# 国家网络空间威胁情报大数据共享开放平台建设的思考

刘宝旭　研究员

中国科学院信息工程研究所

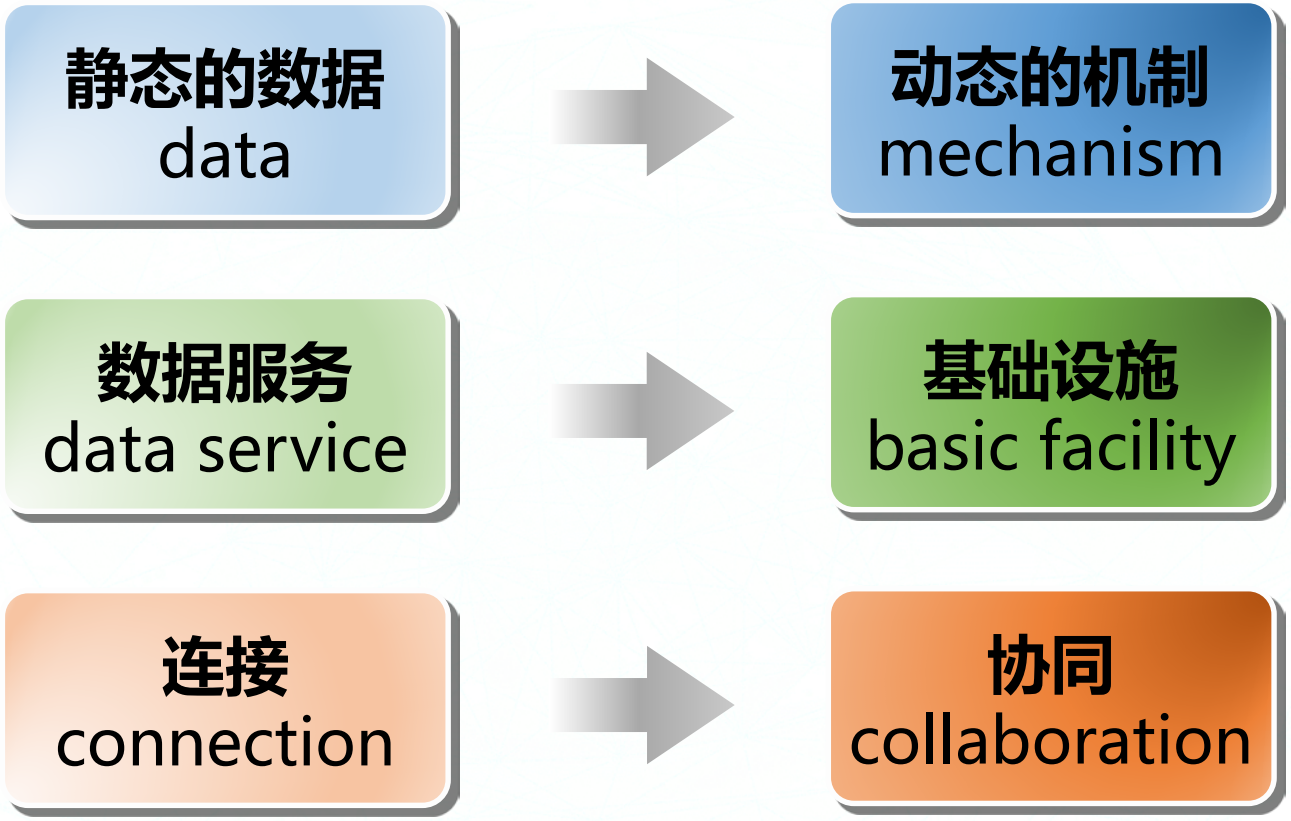
# 大纲

**建设背景**

主要设计与实现

现状

# 对网络威胁情报的再认识




- 威胁情报已成为国家网络空间安全对抗的重要战略资源，是APT监测发现、攻击溯源与主动防御能力的重要基础。

# 美国网络威胁情报生态状况

**出台网络安全信息共享的政策法规**

- 网络安全信息共享法案CISA
- 网络威胁信息共享指南NIST 800-150
- 国家网络战略强调网络威胁信息共享
- …

**成立专门的网络威胁情报共享机构**

- 网络威胁情报整合中心CTIIC
- 国家网络安全与通信整合中心NCCIC
- 行业信息共享和分析中心ISAC
- 非行业信息共享和分析组织ISAO
- …

**开展网络信息共享计划**

- 网络信息共享与协同计划CISCP
- 网络安全增强服务ECS等
- 网络天气地图Cyber Weather Map
- …

**编制行业规范并推向国际标准**

- STIX结构化威胁信息表达规范
- CybOX网络可观测指标表达规范
- TAXII指标信息可信交互规范
- OpenC2开放式控制与命令规范
- …

**出现提供多样威胁情报服务的厂商**

- IBM X-Force
- 网络威胁联盟CTA (Fortinet、Intel Security、Palo Alto Networks、Symantec、Check Point、CISCO)
- Alien Vault
- Crowd Strike
- Fire Eye
- Threat Connect
- Recorded Future
- …

