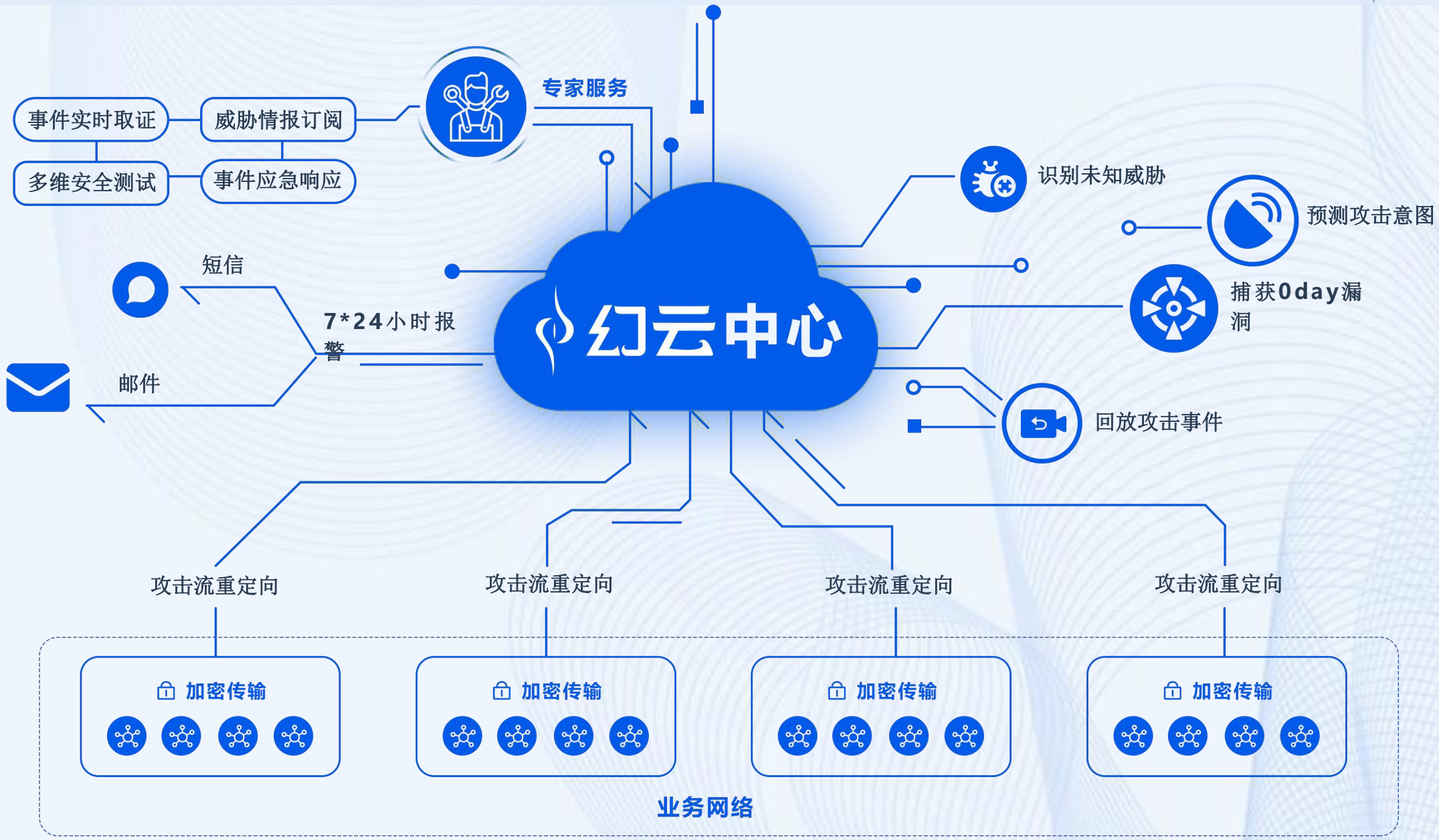
感谢信


感谢信

2.5-市场认可

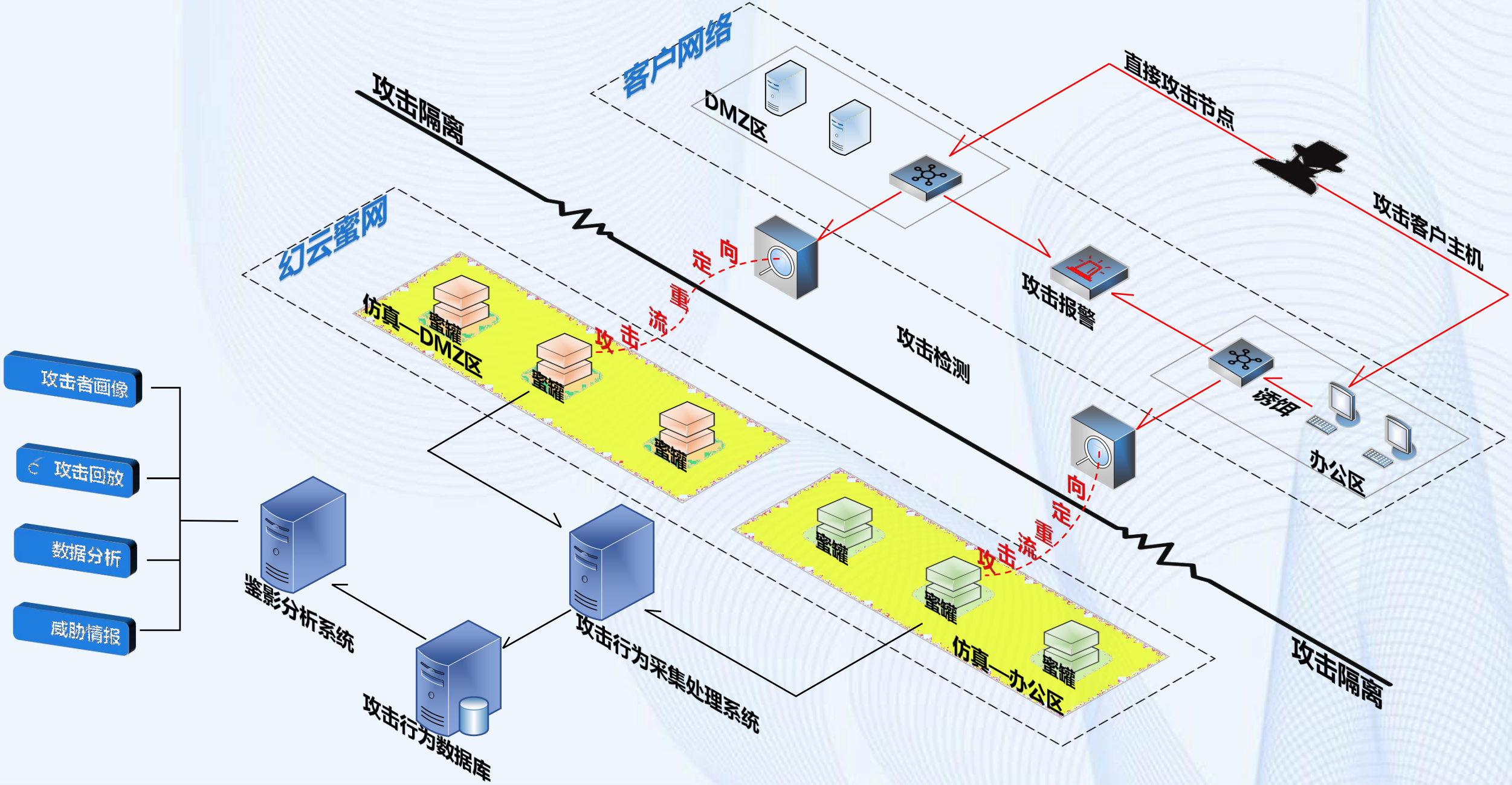
- 2022年安全牛《中国网络安全行业全景图》（第九版）上榜6大领域8项产品服务上榜；
- 荣获CCIA“2021中国网安产业成长之星”；
- 《2021年嘶吼●网络安全产业链图谱》欺骗防御等9项产品及服务上榜；
- 《2021郑州高新区●胡润中国网络安全企业百强》获得“中国最具成长潜力网络安全企业”；
- 2021年安全知名媒体freebuf发布《CCSIP 2021中国网络安全产业全景图》（第三版）欺骗诱捕/蜜罐、安全靶场、攻防演练、渗透测试产品入选；
- 2021年数说安全发布国内蜜罐产品顶级供应商，锦行科技蜜罐产品入选。《数说安全市场全景图》漏洞扫描与漏洞管理、欺骗防御、渗透测试、攻防实训/靶场产品上榜；
- 2021年数世咨询评选中荣获“创新者”称号；
- 2020年国内知名信息安全咨询机构数世咨询发布的2020网络安全能力图谱中，锦行科技上榜蜜罐欺骗防御专注领域厂商；
- 2020年数世咨询发布发布的“2020年网络安全创新能力100强”，锦行科技以“仿真技术新领域（蜜罐）”上榜。

