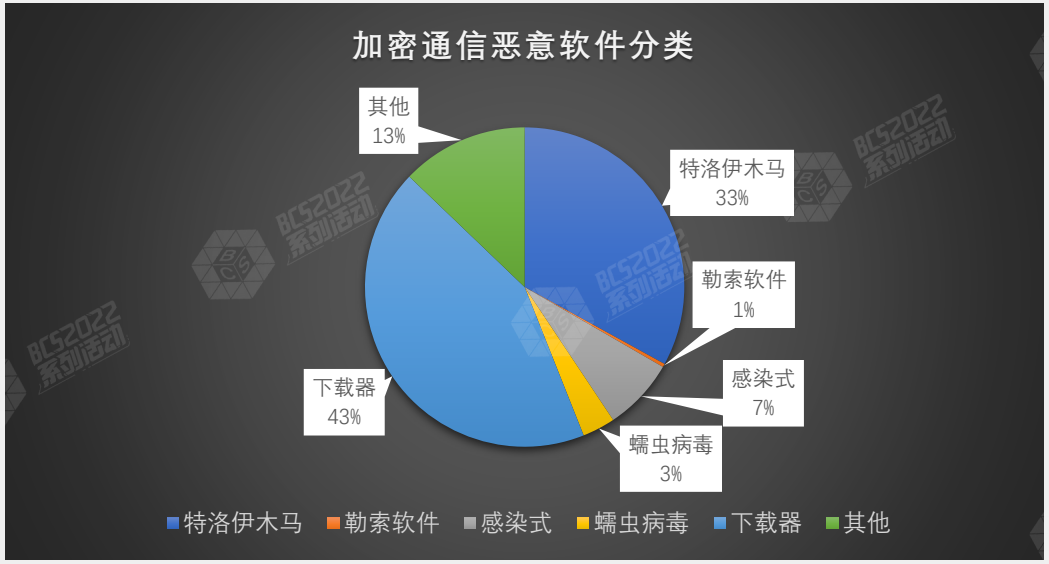
2022北京网络安全大会
2022 BEIJING CYBER SECURITY CONFERENCE
全球网络安全 倾听北京声音

基于加密流量的威胁检测与响应

观成科技 联合创始人/于海东

威胁加密化趋势明显

恶意软件转向加密通信占比大幅提升



使用加密通信样本所占比例**超过40%**；

使用加密通信样本家族数量**超过300种**；

每日新增加密通信恶意样本数量**超过1000个**；

几乎覆盖了所有常见类型，如：**特洛伊木马、勒索软件、感染式、蠕虫病毒、下载器等。**

黑客工具支持各类型加密流量

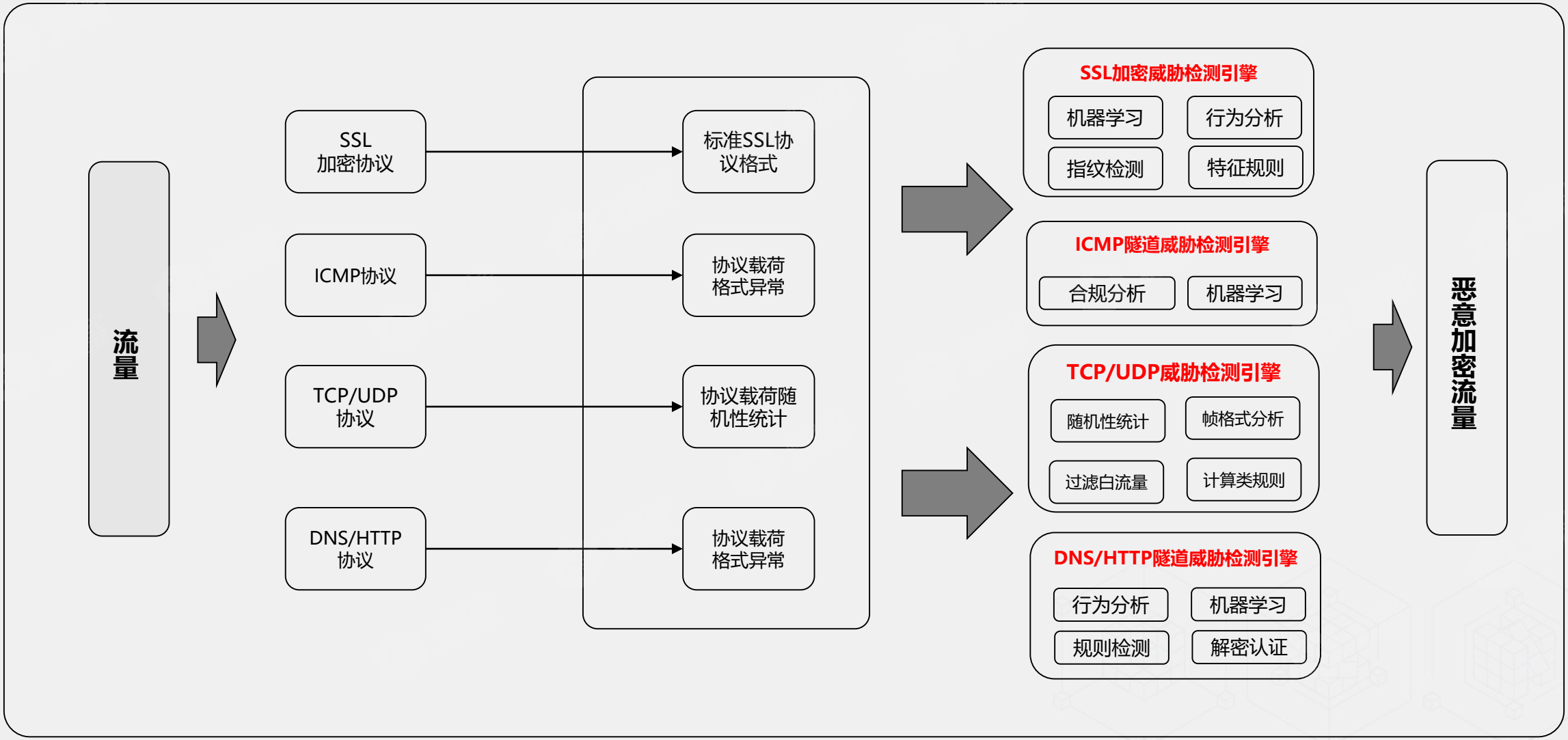
SSL加密 | **HTTP隧道加密** | **ICMP隧道加密** | **DNS隧道加密**