# 国内网络威胁情报协同共享需求与现状

419讲话

**“建立政府和企业网络安全信息共享机制，把企业掌握的大量网络安全信息用起来，龙头企业要带头参加这个机制…综合运用各方面掌握的数据资源”**

**《“十三五”国家信息化规划》**计划在网络安全监测预警和应急处置工程中建立政府、行业、企业网络安全信息共享机制，建设国家网络安全信息共享平台和网络安全威胁知识库

**《网络安全法》**提出网络运营者之间进行合作，促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享

# 国内网络威胁情报协同共享需求与现状

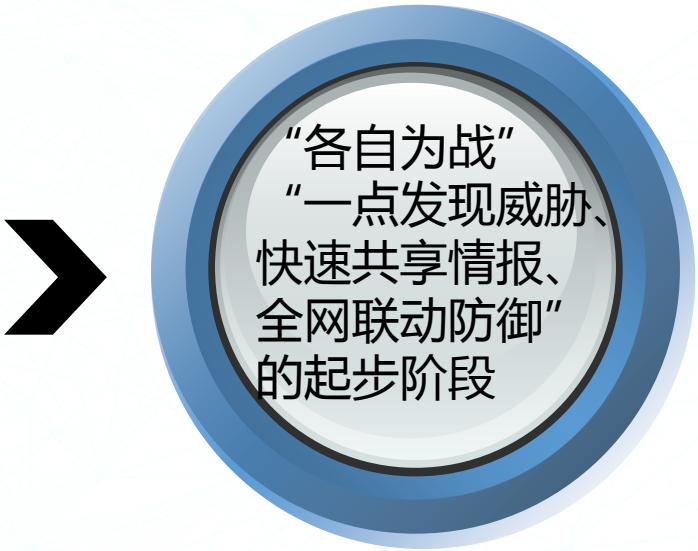
综合性安全公司专门推出威胁情报业务能力，威胁情报创业公司涌现

多种性质的网络威胁情报共享联盟组建

相关国家标准规范获批发布，行业标准规范也在编制中

大型的甲方单位开始使用威胁情报，相关部委十三五工程中引入威胁情报

国家级网络威胁情报体系建设刚启动，数据分散在不同单位或部门，尚存在共享和协同的壁垒



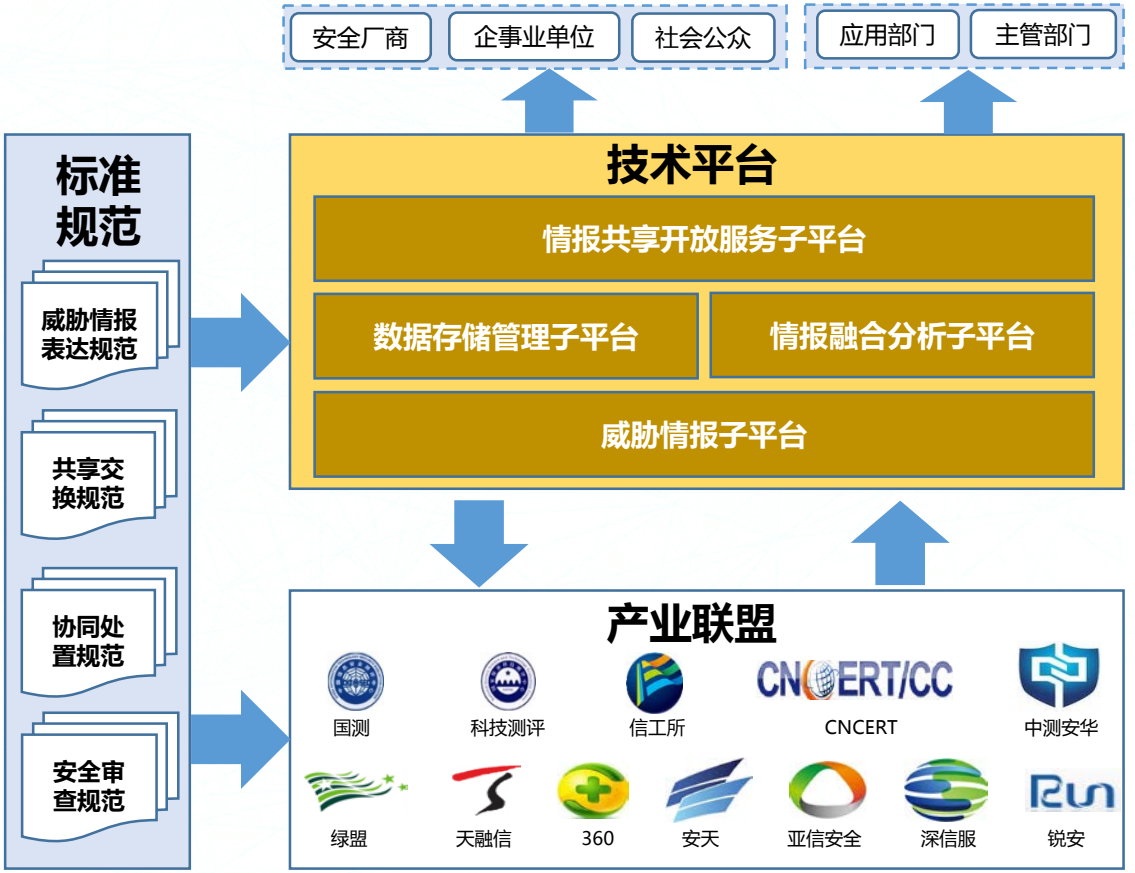
# 发改委批复CNTIC立项

国家发改委2017年批复的促进大数据发展重大工程中**网络空间安全**领域**唯一**的项目——**CNTIC**

- 信工所牵头，联合11家单位共建
- 建设内容为技术平台+标准规范+产业联盟
- 基础安全数据总量近**20万亿**条
- 完全建成后可访问记录达**千亿**条
- 覆盖“海网云”（云管端）的威胁数据
- 面向主管部门、应用部门、安全厂商、企事业单位和社会公众共享开放

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

国家网络空间威胁情报大数据共享开放平台



# 发改委批复CNTIC立项

国家发改委2017年批复的促进大数据发展重大工程中网络间安全领域唯一的项目——CNTIC

## 2017年促进大数据发展重大工程项目计划表

单位：万元

| 序号 | 项目名称 | 项目汇总申报单位 | 项目单位（牵头单位） | 建设内容 | 国家补助资金 |
|---|---|---|---|---|---|
| 1 | 国家网络空间威胁情报大数据共享开放平台重大工程项目 | 国家保密局 | 中国科学院信息工程研究所 | 在充分利用已有设施资源的基础上，购置完善相关的设备设施等，联合相关单位建立数据采集汇集和共享开发利用机制，构建国家网络空间威胁情报大数据共享开放平台，整合汇聚网络安全主管部门、安全厂商、网络安全科研机构、安全保密测评机构等数据资源，制定威胁情报开放共享评估、安全审查制度，突破威胁情报数据的采集汇聚、存储管理、融合分析、共享服务等关键技术，形成集创新、数据、技术、服务、标准于一体的威胁情报生态环境，为支撑安全升级评估、网络攻击追踪溯源、内容检查、安全事件应急处置、社会舆情治理等提供大数据服务，助力提升国家网络安全整体防护能力。 | 1000 |

构建国家网络空间威胁情报大数据共享开放平台...形成集创新、数据、技术、服务、标准于一体的**威胁情报生态环境**，为支撑安全升级评估、网络攻击追踪溯源、内容检查、安全事件应急处置、社会舆情治理等提供大数据服务，助力提升国家网络安全整体防护能力