2.6-产品架构



注：诱捕节点

2.7-工作原理


客户网络
DMZ区
攻击隔离
直接攻击节点
攻击客户主机
幻云蜜网
仿真—DMZ区
蜜罐
蜜罐
蜜罐
定向
重流
攻击
攻击检测
攻击报警
诱饵
办公区
定向
重流
攻击
仿真—办公区
蜜罐
蜜罐
蜜罐
攻击隔离
攻击者画像
攻击回放
数据分析
威胁情报
鉴影分析系统
攻击行为采集处理系统
攻击行为数据库

03 幻云特色

- 场景仿真
- 动态密网
- 诱饵系统

3.1-场景仿真

高交互蜜罐

- 基于虚拟机技术可仿真与真实操作系统和业务系统无差别的环境。
- 支持常见主流Windows系列蜜罐与Liunx系列蜜罐。
- 仿真程度高，占用资源大，成本高，适合针对性部署。
- 主要应用场景为攻击诱捕，提取攻击者信息。

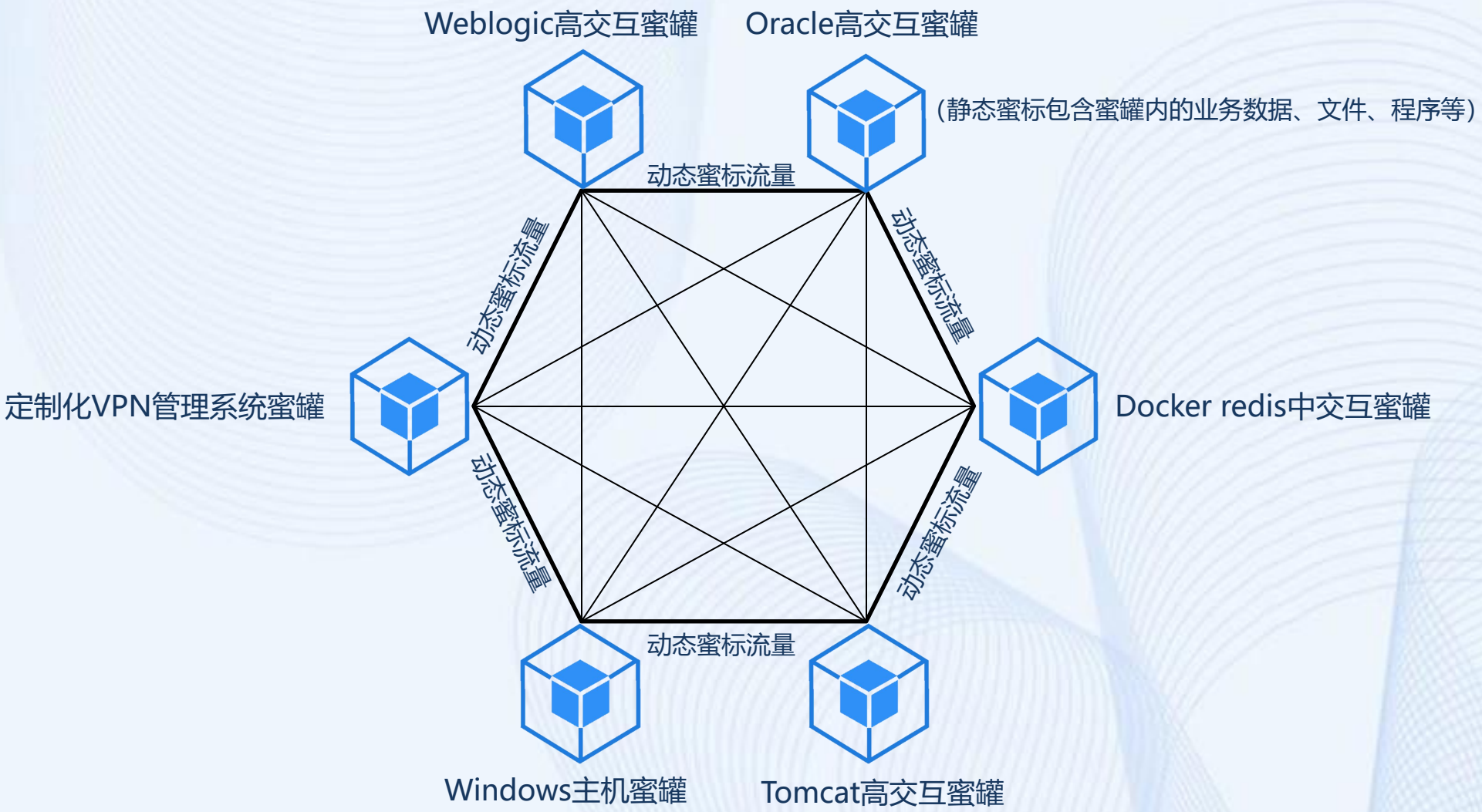
中低交互蜜罐

- 基于程序模拟和协议仿真。提供给攻击者有限交互环境。
- 支持常见网络服务模拟及全端口探测。
- 仿真程度低，占用资源小，成本低，适合大规模覆盖。
- 主要应用场景为攻击探测发现。

蜜网场景

- 通过蜜罐组网通讯，构建提供给攻击者渗透的内部蜜罐网络环境。
- 支持自定义搭建，可仿真典型企业内部网络区域如DMZ区、堡垒区、办公区、内网区域等。
- 提高场景真实度、拖延攻击者时间、提取更多攻击者的行为操作信息。

3.2-动态蜜网


Weblogic高交互蜜罐
Oracle高交互蜜罐
（静态蜜标包含蜜罐内的业务数据、文件、程序等）
动态蜜标流量
动态蜜标流量
动态蜜标流量
定制化VPN管理系统蜜罐
Docker redis中交互蜜罐
动态蜜标流量
动态蜜标流量
动态蜜标流量
Windows主机蜜罐
Tomcat高交互蜜罐

3.3-诱饵系统

轻量级脚本实现，安全系数高，可随时灵活卸载，对正常业务系统不会产生影响。

种类丰富， 兼容性高、可支持Windows、Linux系统的常见诱饵类型hostname诱饵、SSH公钥配置诱饵、RDP服务连接诱饵、HOSTS映射诱饵、XSHELL应用连接诱饵、SECURECRT应用连接诱饵、登录信息文本诱饵等二十余种诱饵类型。