APT攻击加密通信已成为主流

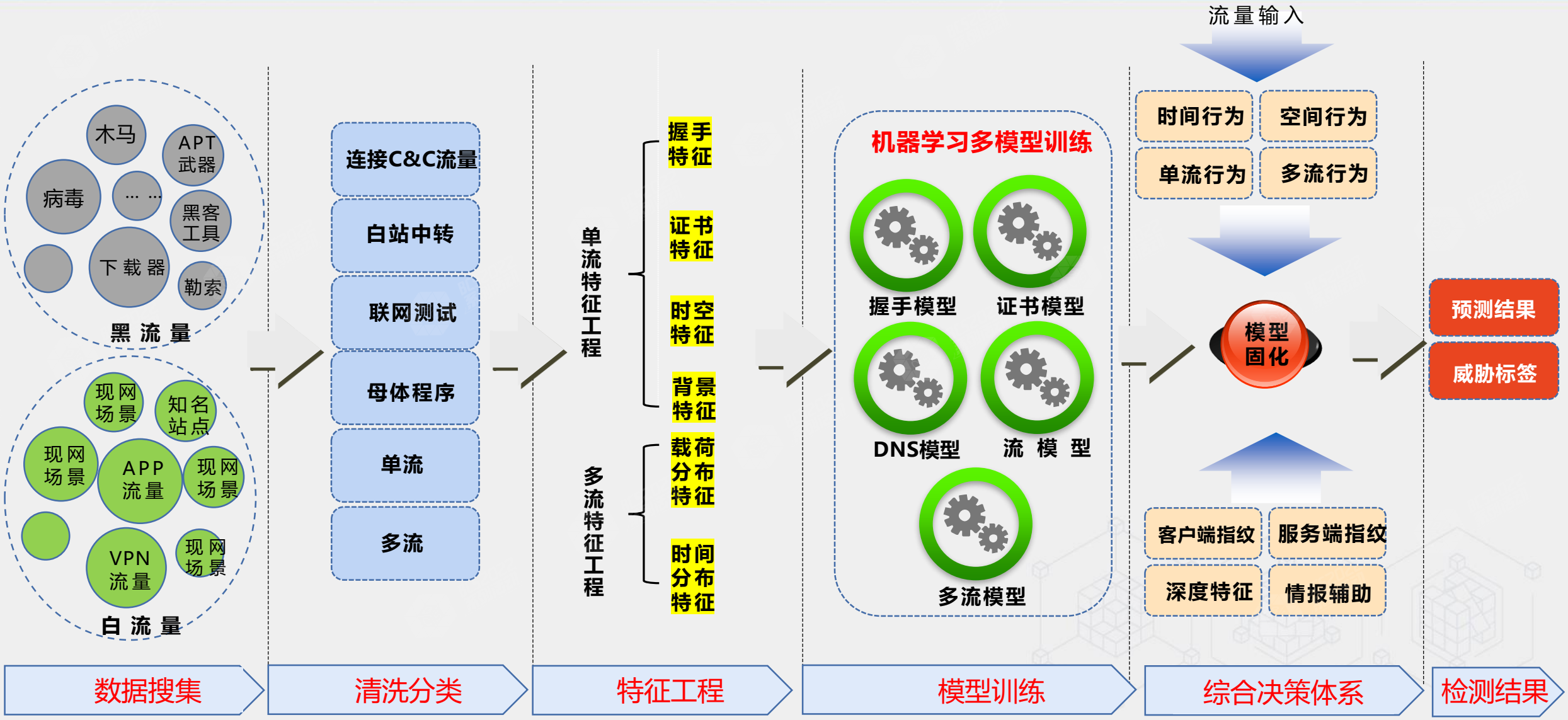
恶意加密流量类型总结

分类	标准加密协议	隐蔽隧道（非标准加密协议）		
	①SSL加密	②网络层隧道（ICMP等）	③传输层隧道（TCP/UDP/SCTP等）	④应用层隧道（DNS/HTTP等）
部分重要APT组织恶意样本	美：Equation Group 美：CIA 俄：Turla 俄：APT28、APT29 朝：Group123 印：响尾蛇、白象 越：OceanLotus	美：CIA 俄：Turla	美：Equation Group 美：CIA 俄：Turla 俄：APT28 朝：Group123 印：蔓灵花、白象 越：OceanLotus	越：OceanLotus 俄：Turla
部分黑客工具	Cobalt Strike Metasploit 等	Icmpsh PingTunnel Icmptunnel ptunnel-ng Icmpdoor icmptx	Metasploit	Cobalt Strike Metasploit Godzilla Behinder ABPTTS reGeorg HTTPTunnel Dns2tcp