# 大纲

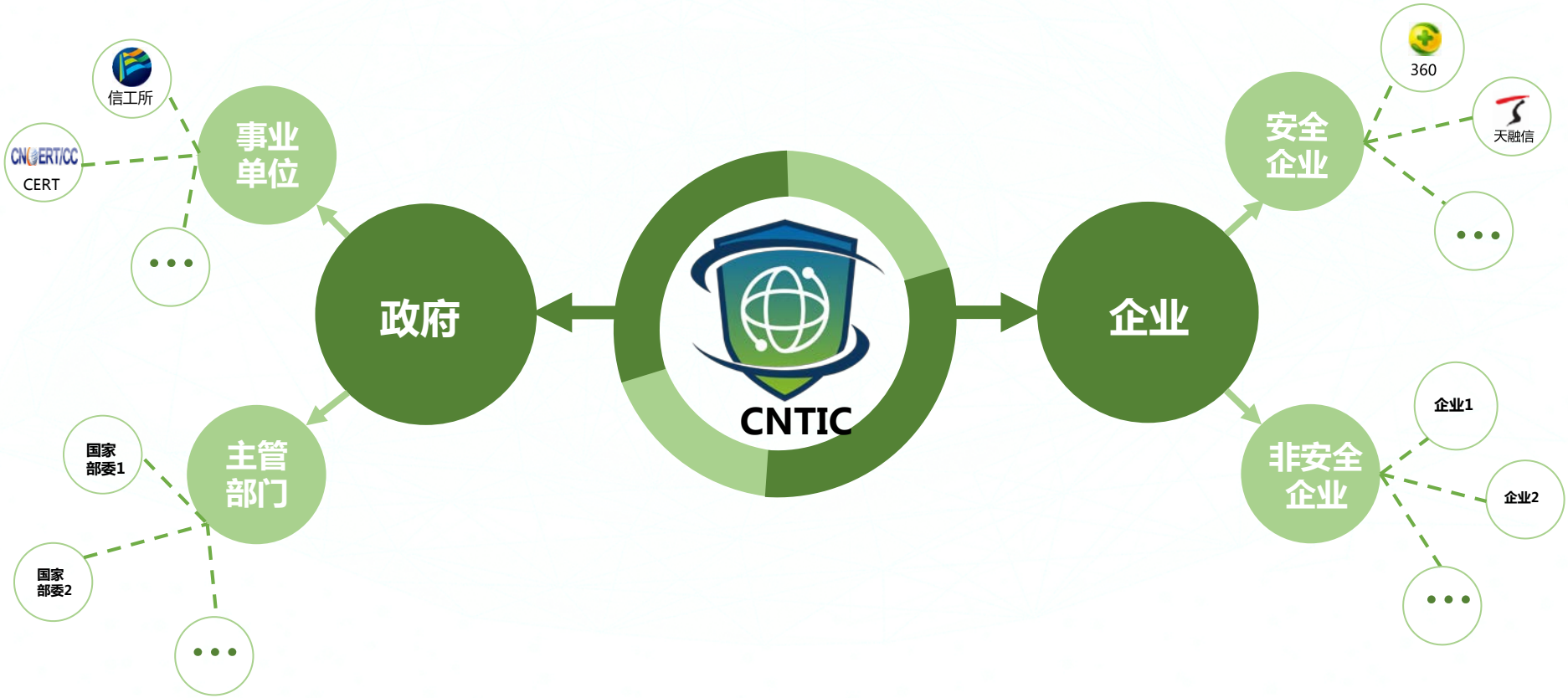
建设背景

**主要设计与实现**

现状

# 平台定位

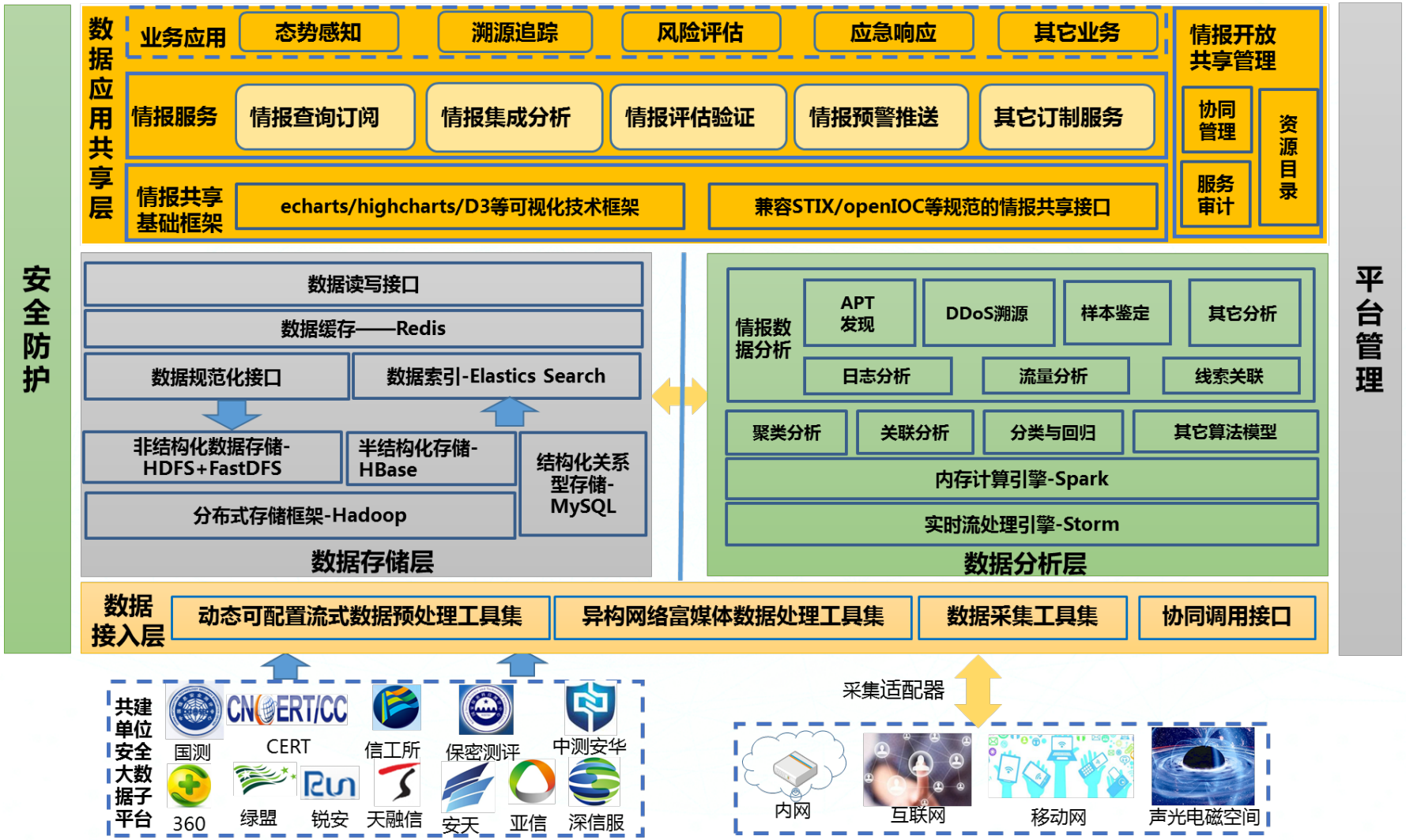
- 第一个政企合作的国家级网络空间威胁情报共享开放平台
- 网络安全信息共享机制中连接多方的“桥梁”与“纽带”