完全基于攻击者视角出发的诱饵部署和诱导设计，准确布设在攻击者横向移动过程中的每个关键路径上。

全自动化的诱饵生成引擎，仅需在界面上输入诱饵相关自定义信息即可一键生成各种形态的诱饵信息。

04 产品功能

- 欺骗与转移
- 资产隔离
- 反制溯源
- 攻击捕获
- 攻击回访
- 攻击展示
- 数据分析
- 数据统计
- 报警通知
- 态势输出
- 集群管理
- 安全设置

4.1-欺骗与转移

① 直接诱导

弱口令、漏洞等引诱攻击

诱捕节点

攻击转移

② 间接诱导

直接攻击

业务主机

证书、密钥、cookies、
账号密码等各种凭证
诱引攻击

诱捕节点

攻击转移

③ 诱饵类型

Linux：host、bash_history、SSH登陆凭证

Windows：host、3389登陆日志、工具登陆痕迹（Xshell、secureCRT）、账号密码记录

4.2-资产隔离

注：真实主机　幻云蜜罐　诱捕节点

4.3-反制溯源

一代溯源

一代的溯源方式，是基于威胁情报分析和攻击数据采集系统等，对攻击者的IP地址、MAC地址、社交ID、行为手段等进行采集。

新一代溯源

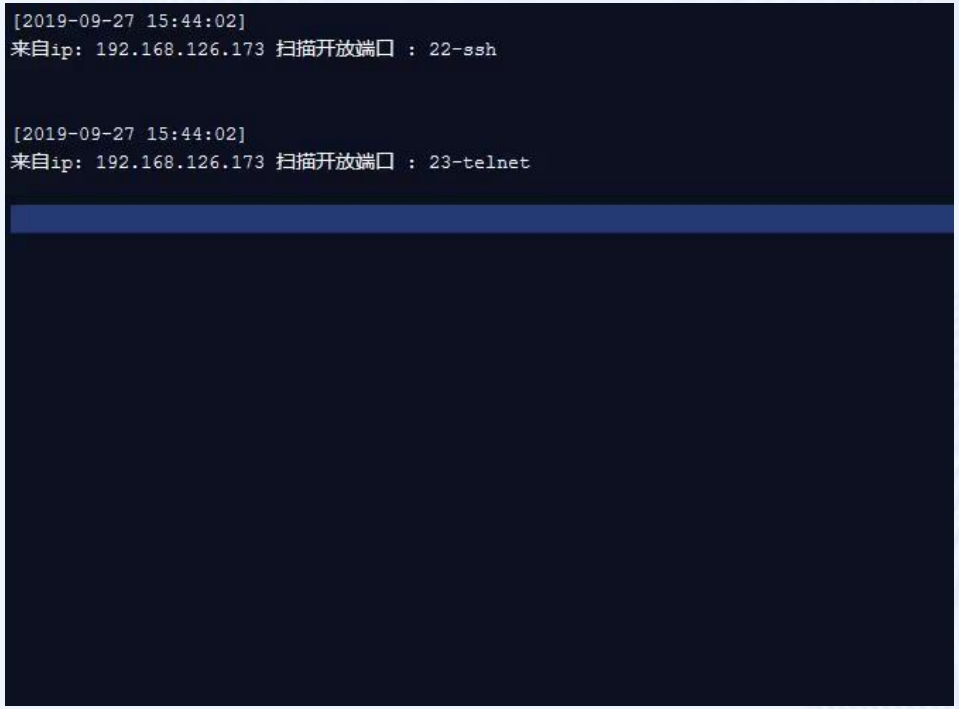
锦行科技提出的下一代新型溯源方式，具备独创的定制化反制溯源模块，可在法律允许的框架内诱捕攻击者执行幻云的远程溯源模块，不仅可以主动对攻击者身份信息进行精准采集，还可以对攻击进行控制，比如，控制其摄像头获取其真人照片，控制其麦克风获取其声音特征。

4.4-攻击捕获

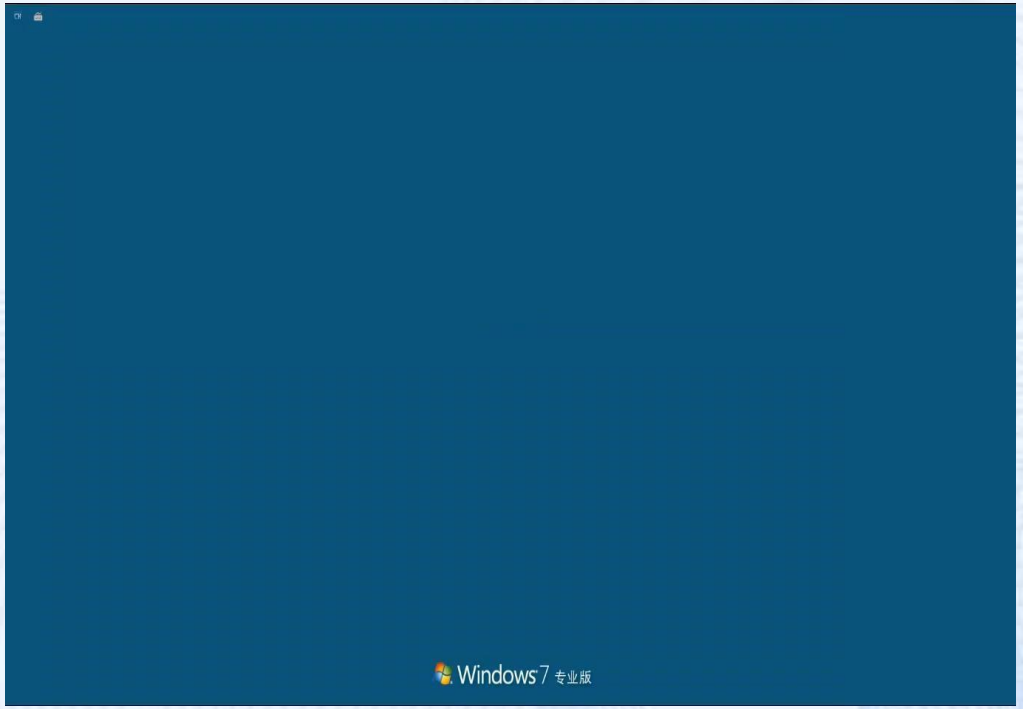
- 攻击事件日志
  - **异常流量捕获**：对所有异常流量进行7*24小时监控和报警
  - **蠕虫端口扫描**：常见蠕虫端口扫描报警：135、137、138、139、445、1434、6379、4444.....
  - **漏洞利用攻击**：全程捕获和还原已知/未知的系统漏洞利用攻击行为
  - **Arp欺骗捕获**：捕获Arp欺骗过程的全部数据
  - **嗅探行为捕获**：捕获半开放扫描和ping行为数据
  - **捕获原始数据包**：攻击流量全流量抓包，并提供原始数据包留存提供分析