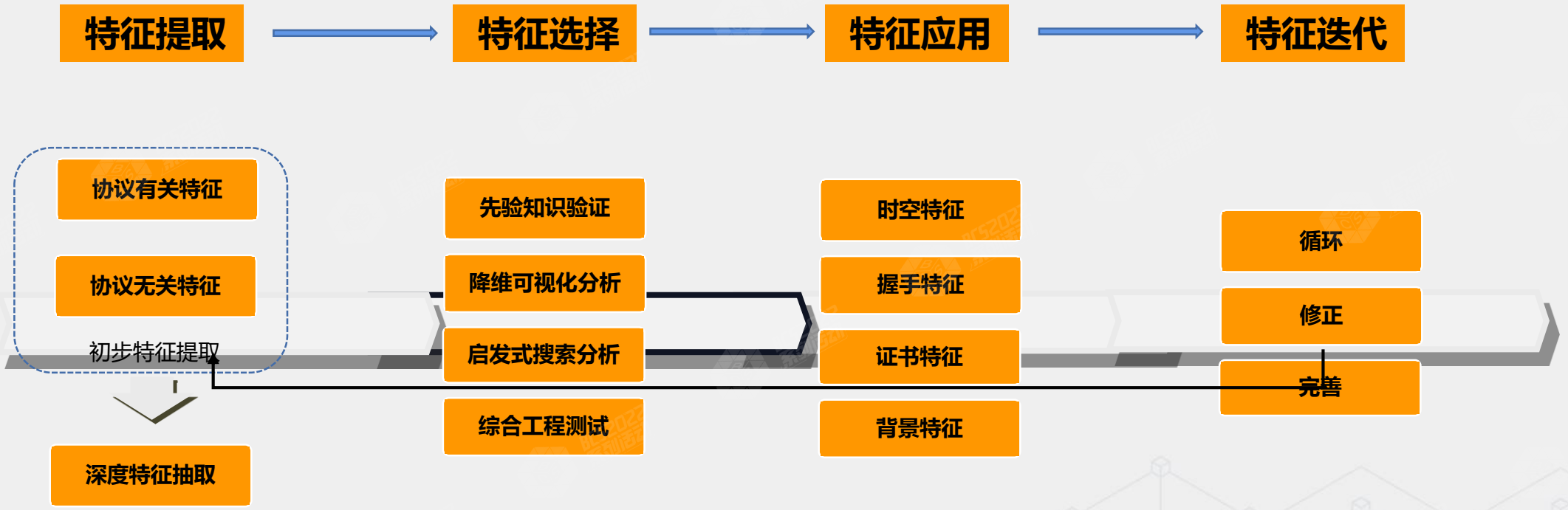
恶意加密流量检测概要技术路线



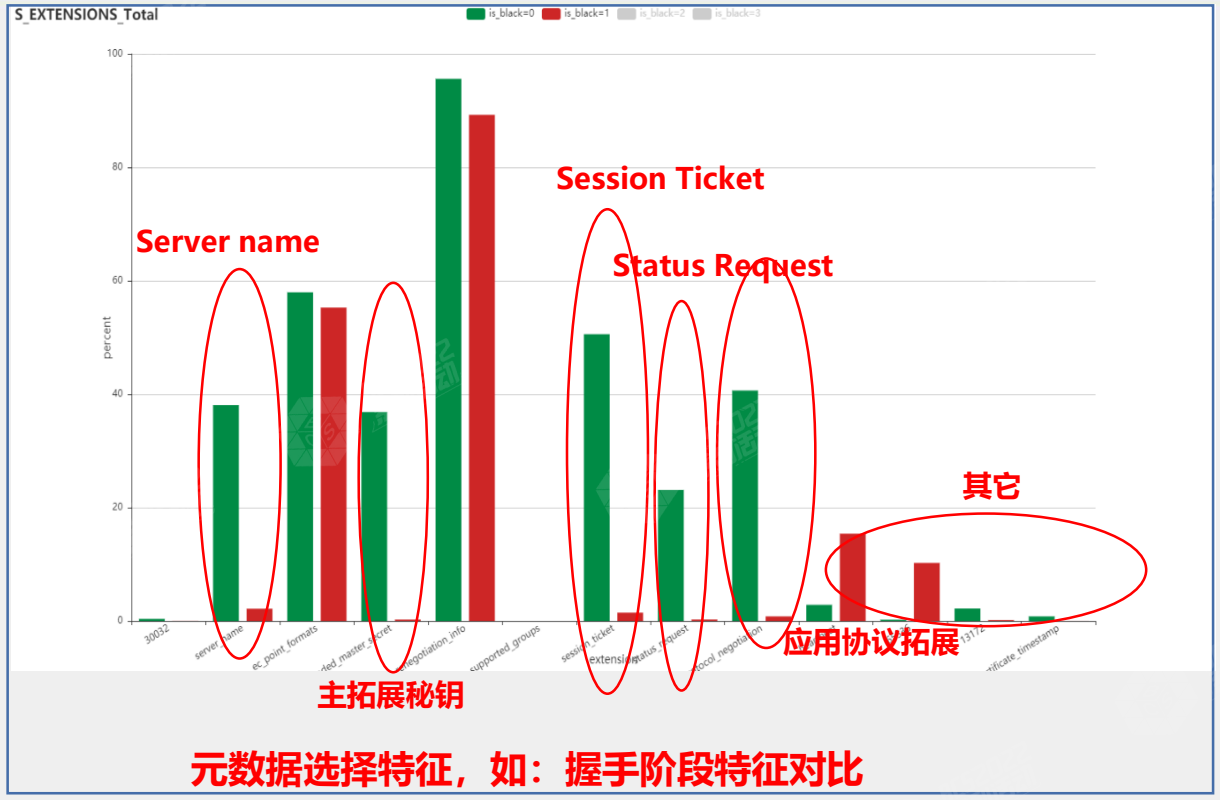
SSL加密检测技术路线



特征工程构建方法


特征提取
特征选择
特征应用
特征迭代
协议有关特征
协议无关特征
初步特征提取
深度特征抽取
先验知识验证
降维可视化分析
启发式搜索分析
综合工程测试
时空特征
握手特征
证书特征
背景特征
循环
修正
完善

