2017 中国互联网安全大会
China Internet Security Conference

用户视角下的威胁情报质量评估方法

姜政伟 中国科学院信息工程研究所，高级工程师

李强 中国科学院信息工程研究所，博士研究生

目录

用户视角下的威胁威胁情报质量评估方法

- 研究现状
- 评估方法
- 评估实例
- 项目应用
- 参与方式

质量评估需求

指导供应商规范化威胁情报质量体系

国内外威胁情报供应商众多

- Gartner ”Market Guide for Security Threat Intelligence Services” 列举49家
- Forrester ”Vendor Landscape: External Threat Intelligence” 列举30家

帮助用户评选合适的威胁情报服务

实施难点

- 指标的选取与量化困难
- 威胁情报的业务侧重点各异
- 威胁情报体现的服务形式多样

研究现状

研究机构/人员	主要思路	特点
CMU/ Metcalf	25个公共源上的黑名单，统计独有指示器总数及比例、交叉覆盖度	仅针对黑名单
RUB/Kührer	15个公共源及4个反病毒的黑名单，评估、识别和判断黑名单的有效性	
Niddel/ Pinto	评估 feeds的新鲜度、覆盖度、流行度、过期性、唯一性等	侧重数据层面
Polska/Pawlinsk	从信息分级、情报类型展开，评估相关性、准确性、完整性、实效性和可利用性，从检测方法、优势和容量评估诈源范围	缺乏数量、成本等因素
Dragos/Sergio	相关性、及时性、准确性、完整性	笼统概括
CMU/Troy	搜集及时性、有效性、可实施性的人员反馈来评分	主观性很强
UB/Omar	正确性、相关性、有效性、唯一性	提出相应的 量化方法
Gartner	可利用程度、数据深度、广度、实效性；分析师能力	主要针对厂商的评选
ASU/Ajay	通过知识图谱计算可信性和相关性得到情报优先级排序	形成信任分值计量系统