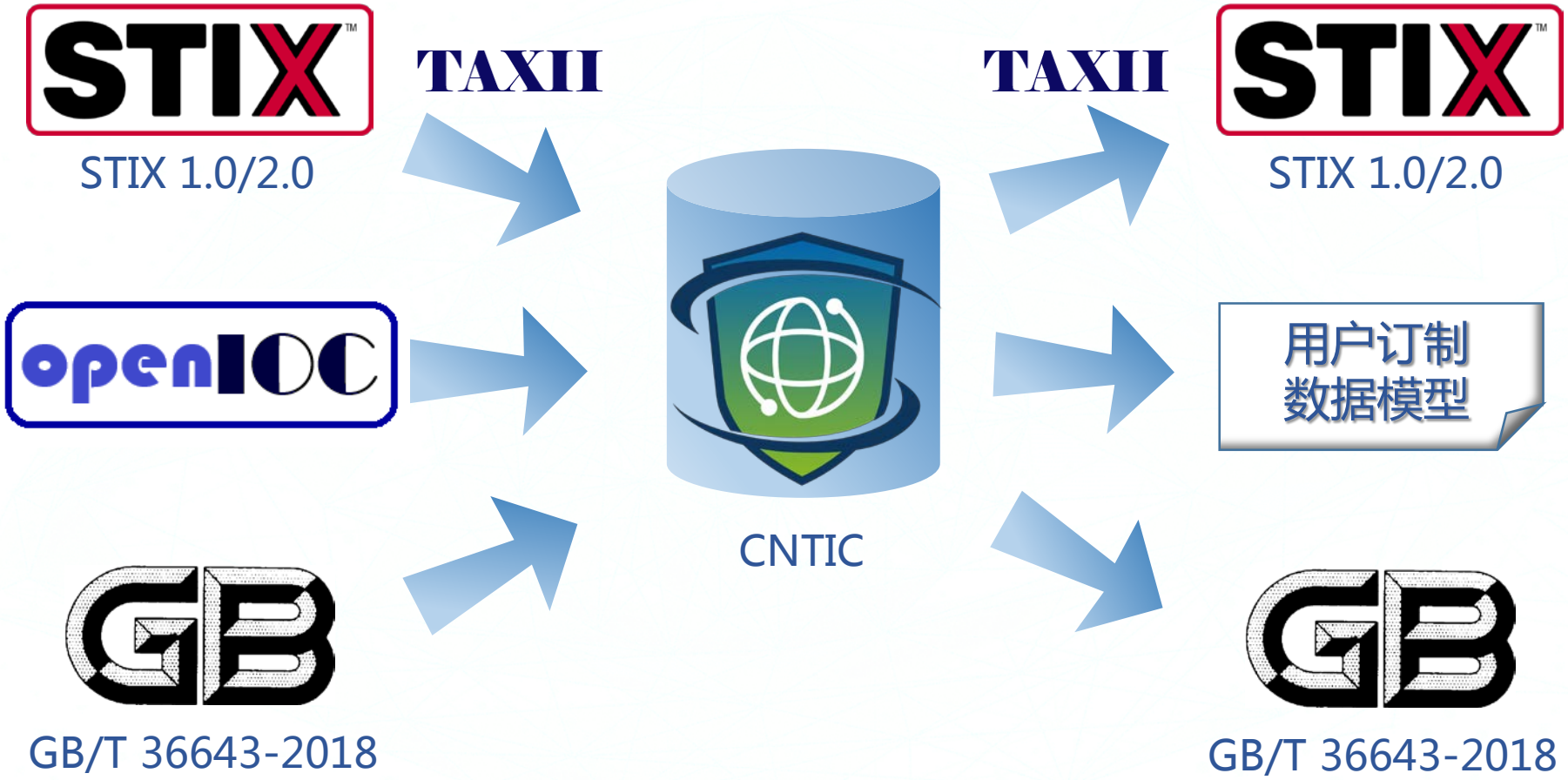
# 平台定位

面向多网络空间，以支撑全链条的网络威胁痕迹拼接和跨网跨域的威胁协同响应

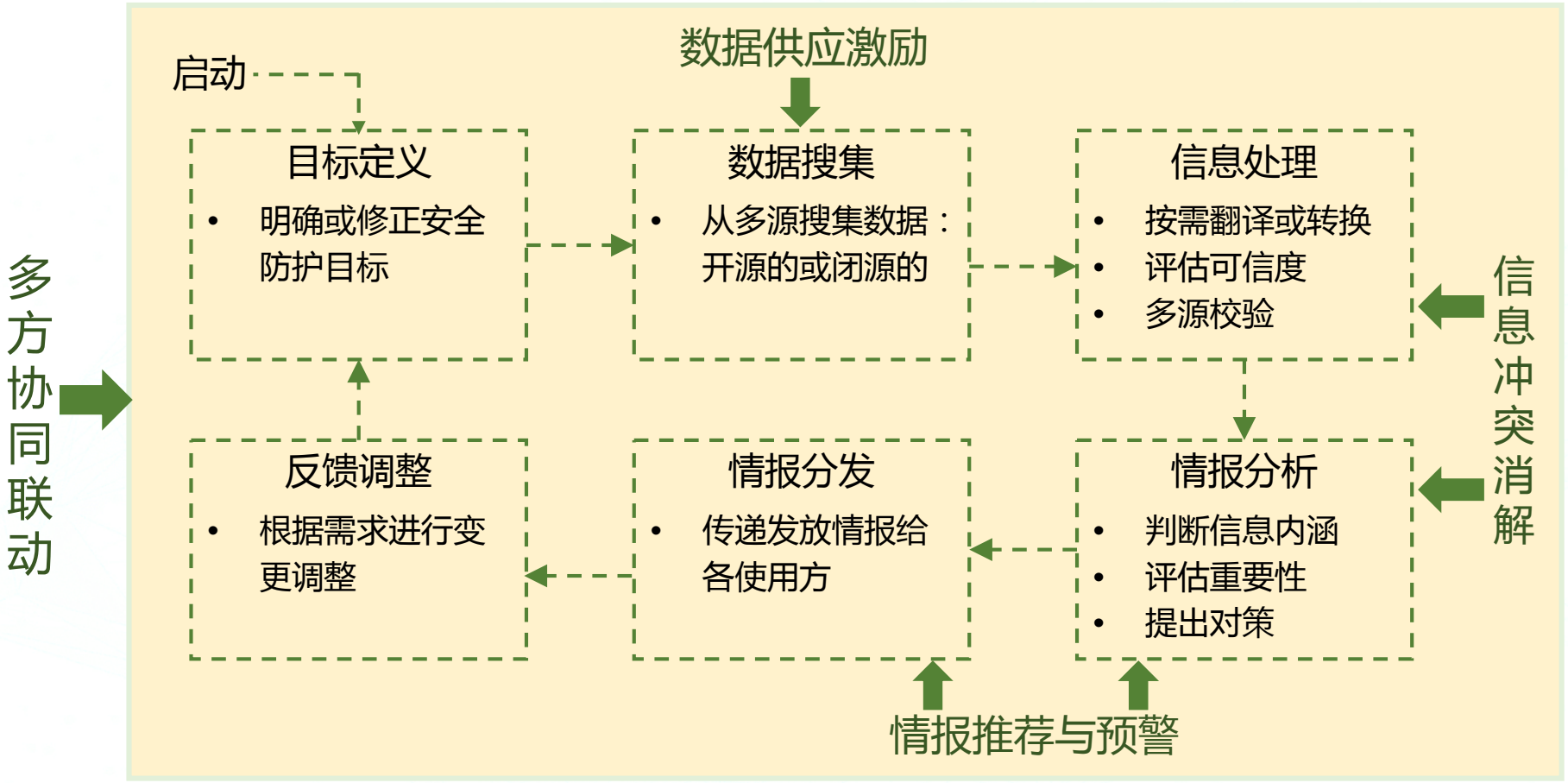
# 平台主体技术架构


安全防护
数据应用共享层
业务应用
态势感知
溯源追踪
风险评估
应急响应
其它业务
情报服务
情报查询订阅
情报集成分析
情报评估验证
情报预警推送
其它订制服务
情报共享基础框架
echarts/highcharts/D3等可视化技术框架
兼容STIX/openIOC等规范的情报共享接口
情报开放共享管理
协同管理
资源目录
服务审计
平台管理
数据读写接口
数据缓存——Redis
数据规范化接口
数据索引-Elastics Search
非结构化数据存储-HDFS+FastDFS
半结构化存储-HBase
结构化关系型存储-MySQL
分布式存储框架-Hadoop
数据存储层
情报数据分析
APT发现
DDoS溯源
样本鉴定
其它分析
日志分析
流量分析
线索关联
聚类分析
关联分析
分类与回归
其它算法模型
内存计算引擎-Spark
实时流处理引擎-Storm
数据分析层
数据接入层
动态可配置流式数据预处理工具集
异构网络富媒体数据处理工具集
数据采集工具集
协同调用接口
共建单位安全大数据子平台