4.5-攻击回放

指令回放



Win蜜罐RDP录屏回放



4.6-攻击展示

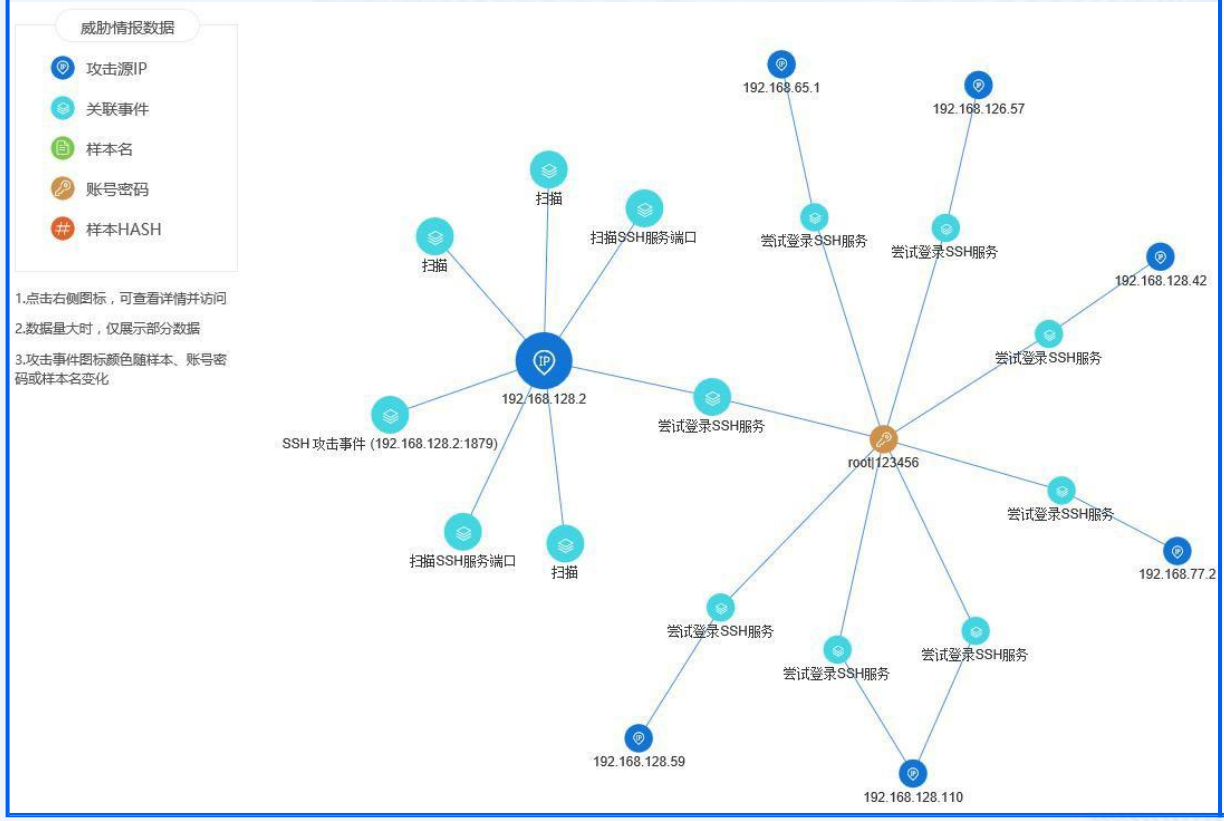
攻击态势大屏

通过数据大屏
实时观看攻击全景态势感知展示

4.7-数据分析

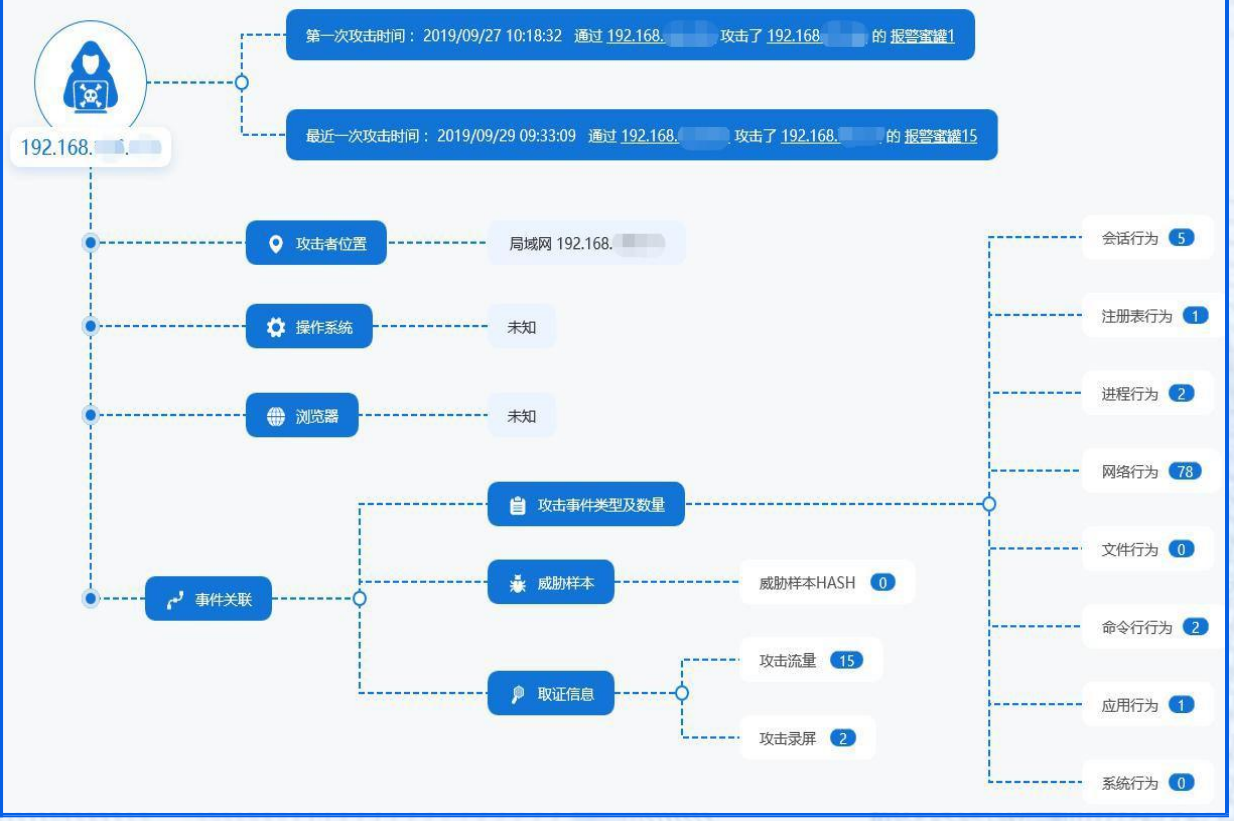
威胁数据分析

协助客户分析攻击行为和攻击者特征，同时威胁情报可导至其他安全防护设备，提升协同防御能力



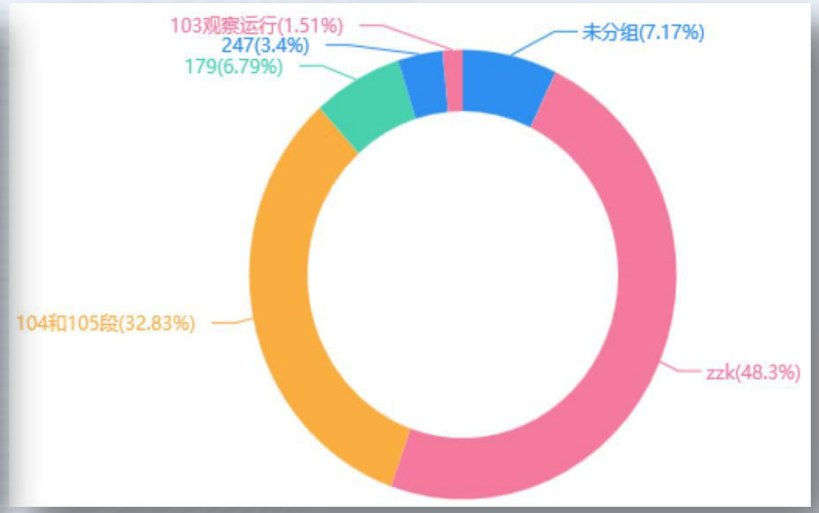
攻击者画像

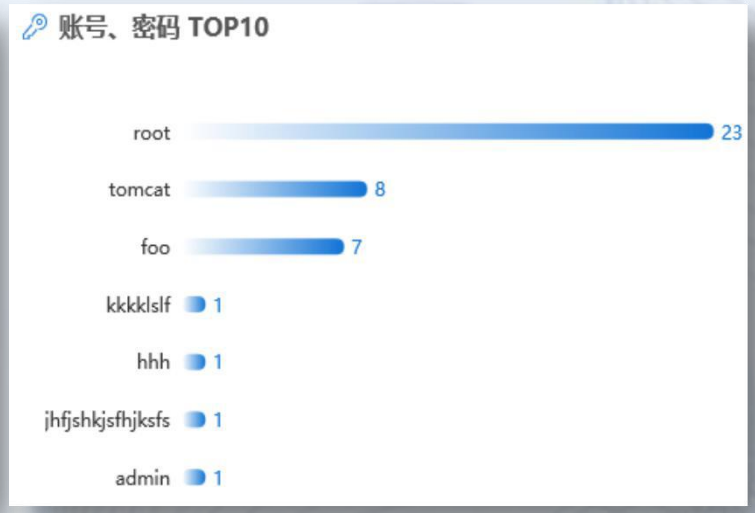
对攻击者行为特征的“画像”功能，便于溯源分析、攻击意图分析等

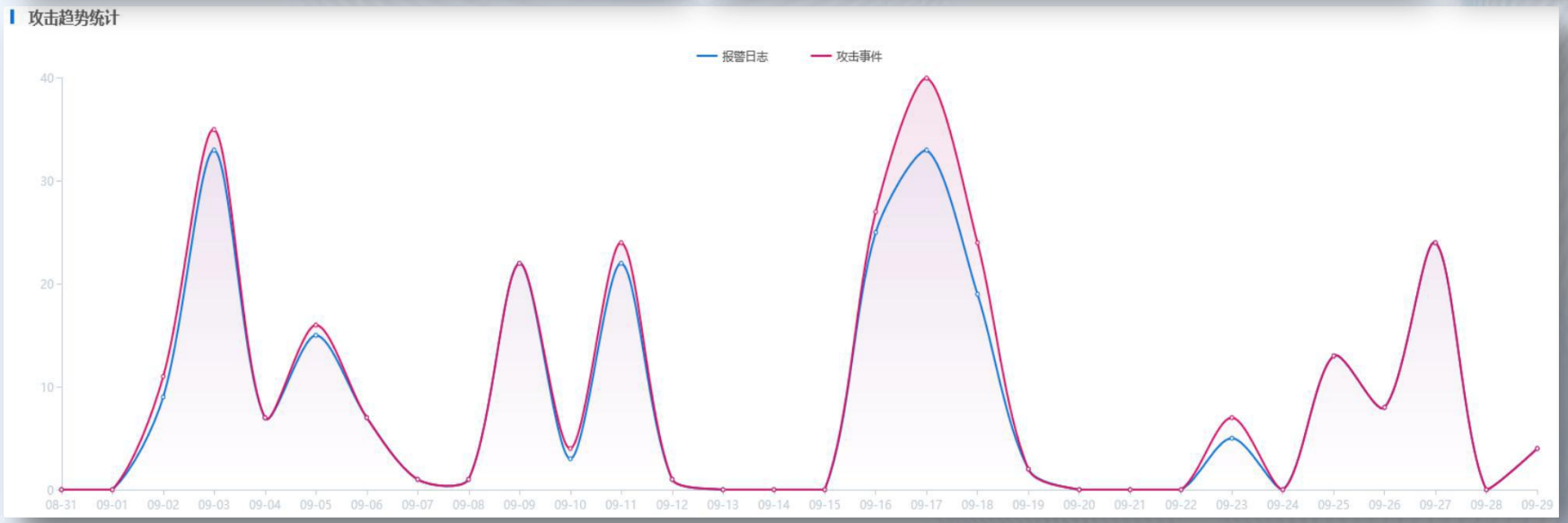


4.8-数据统计


被攻击服务 TOP10
ssh 83
rdp 66
http 34
redis 14
mysql 12
IEC104 4
samba 3
telnet 2
mssql 2
oracle_database 2


103观察运行(1.51%)
247(3.4%)
179(6.79%)
未分组(7.17%)
104和105段(32.83%)
zzk(48.3%)


账号、密码 TOP10
root 23
tomcat 8
foo 7
kkkklslf 1
hhh 1