维度未成体系

人工处理为主

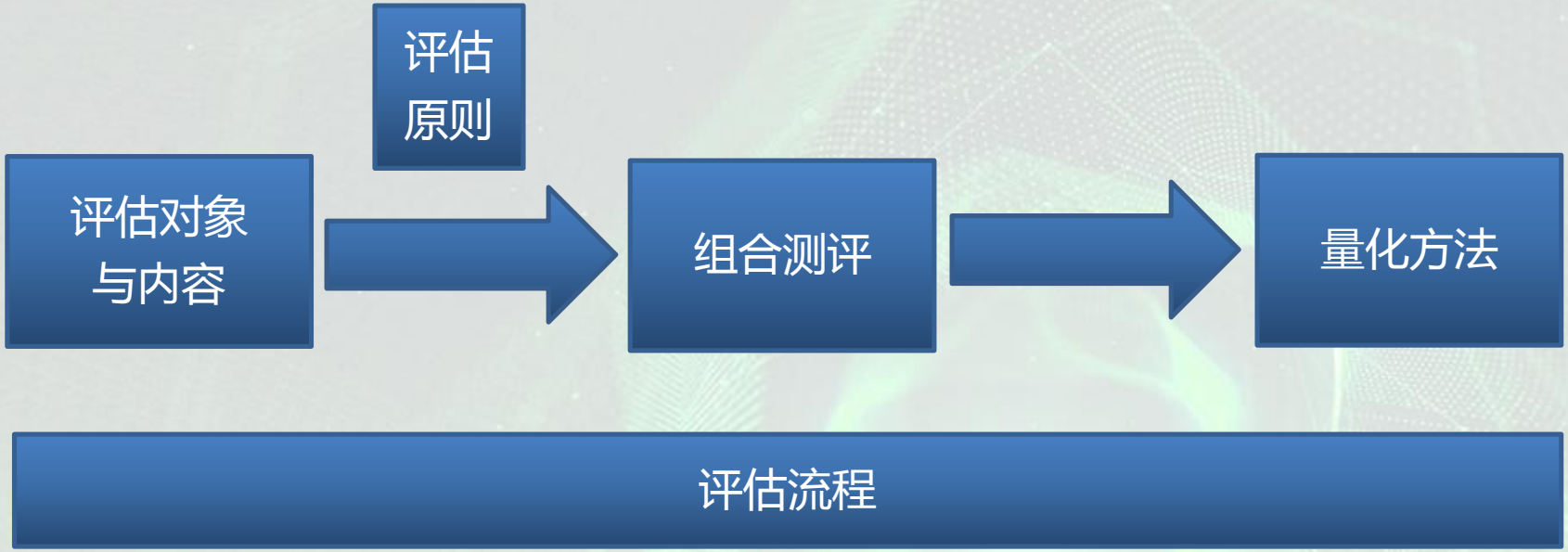
区分度不明显

ISC 2017 中国互联网安全大会

360互联网安全中心

威胁情报质量评估方法

评估方法要素



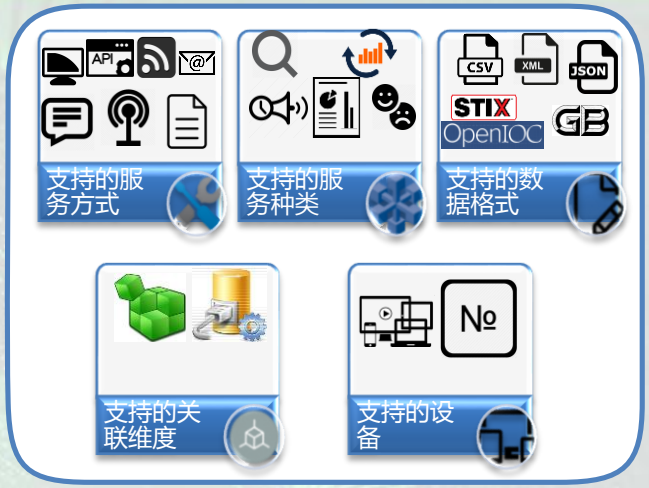
评估原则

科学性与实用性	系统性和层次性	全面性和代表性	动态性和静态性
• 遵循数学原理 • 可实际操作	• 体系化的框架 • 按层次分解	• 相对全面 • 有所选取	• 可剪裁 • 有核心指标

组合测评/设计中考虑的维度

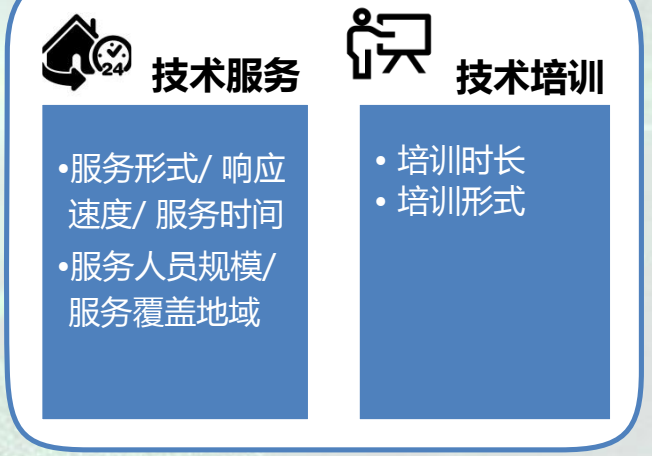
测评项目/内容


数据价格
服务价格
价格
硬件价格
软件价格


API