国测
CERT
信工所
保密测评
中测安华
360
绿盟
锐安
天融信
安天
亚信
深信服
采集适配器
内网
互联网
移动网
声光电磁空间

# 核心数据模型设计


STIX
TAXII
TAXII
STIX
STIX 1.0/2.0
STIX 1.0/2.0
openIOC
用户订制
数据模型
CNTIC
GB
GB
GB/T 36643-2018
GB/T 36643-2018

# 威胁情报生命周期与核心难题



# 数据供应激励

## 情报供应不积极

威胁情报是厂商的“**命脉**”
-重要资产

共享数据得不到相应**收益**
-效益损失

数据使用得不到有效**控制**
-利益损失

## 情报质量不达标

情报供应存在“**供求关系**”
-生态需求

共享数据不符合用户“**胃口**”
-繁杂无效

共享数据质量“**参差不齐**”
-劣质无用

# 数据供应激励

**短期激励机制**

**基于数据价值的收益分配机制**

**长效激励机制**

**情报联盟会员制度**

# 信息冲突消解


厂商情报不完整
信息缺失
信息过期
数据生成不及时
信息模糊
厂商对情报缺乏明确分类或标注
数据规范不统一
厂商对情报的表达不一致
信息源低质
情报供应链上游数据可靠度不高
信息时效性
分析时间不同
信息主观性
非厂商能力侧重点
信息冲突