jhfjshkjsfhjksfs 1
admin 1


攻击趋势统计
报警日志
攻击事件
40
30
20
10
0
08-31 09-01 09-02 09-03 09-04 09-05 09-06 09-07 09-08 09-09 09-10 09-11 09-12 09-13 09-14 09-15 09-16 09-17 09-18 09-19 09-20 09-21 09-22 09-23 09-24 09-25 09-26 09-27 09-28 09-29


攻击源IP TOP10
192.168.65.1 89次
192.168.126.57 22次
192.168.126.47 19次
192.168.126.173 17次
10.60.179.1 16次
192.168.128.59 15次
192.168.128.110 11次
192.168.128.2 11次
192.168.75.30 10次
192.168.128.180 9次

4.9-报警通知

报警等级

根据攻击类型的危害程度不同，对攻击类型进行分级；

报警规则

对测试流量、特定IP进行报警通知过滤；

过滤规则

对特定IP和端口进行检测过滤，避免误报；

4.10-威胁态势输出

支持三种形式输出威胁态势

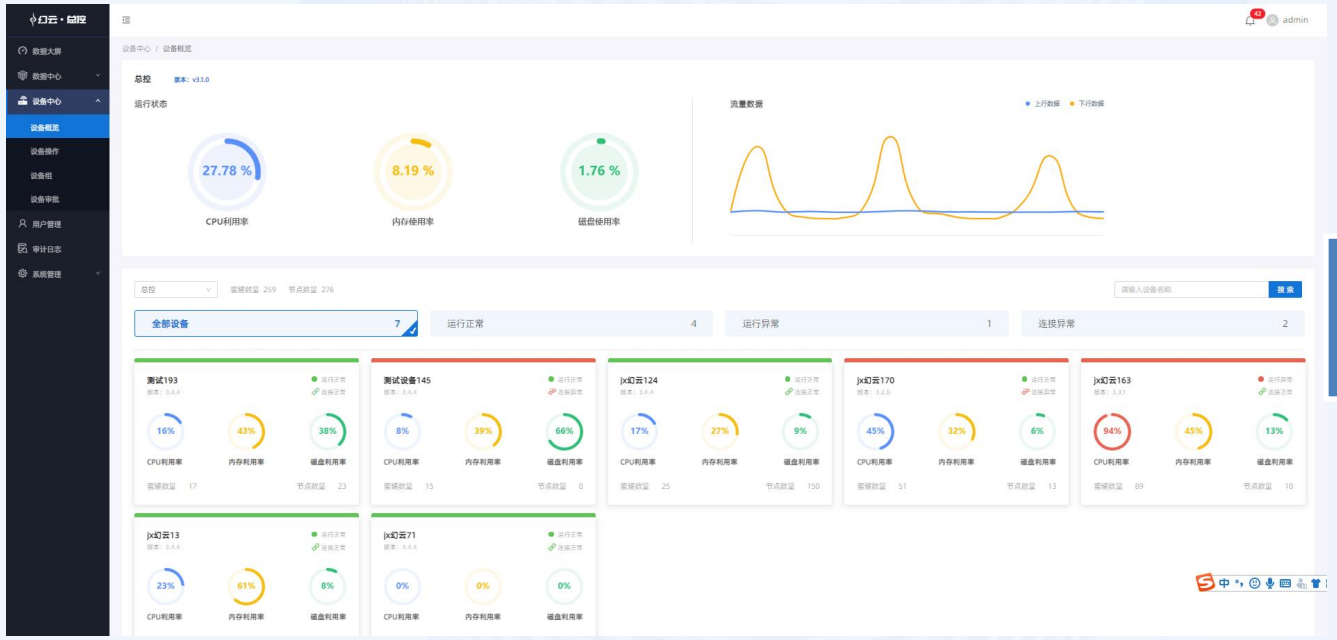
幻云基于攻击数据智能分析的结果，自动加工形成标准威胁态势统计报表输出，支持多种推送方式。