支持的服务方式
支持的服务种类
CSV
XML
JSON
STIX
OpenIOC
GB
支持的数据格式
支持的关联维度
№
支持的设备


数据
类别
数据量
数据
来源
数据
性质


信誉
资质
PR
ISO
ISCCC
ITSM
IS


技术服务
•服务形式/ 响应速度/ 服务时间
•服务人员规模/ 服务覆盖地域
技术培训
• 培训时长
• 培训形式

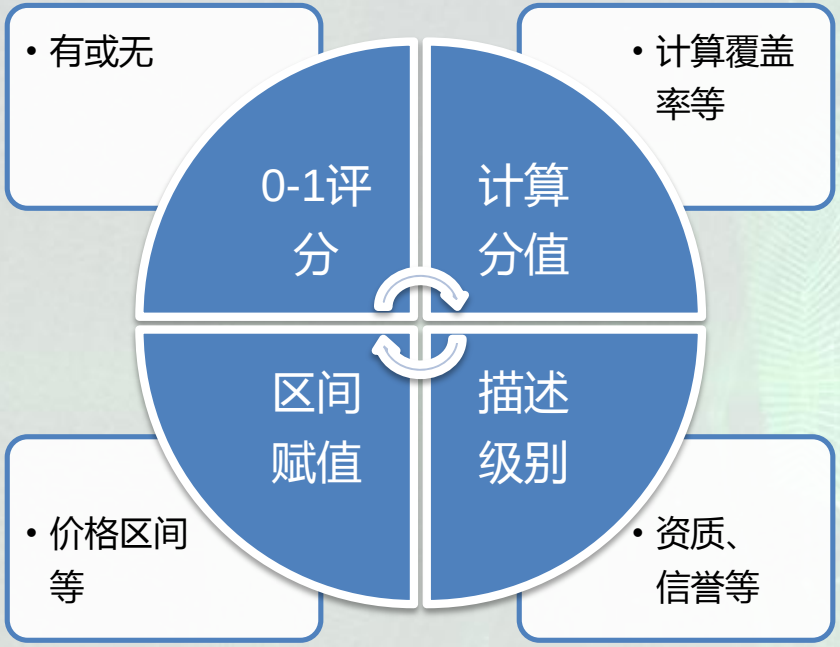
测试属性和方法


相关性
Relevance
及时性
Timeliness
准确性
Accuracy
完整性
Completeness
可执行性
Performability
定制性
Customizability
可预测性
Predictability
...