单流（一次会话）层面特征工程



元数据选择特征，如：握手阶段特征对比

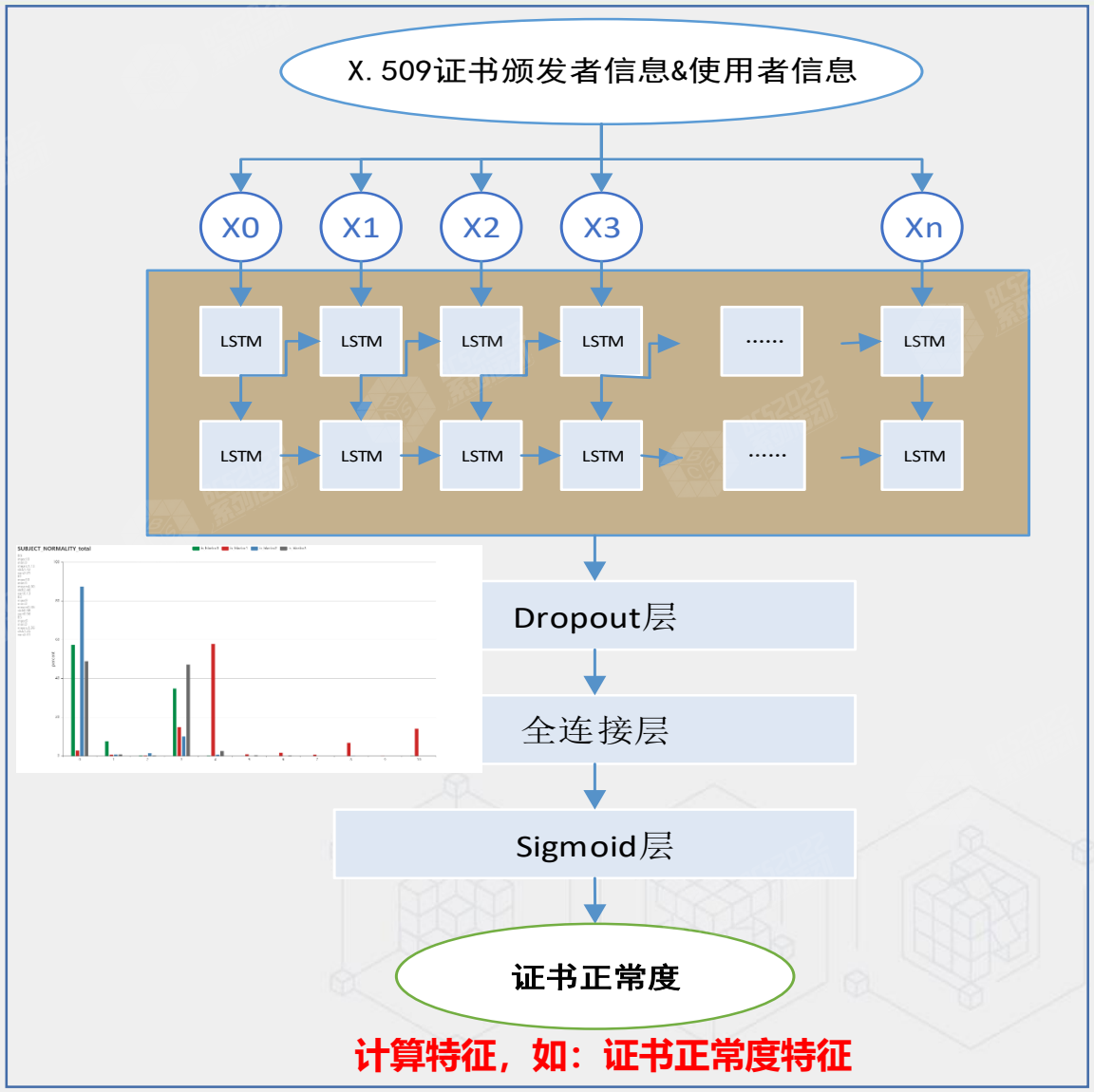
时空特征：时间特征，如流时长、包间隔等；空间特征，如包大小转移矩阵、熵值等。

握手特征：客户端和服务端在握手阶段的特征。如协议版本、支持的扩展项等。

证书特征：使用的数字证书的一系列特征。如证书链长度、使用者正常度等。

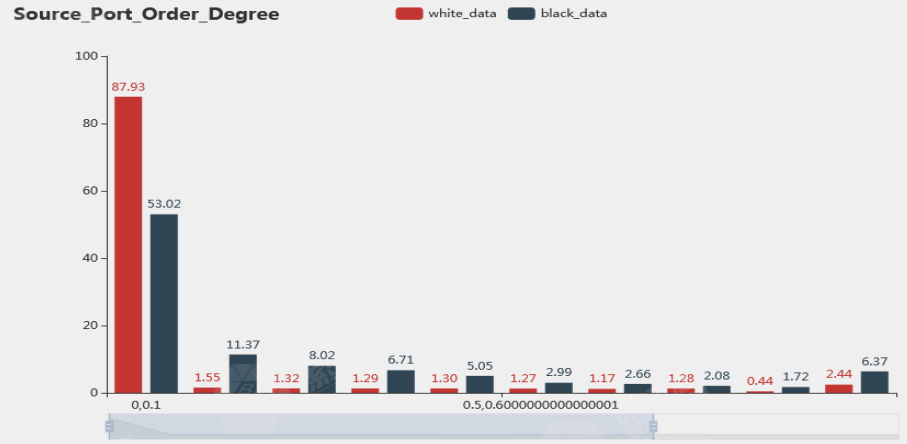
背景特征：指从背景流量中提取并选择的一类特征，如DNS、HTTP等背景流量特征。