# 信息冲突消解

平台汇聚融合后，进行去重、验证，返回相对可靠的情报


# 情报聚合挖掘

## 精益求精

单一来源情报各有优势，但内容不够丰富

通过多源异构情报聚合，提高情报知识密度

**提升情报质量**

## 穿针引线

多源情报相互独立，碎片化严重，无法进行有效利用

通过挖掘，找出隐蔽或潜在关联，将情报碎片编织在一起

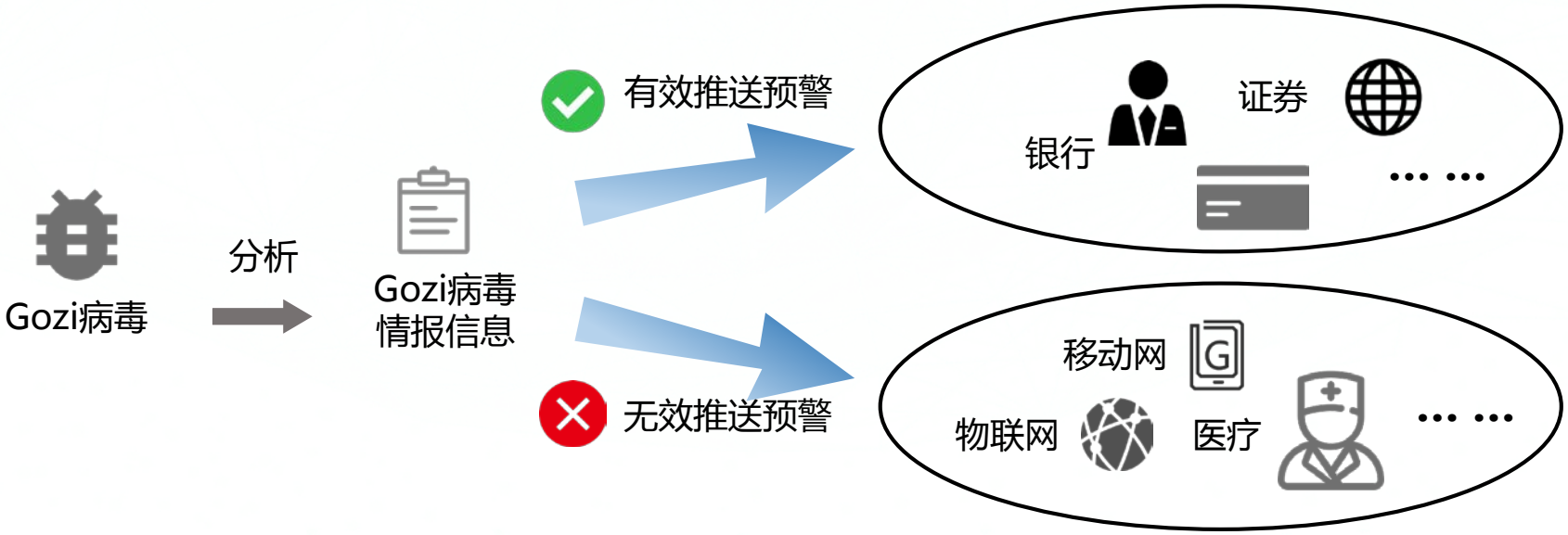
**提升情报应用价值**

# 情报推荐与预警

## 情报价值受用户属性影响

**Gozi病毒**

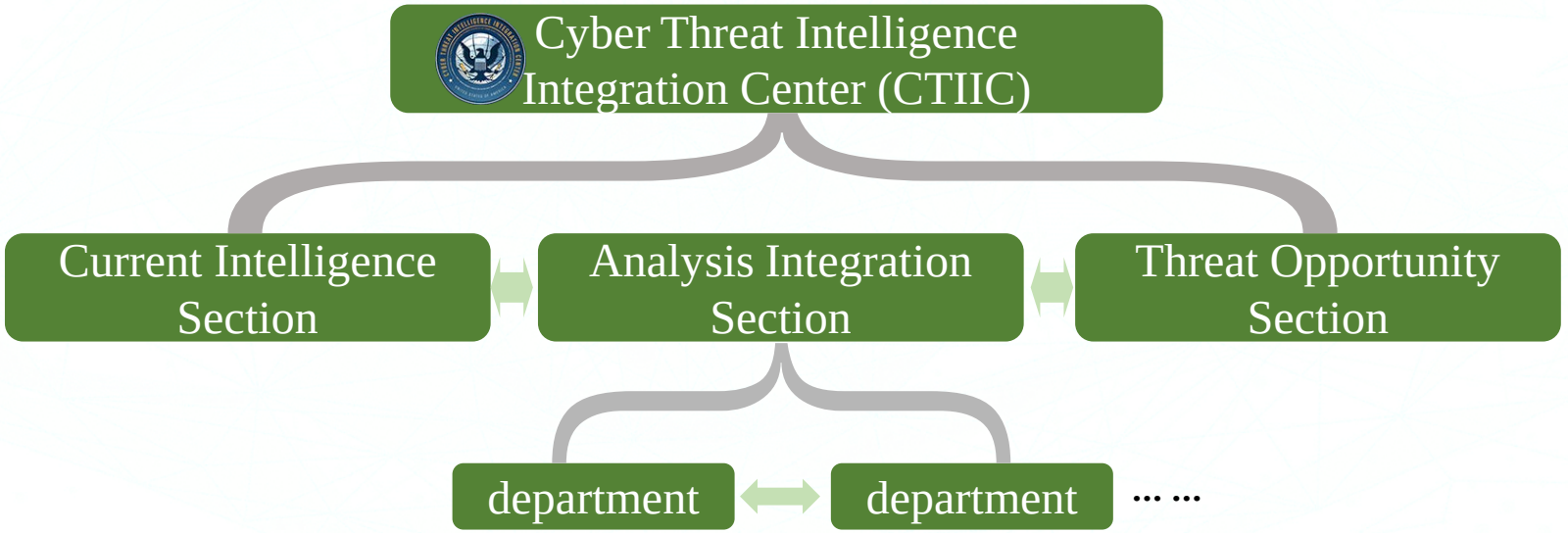
Gozi称为**金融界**历史上破坏性最强的病毒之一，其感染了全球超过100万台电脑，仅美国就有4万余台电脑被感染，这些黑客组织制造并传播病毒，攻击**特定金融机构**，从个人银行账户中窃取了上千万美元。联邦法官将案件定性为受商业利益驱动的跨国网络犯罪。



# 多方协同联动

**Wannacry**

2017年5月12日，Wannacry勒索病毒在全球互联网上迅速蔓延，先后袭击了全球超过150个国家的近30万台电脑设备。但在这次危机中，美国联邦政府网络受到的影响几乎为零，根据特朗普的国土安全及反恐顾问称，美国网络威胁情报中心(CTIIC）经过多方协调，在让白宫掌握事态发展和应对方面发挥了重大作用。