新鲜度测试
Novelty
流行度测试
Population
独特性测试
Uniqueness
覆盖测试
Overlap
过期测试
Aging
关联测试
Association

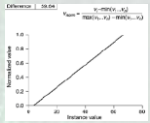
量化方法：归一化

源数据提取 → 数据映射转换 → 一致化 → 规范化

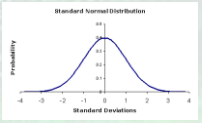


归一化

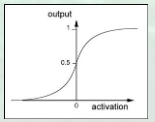
- MIN-MAX标准化 $x^* = \frac{x - \min}{\max - \min}$



- Z-SCORE标准化 $x^* = \frac{x - \mu}{\sigma}$



- SIGMOID函数 $S(x) = \frac{1}{1 + e^{-x}}$



量化方法：权重及得分计算

- AHP层次分析法预处理
- 德尔菲法多方收集建议
- 序关系分析法调整

专家群决策赋权

合成权重

- 规范化决策矩阵$R = (r_{ij})_{n\times m}$
- 离差最大化
- 权重集结，排序择优

- 打分与权重乘积累加
- 单项：$N_k = \sum v_i * I_i$
- 综合：$Score = \sum w_k * N_k$

计算总分

实例测试

Feeds数据测试

测试内容

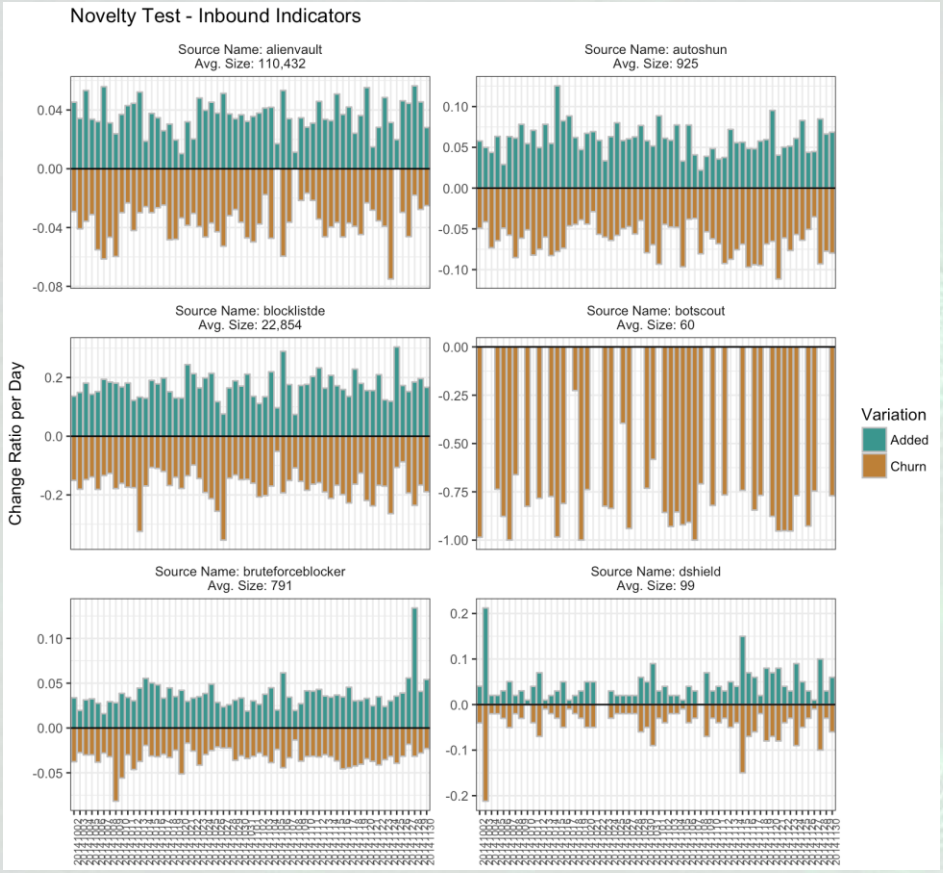
- Data Feeds的若干属性，包括新鲜度、覆盖度、流行度等

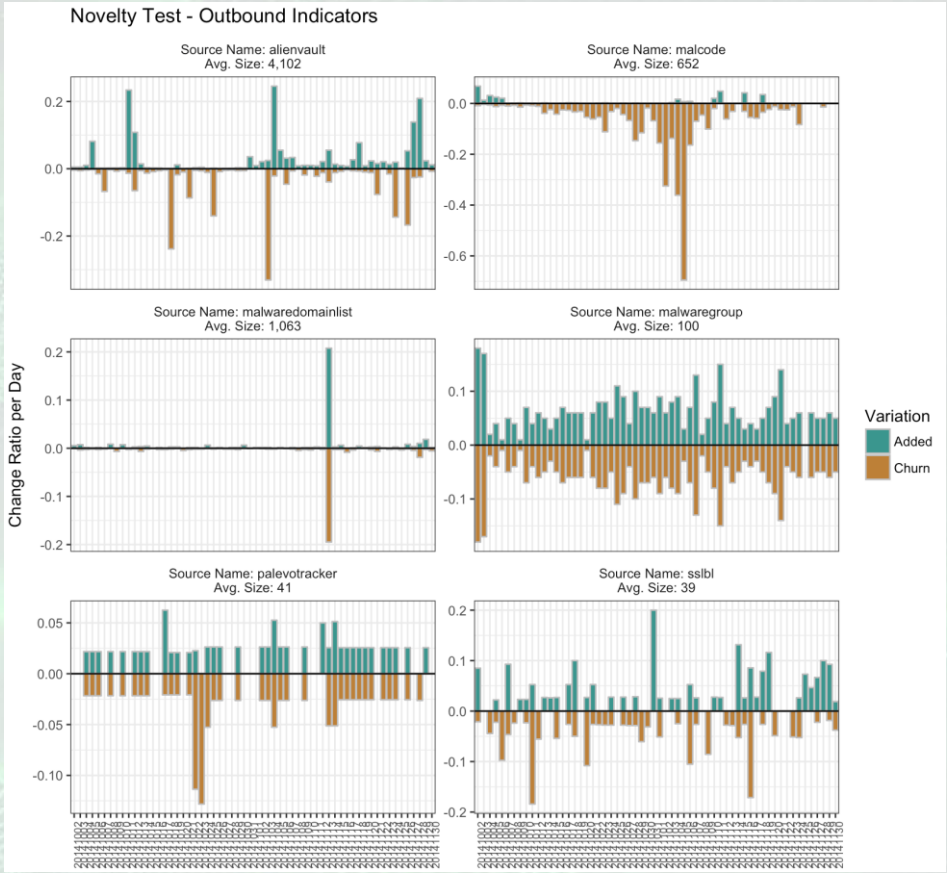
测试数据

- tiq-test测试数据集
- 20多个情报源收集的情报数据，包括alienvault、feodo、malcode、blocklistde等

Feeds数据新鲜度测试

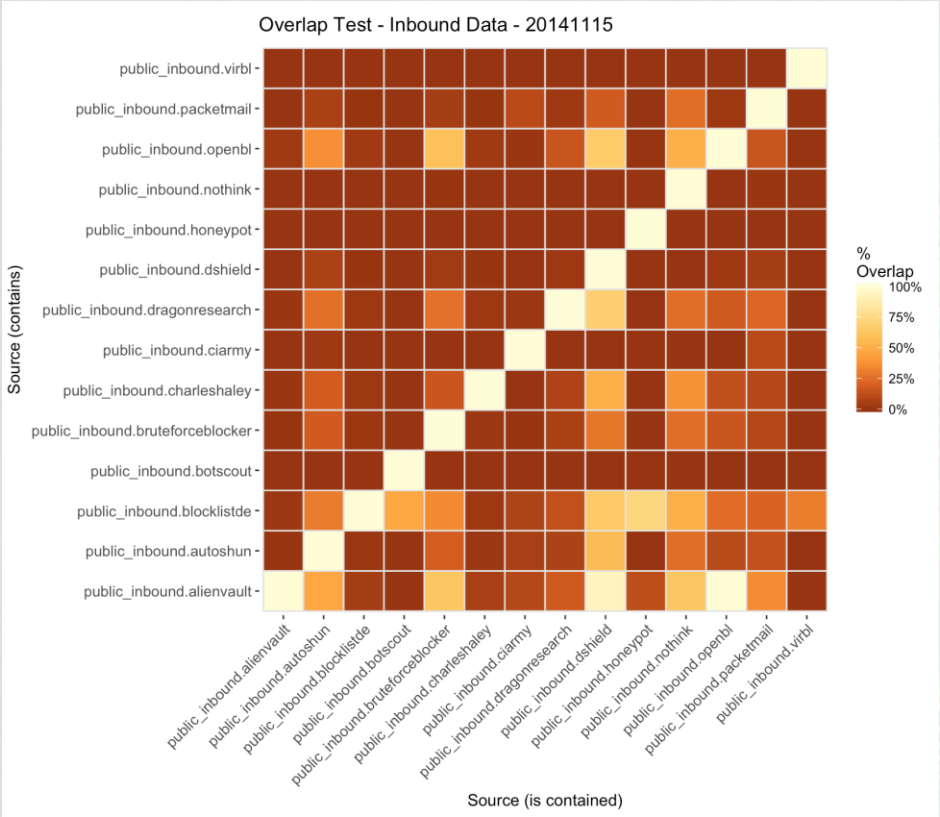
新鲜度（NOVELTY）：FEEDS的更新频率