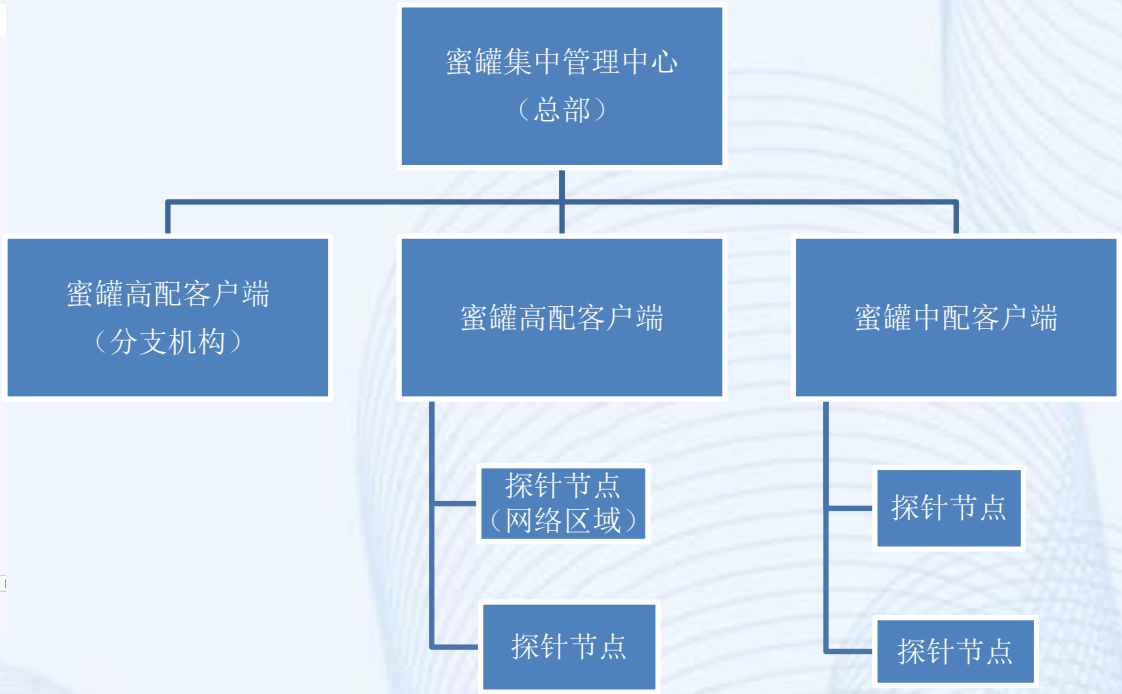
（指定邮箱每月或每季度定时收到报表）

（实时生成报表并本地下载）

（实时生成报表并发到邮箱）

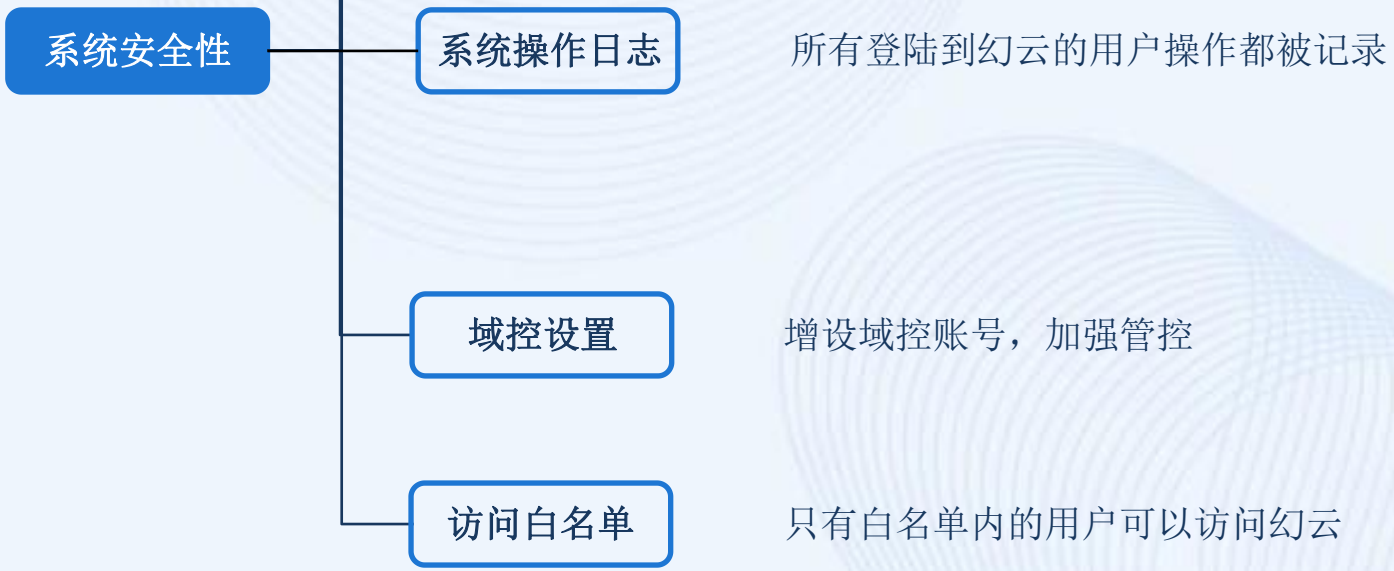
4.11-集群管理





针对一些网络规模较大、具备众多分支机构的大型政企单位，产品还支持进行蜜罐服务端的分布式集群管理，实现全机构范围内的集群化部署覆盖和总部统一集中管理。

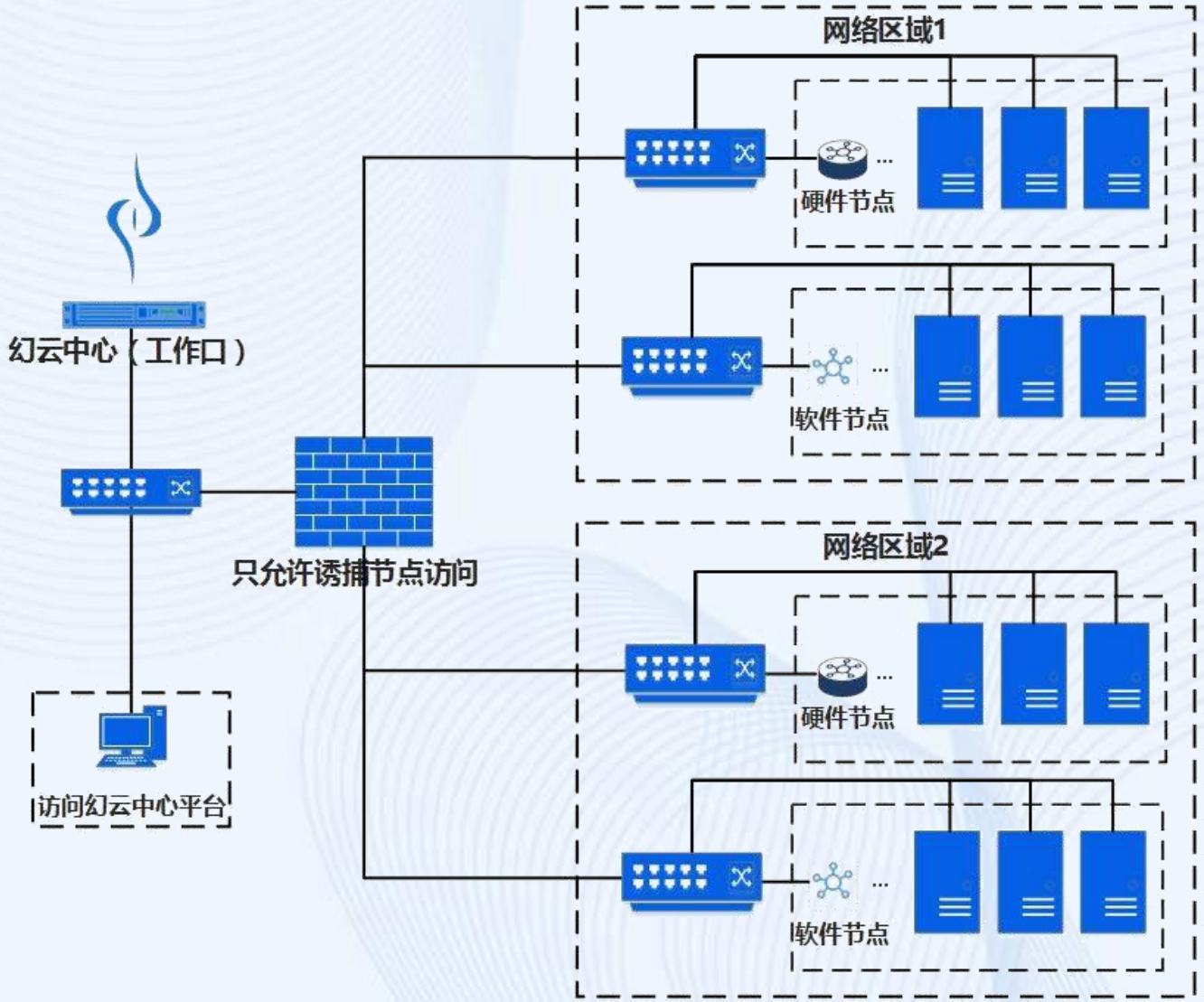
4.12-安全设置


系统安全性
登陆安全设置
管理员锁定时间
管理员身份验证过期时间
运行密码错误次数
分配用户权限
为不同的用户分配不同的权限
系统操作日志
所有登陆到幻云的用户操作都被记录
域控设置
增设域控账号，加强管控
访问白名单
只有白名单内的用户可以访问幻云