四个维度，构建1500余种特征。

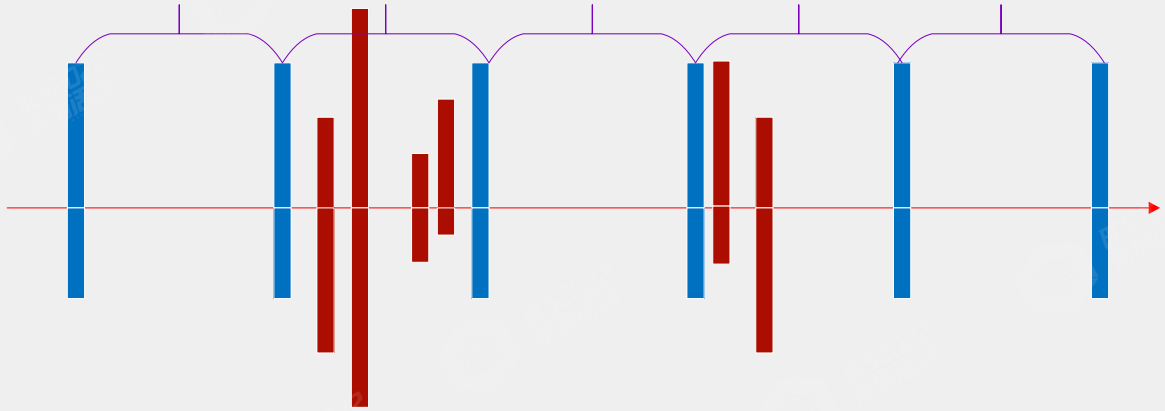


计算特征，如：证书正常度特征

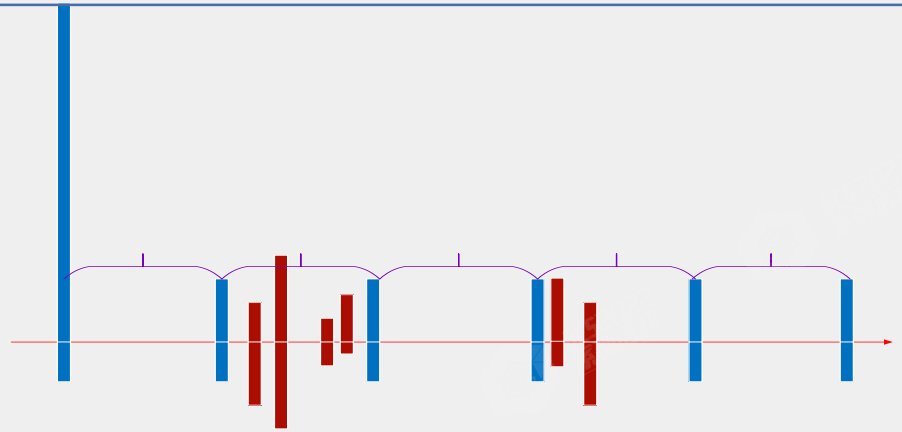
多流（多次会话）层面特征工程（400余种）



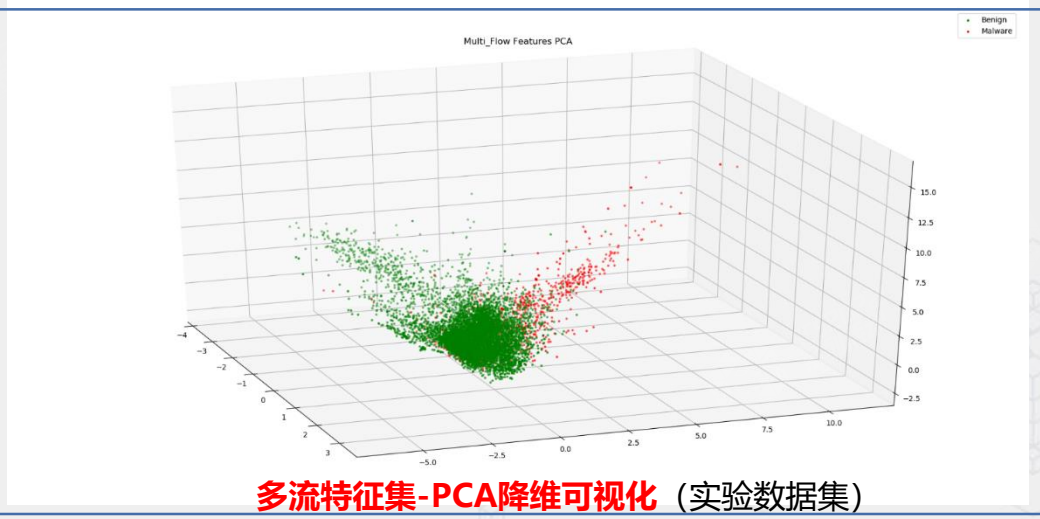
源端口有序度：可反映桌面操作与程序自动发包的区别



流簇上/下行首流相似度：可反映含噪声的心跳行为

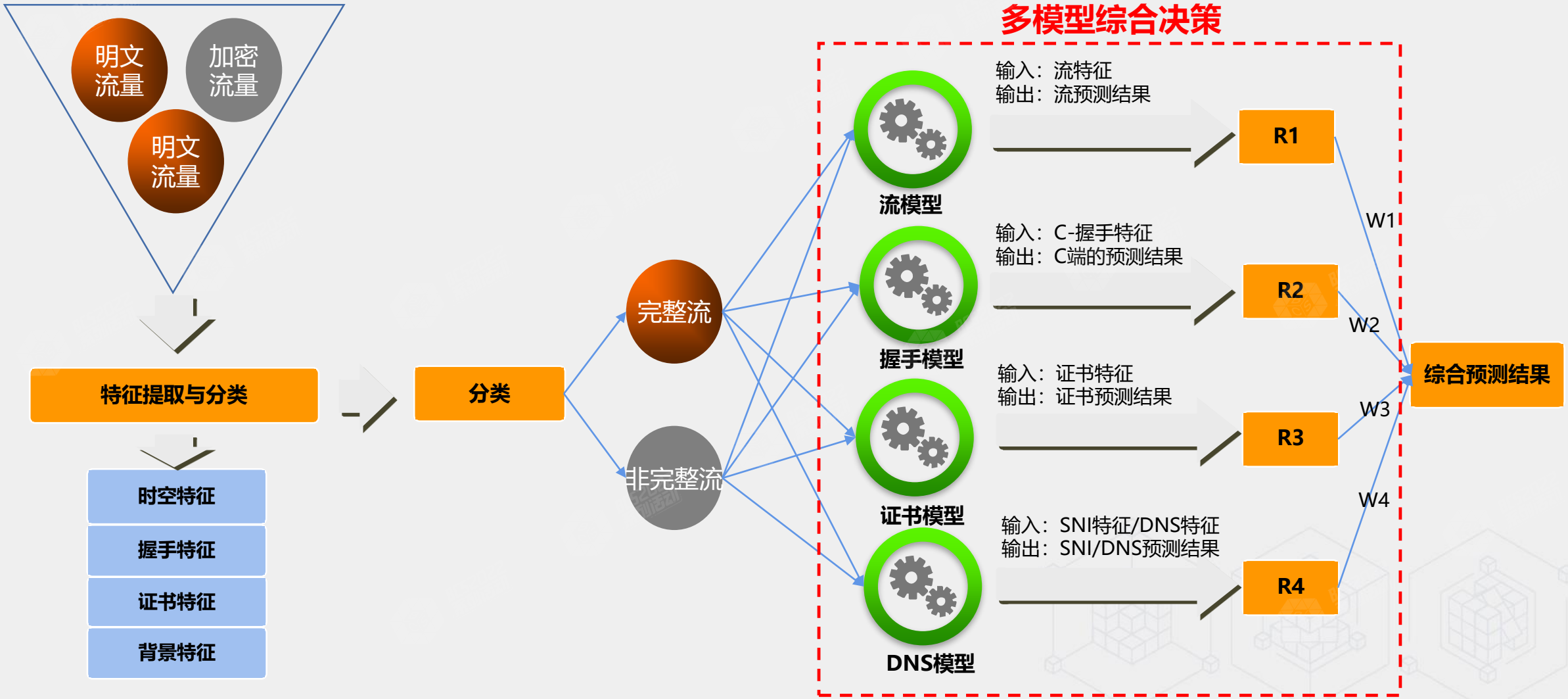


流簇上/下行首流畸形度：可反映上线信息+下发执行+心跳

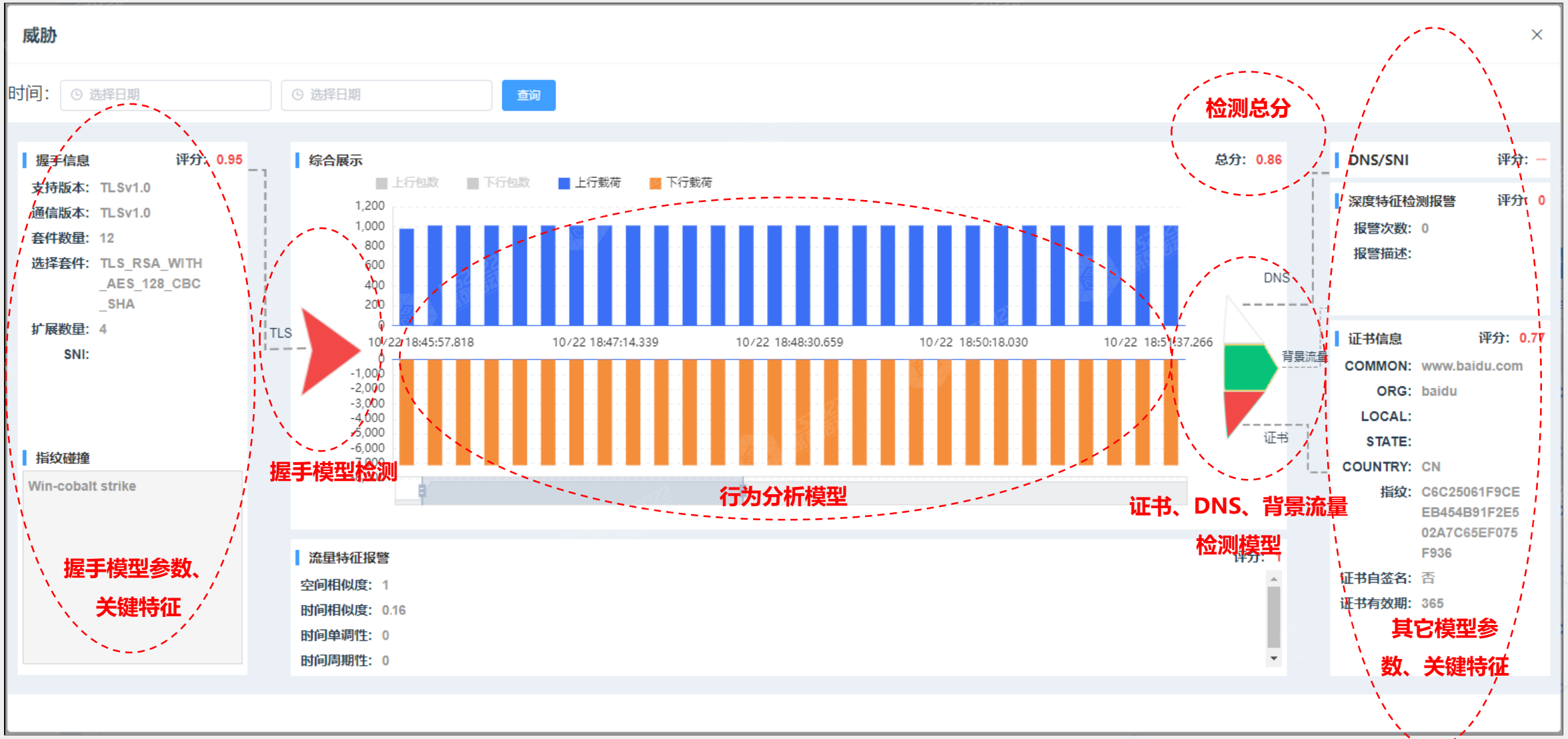


多流特征集-PCA降维可视化（实验数据集）