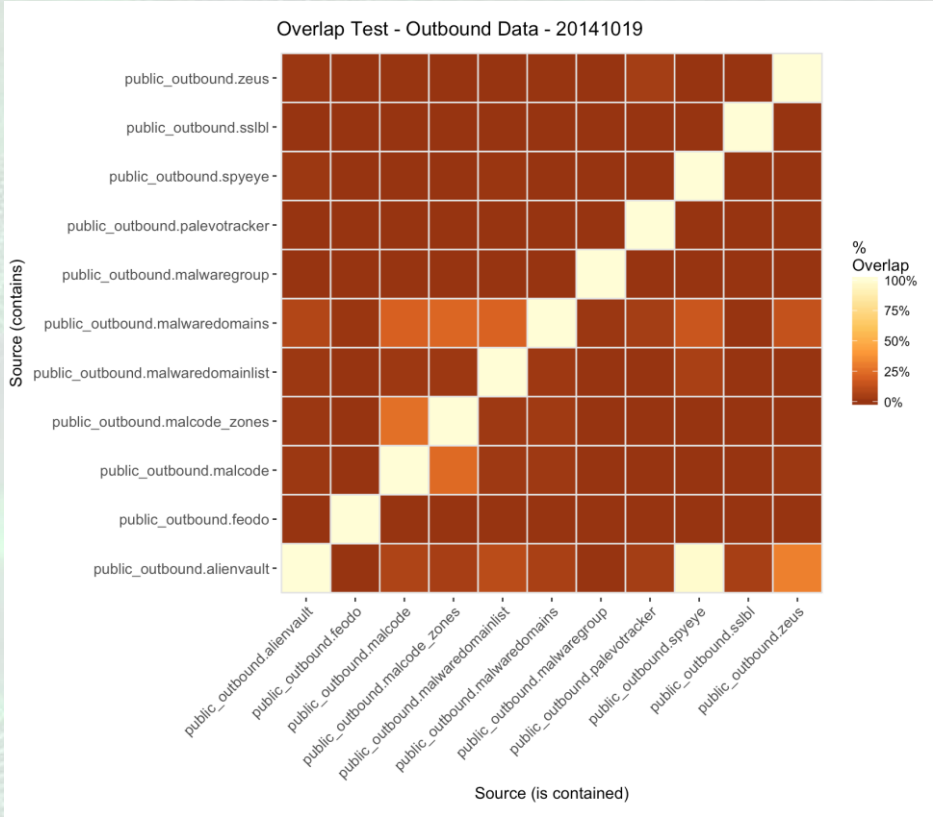




Feeds数据覆盖度测试

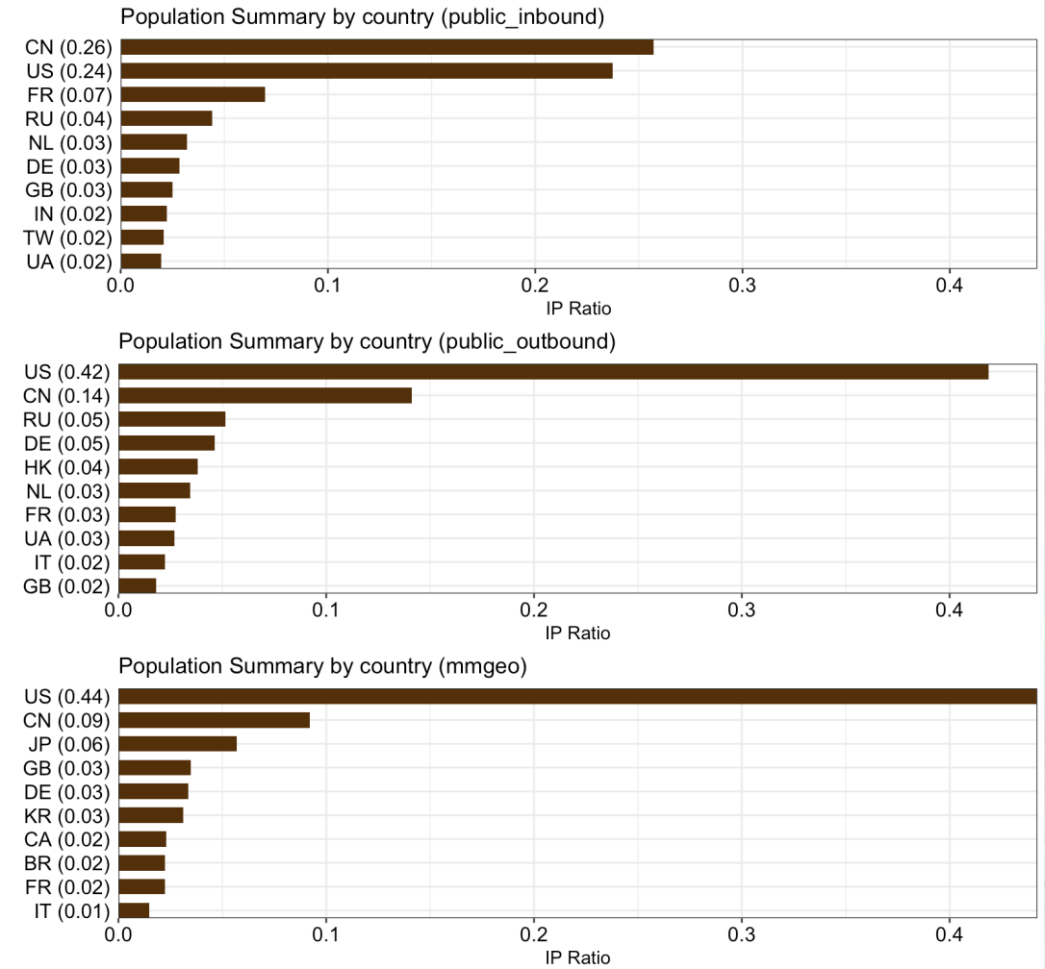
覆盖度（OVERLAP）：情报源相互之间情况对比





Feeds数据流行度测试

流行度（POPULATION）：数据具体内容情况，如区域



关联搜索测试

测试内容

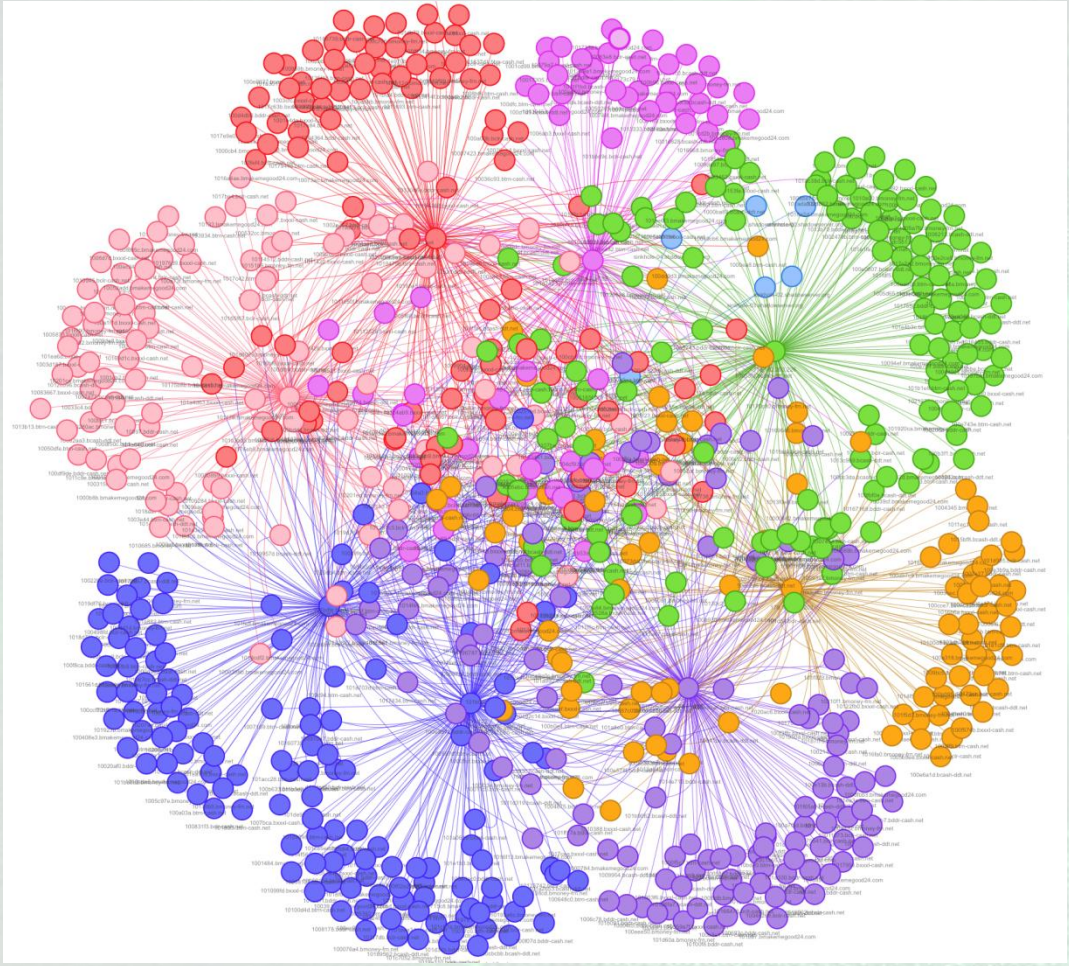
- 关联搜索是网络攻击溯源中常用的方法
- 模拟分析人员关联搜索操作，测试基础支撑数据的情况，包括覆盖度、命中率等