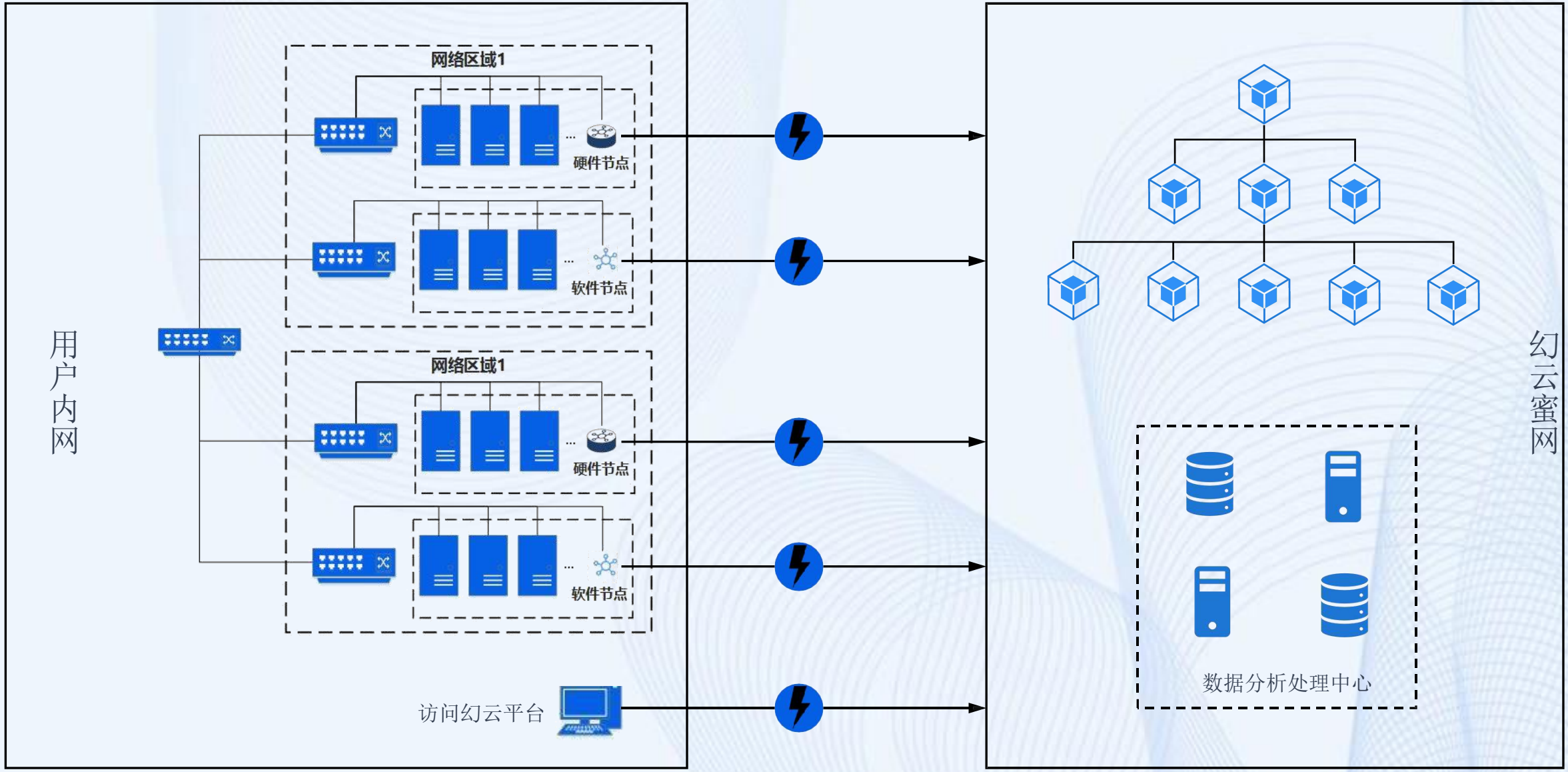
05 部署应用

- 本地部署
- 云端部署
- 部署流程

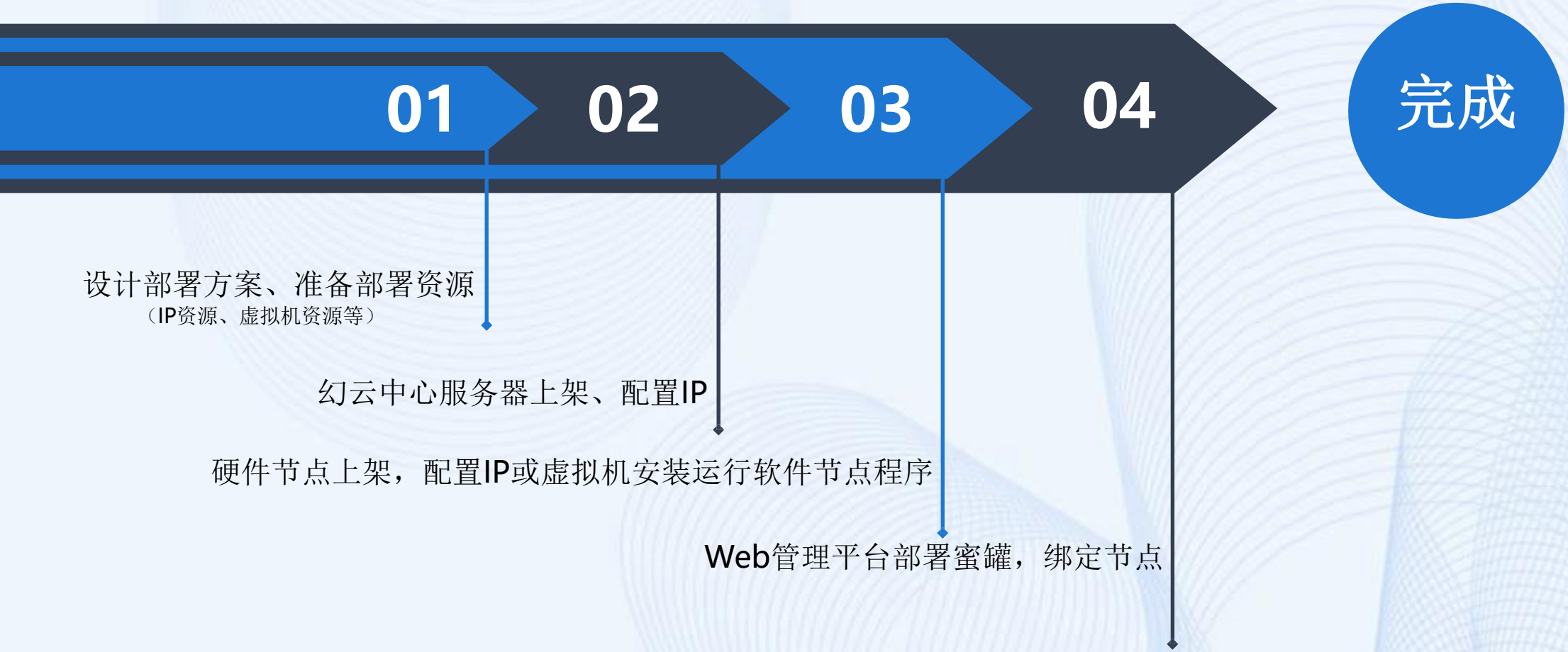
5.1-本地部署


网络区域1
硬件节点
软件节点
幻云中心（工作口）
只允许诱捕节点访问
网络区域2
硬件节点
软件节点
访问幻云中心平台

5.2-云端部署



5.3-部署流程

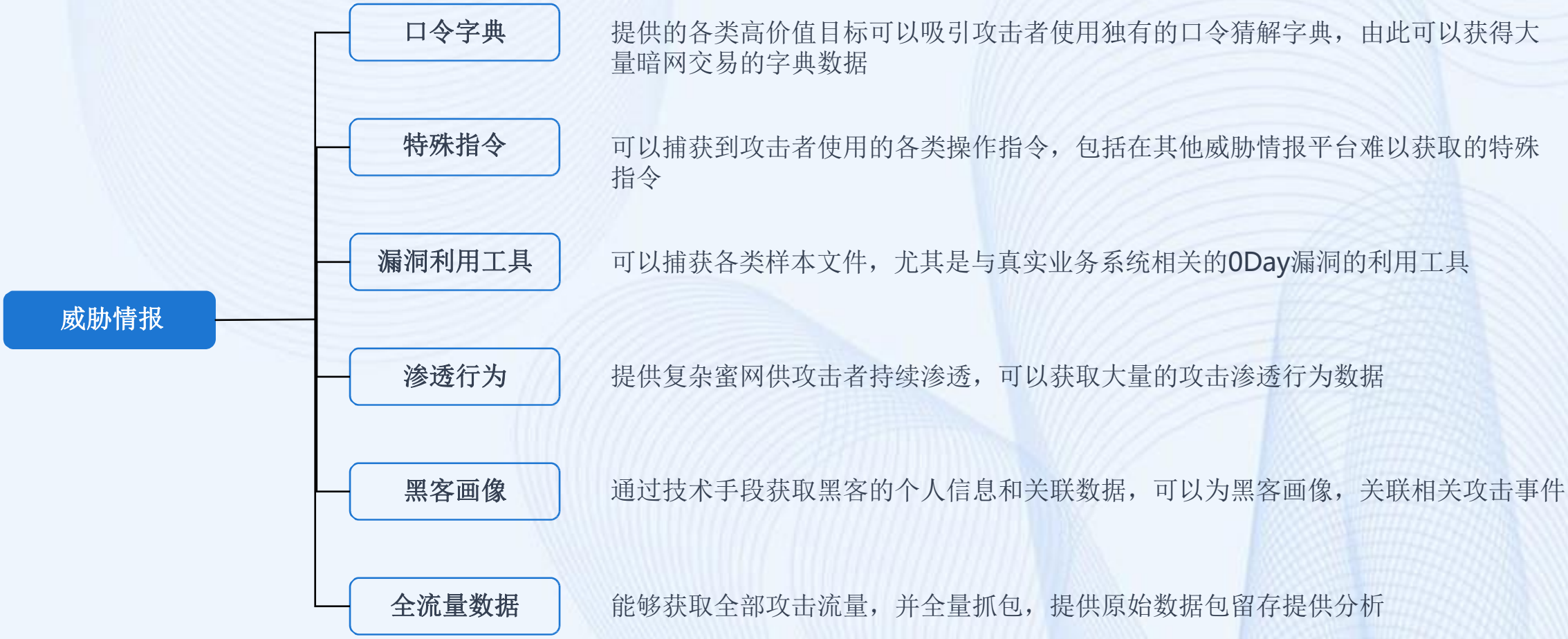

01
02
03
04
完成
设计部署方案、准备部署资源
（IP资源、虚拟机资源等）
幻云中心服务器上架、配置IP
硬件节点上架，配置IP或虚拟机安装运行软件节点程序
Web管理平台部署蜜罐，绑定节点

06 威胁情报

- 高价值威胁情报
- 标准化输出

6.1-高价值威胁情报

幻云使用轻量级节点，可以方便快捷的部署在互联网中，通过业务仿真技术、动态绑定蜜罐技术、复杂蜜网技术等，可以为客户捕获大量的高价值威胁情报数据，进而为态势感知平台提供高精准的威胁数据。



6.2-标准化输出

幻云支持以IOC标准化威胁情报数据的格式输出威胁数据，同时支持API接口、syslog等数据同步方式提供高价值威胁情报的输出和再利用。可以为各类威胁情报平台、态势感知平台、SOC平台等提供各类标准化的威胁数据。

幻云

感谢您的观看！

THANK YOU FOR WATCHING!

锦行科技
Jersect Technologies