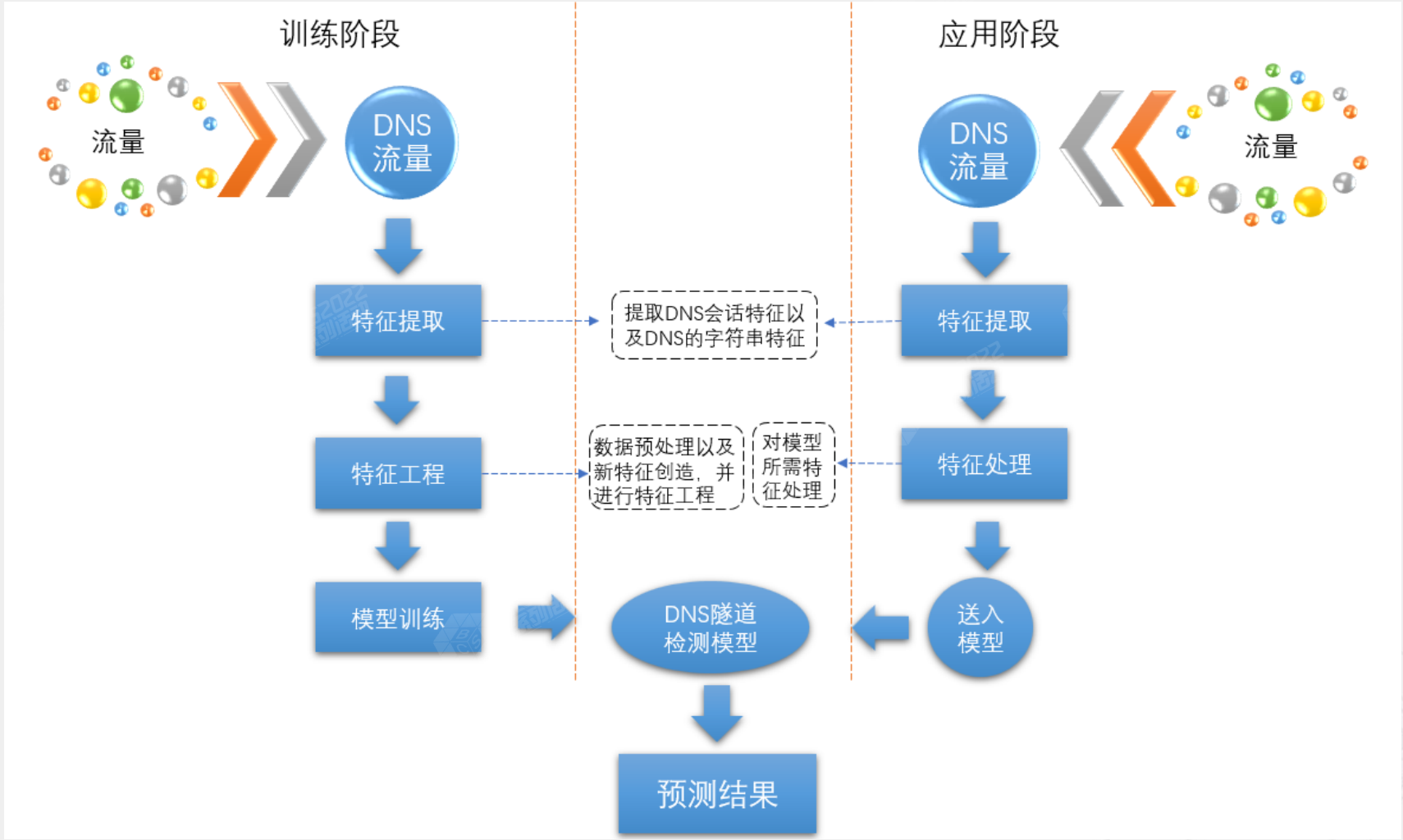
SSL加密威胁检测：机器学习多模型



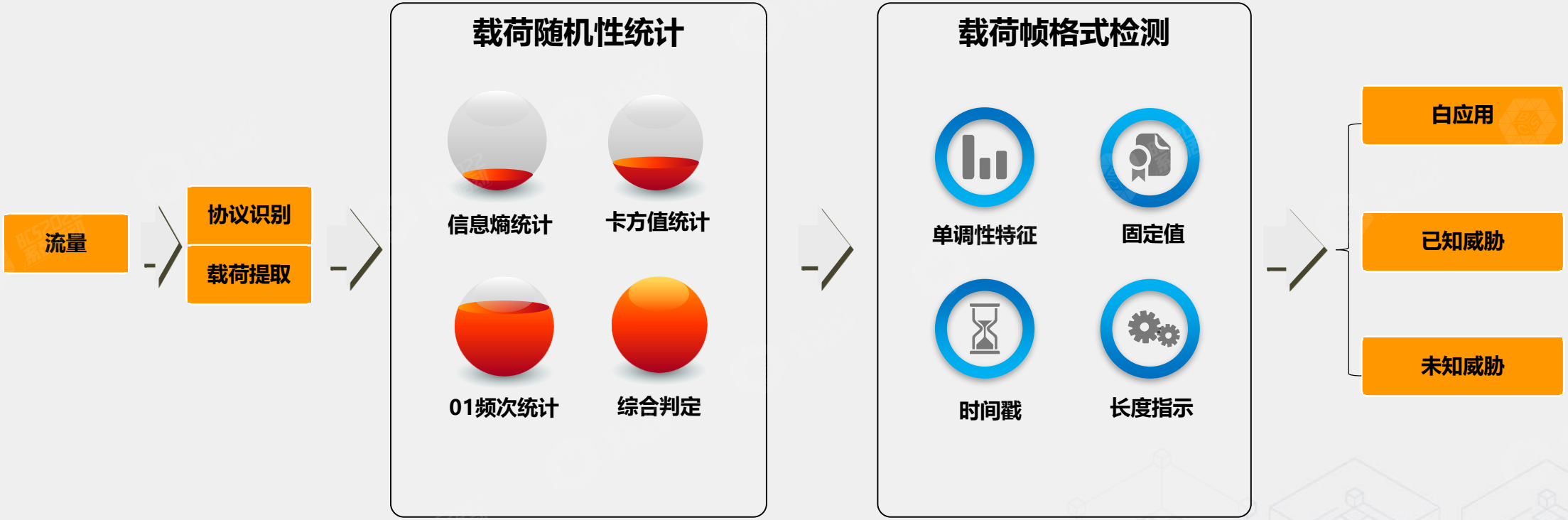
SSL加密威胁检测：原创“鱼骨图”呈现设计



DNS隧道检测技术路线



TCP/UDP隧道加密威胁检测技术路线



案例1： Cobalt Strike SSL 加密流量检测

案例1： Cobalt Strike SSL加密流量异常分析

- 支持最高TLS版本为1.0，版本较低；
- 支持的密码套件数量、顺序能够反映客户端应用程序实现TLS会话的方式；
- 支持扩展项数量较少，正常应用通常超过6项；
- 指纹库匹配：Java库、.NET库、系统库、各个平台常用APP指纹库、常见恶意程序指纹库。

1、握手特征异常分析