测试数据

- 从开源、自产、共享情报中构建测试数据集
- 调用威胁情报供应商的情报API
- 测试国内外多家知名威胁情报供应商
- 基础支撑数据服务包括PassiveDNS、Whois等

关联搜索测试

按类别标记



综合测试

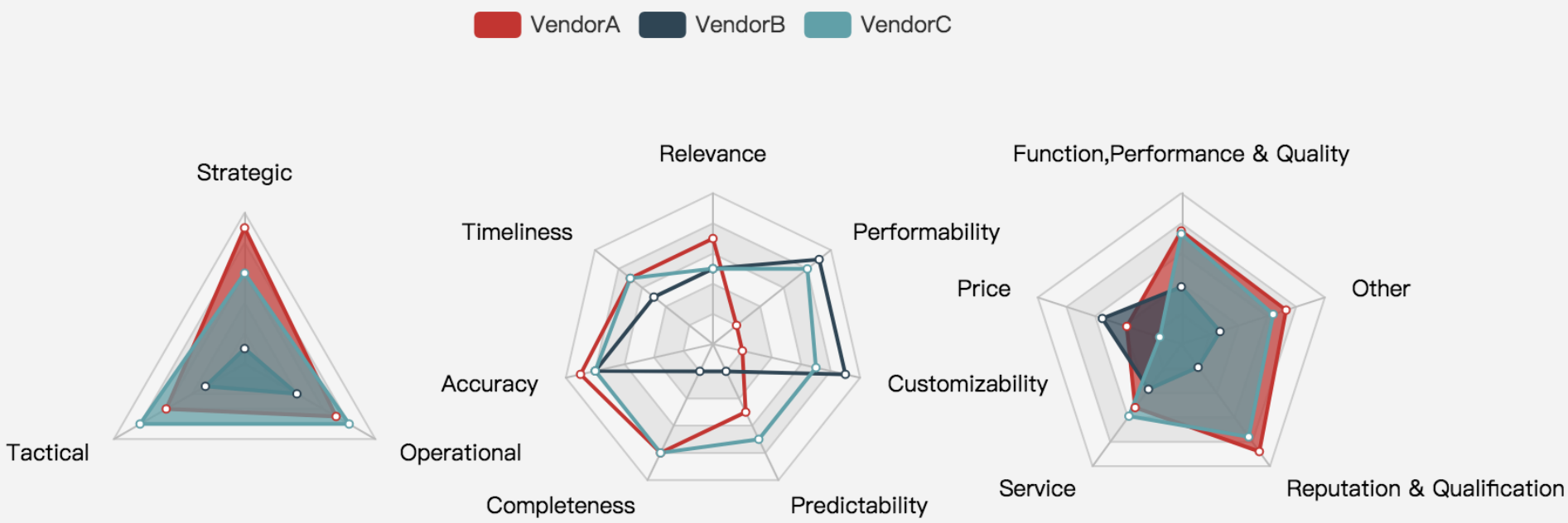
测试内容

- 综合评估供应商的威胁情报服务质量
- 基于组合评估维度和多级指标量化评估体系

测试数据

- 数据分析测试 + 人工搜集
- 测试国内外三家知名威胁情报供应商

综合测试

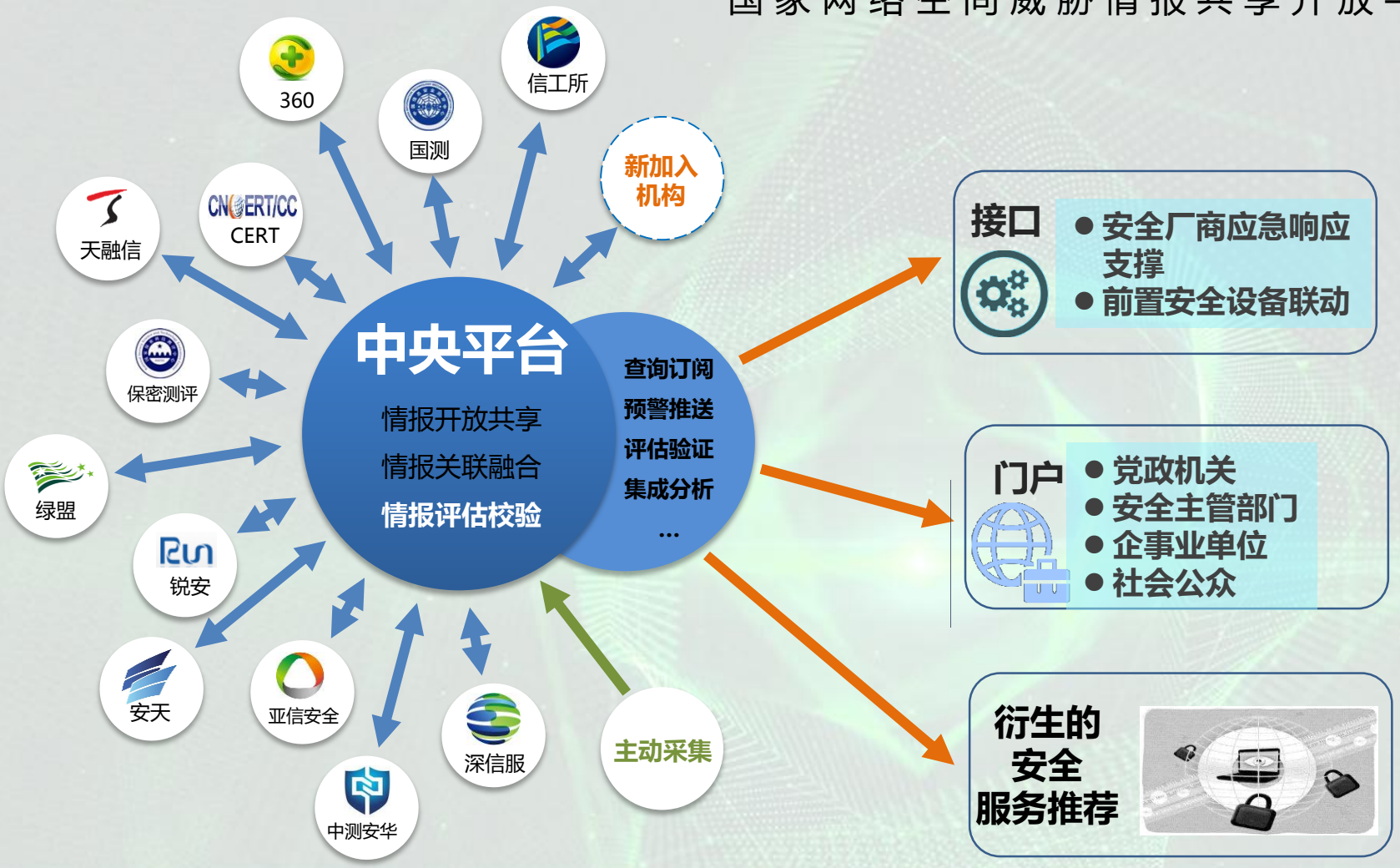

VendorA
VendorB
VendorC
Strategic
Tactical
Relevance
Timeliness
Performability
Accuracy
Operational
Completeness
Predictability
Function,Performance & Quality
Price
Other
Customizability
Service
Reputation & Qualification

项目应用

项目应用

China National Cyberspace Threat Intelligence Collaboration(**CNTIC**)

国家网络空间威胁情报共享开放平台



如何参与

参与测评

- 提供接口API或其它形式服务
- 提供相应说明文档

参与深化设计

- 共同讨论、修订、完善威胁情报质量评估体系

谢　谢