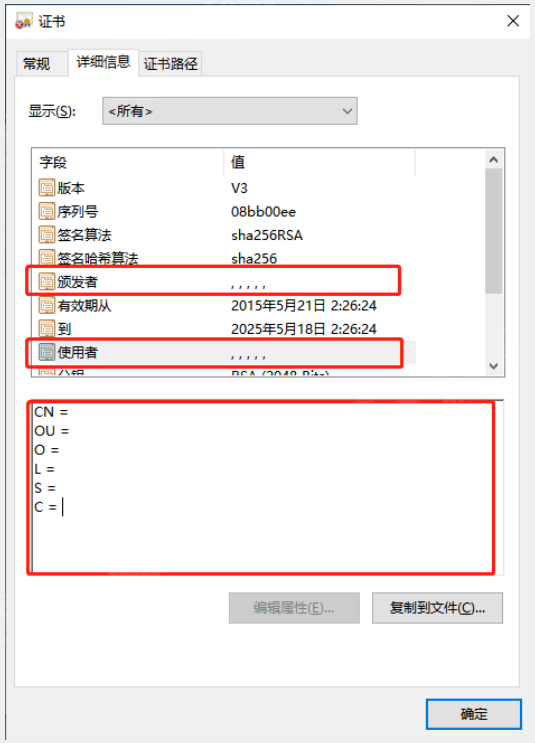
1	09:02:09.197367	192.168.136.128	…	TLSv1	Client Hello
196	09:02:25.673635	192.168.136.128	…	TLSv1	Client Hello
205	09:03:26.333863	192.168.136.128	…	TLSv1	Client Hello
214	09:04:26.892107	192.168.136.128	…	TLSv1	Client Hello
223	09:05:27.514843	192.168.136.128	…	TLSv1	Client Hello
232	09:06:28.042018	192.168.136.128	…	TLSv1	Client Hello

默认配置 心跳间隔60S 抖动比例0%

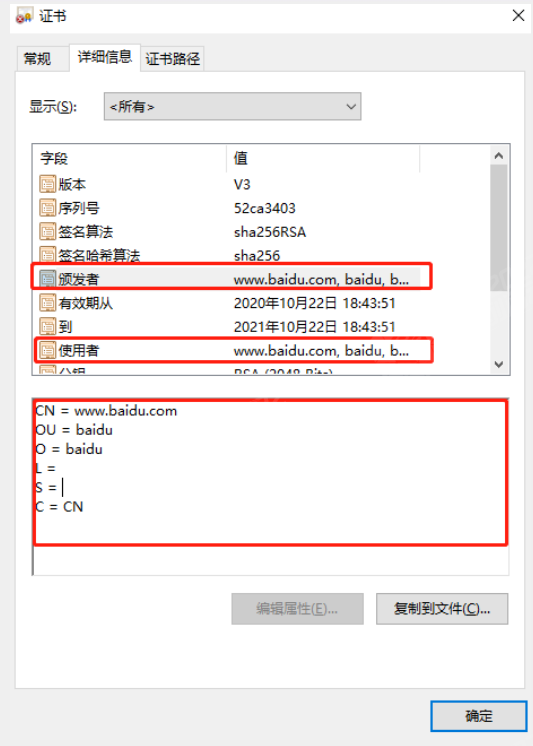
230	18:46:36.807758	192.168.136.128	…	TLSv1	Client Hello
374	18:47:14.340322	192.168.136.128	…	TLSv1	Client Hello
548	18:47:49.784171	192.168.136.128	…	TLSv1	Client Hello
749	18:48:30.661398	192.168.136.128	…	TLSv1	Client Hello
858	18:49:04.790902	192.168.136.128	…	TLSv1	Client Hello
1001	18:49:37.361564	192.168.136.128	…	TLSv1	Client Hello
1188	18:50:18.030602	192.168.136.128	…	TLSv1	Client Hello
1332	18:50:52.397852	192.168.136.128	…	TLSv1	Client Hello
1499	18:51:37.267498	192.168.136.128	…	TLSv1	Client Hello
1689	18:52:13.800784	192.168.136.128	…	TLSv1	Client Hello

修改配置 心跳间隔45S 抖动比例37%

2、行为特征异常分析



默认证书：
每个版本的Cobalt Strike都会有一个默认证书，如果不做修改可以通过证书特征进行检测。



修改证书：
攻击方会修改默认证书特征，且修改内容不可知，无法形成检测规则。

证书异常分析：
1）证书正常度：AI子模型，从200多个维度进行检测；
2）证书可信度：系统内置80+根证书，证书链校验无法通过会记录特征。

3、证书特征异常分析

案例2： Cobalt Strike DNS隧道加密流量检测

DNS隧道

时间： 选择日期 选择日期 查询

概要信息

持续时间： 4分26秒
请求次数： 8629
请求频率： 1918次/分钟

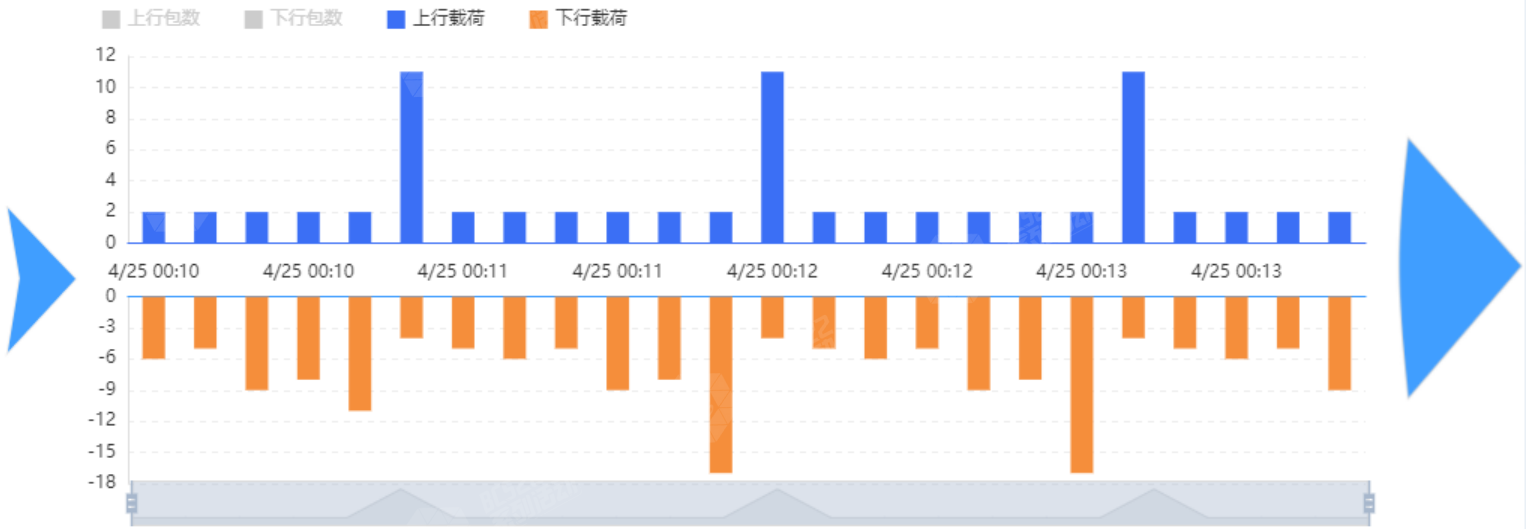
请求频次过高

请求类型分布

类型	数量	占比
A	8629	100%
AAAA	0	0%
CNAME	0	0%
TXT	0	0%
NS	0	0%
NULL	0	0%

综合展示

总分： 0.77



详情

子域名过长、携带数据痕迹明显

post.317551057249a2fac42cdcd31d3387439dc67e2997257255b4dfbe206.6326ec8214e7e4cd6bf13e13ddd40c14bb6766f0ca627b16b1f3b9a1.dc11550144a3612ee053e35832bab0aa7f629fa47371cef83415b7a0.1f52a673f4.88799.ns3.liangyipinecone.xyz

域名信息

主域名： liangyipinecone.xyz
分域名数： 8629

子域名变化频繁

分域名分布

post.317551057249a2...
post.30cd7e4262c89f...
post.1d3387439dc67e...
post.e4262c89f02dd4...
post.3387439dc67e29...
post.4262c89f02dd47...
post.2cdcd31d338743...
post.62c89f02dd470d...
post.3387439dc67e29...
post.4262c89f02dd47...
post.2cdcd31d338743...
post.62c89f02dd470d...

更多

加密威胁检测仍面临很多挑战

大量加密应用中转

TLS 1.3全面普及

顶级APT中的加密流量

道且险阻,行则将至

THANKS

观成科技|加密网络空间安全领航者