# 大纲

建设背景

主要设计与实现

**现状**

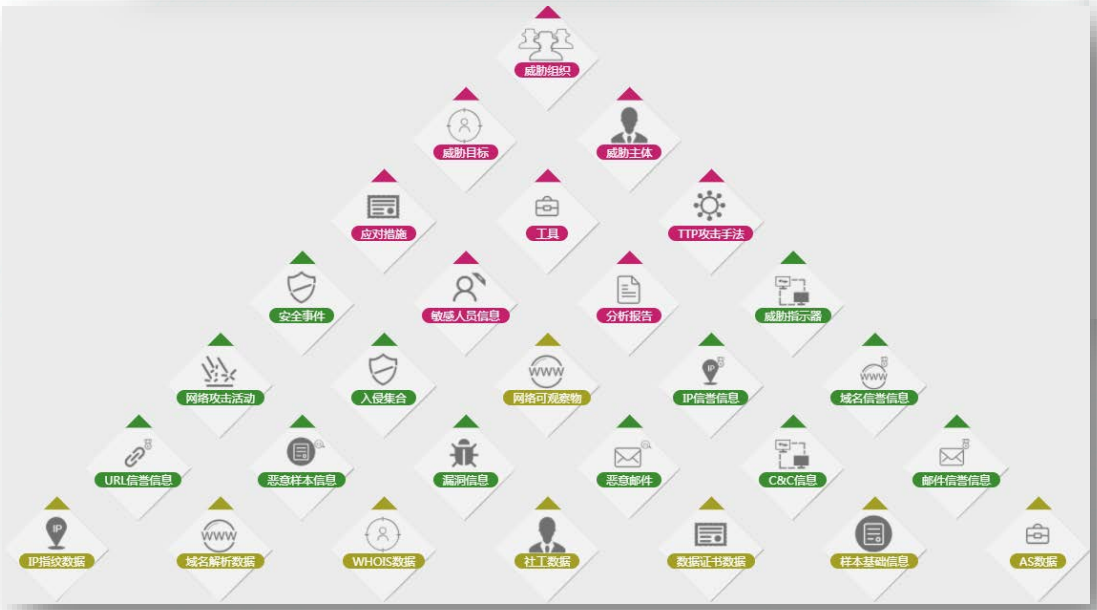
# 平台数据现状

平台可访问数据量

86,646,164,733

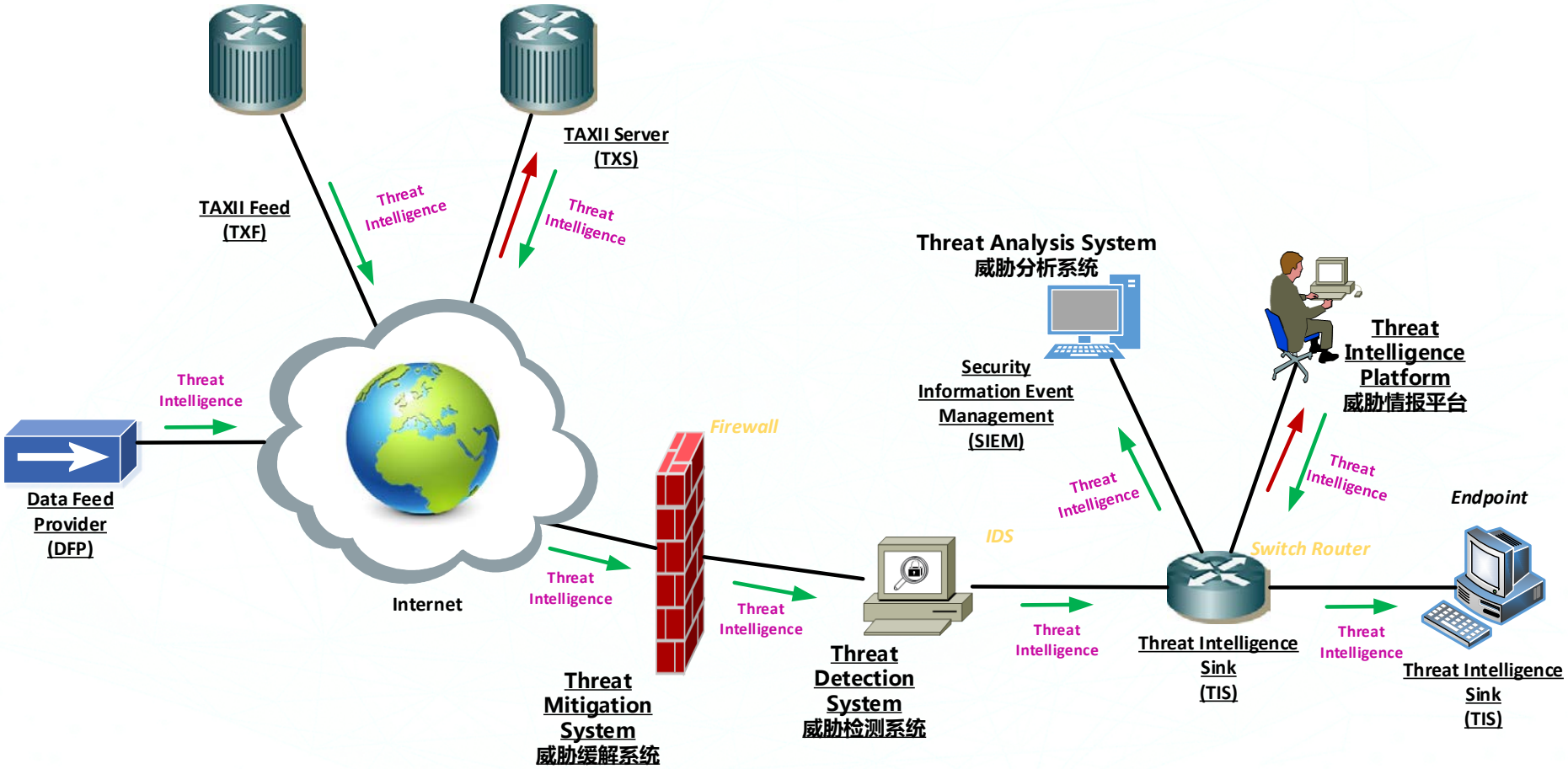
平台本地数据量

8,540,118,610



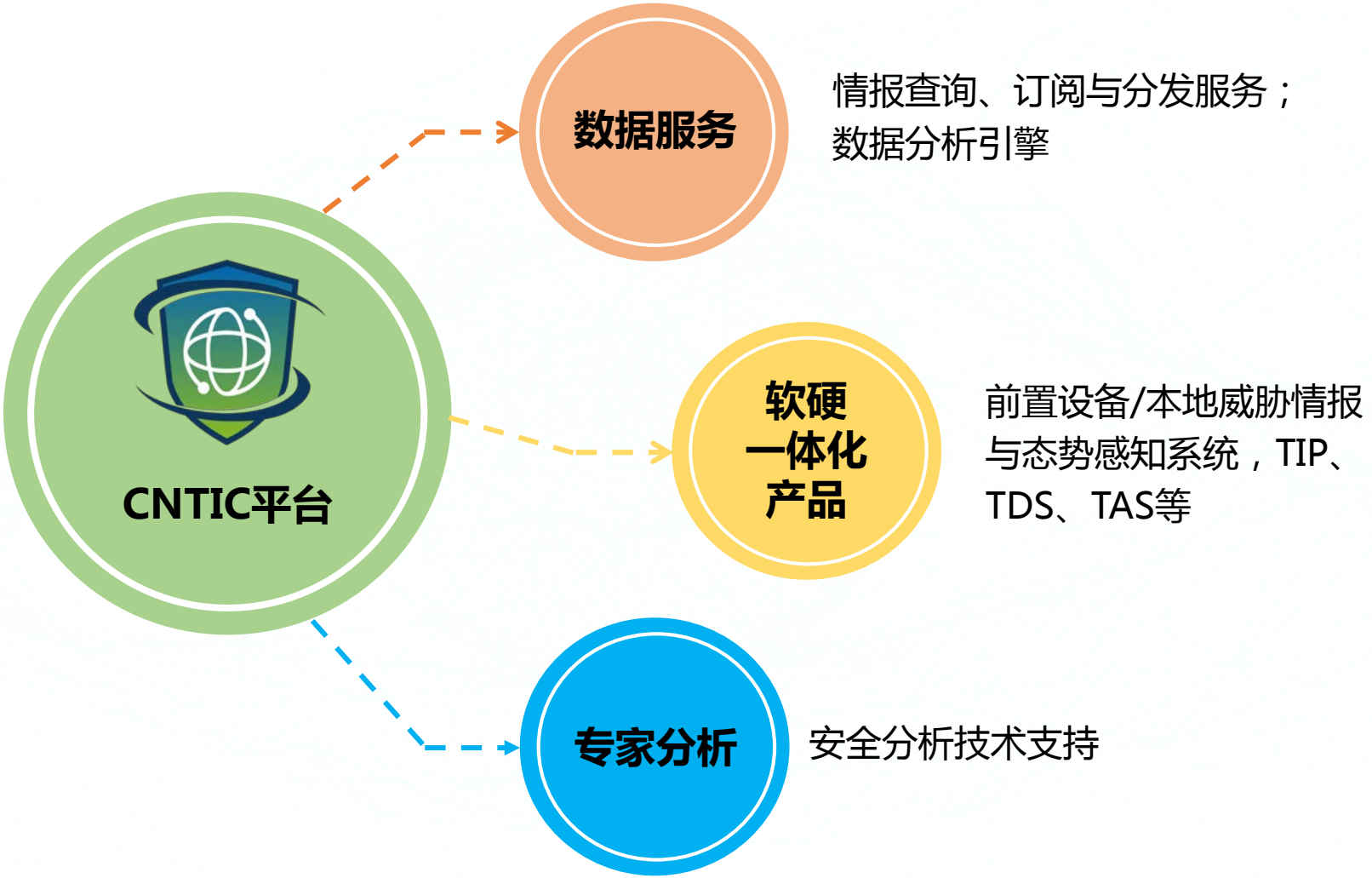

平台接入单位

# 基于STIX/TAXII的部署

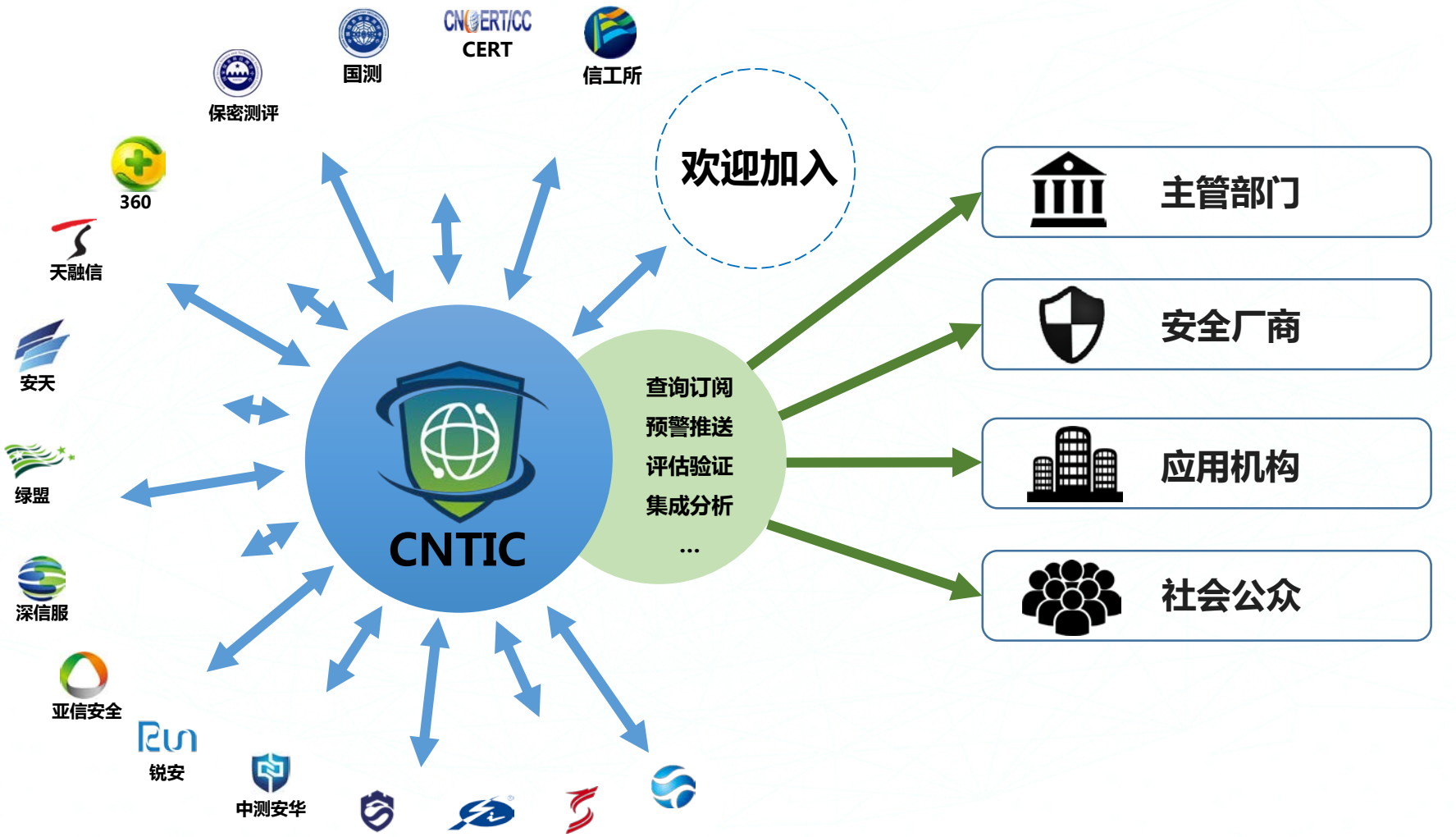



Source：STIX TAXII2 Preferred Training. OASIS

# 服务形式


数据服务
情报查询、订阅与分发服务；
数据分析引擎
CNTIC平台
软硬
一体化
产品
前置设备/本地威胁情报
与态势感知系统，TIP、
TDS、TAS等
专家分析
安全分析技术支持

# 一点发现威胁、快速共享情报、全网联动防御



# 微信公众号

CNTIC

首个政企合作的国家级

网络空间威胁情报共享开放平台

连接政府与企业的“桥梁”与“纽带”

关注公众号（微信号CNTIC2017）后，点击“联盟信息”栏目可见联系信息

# 谢谢！

中科院信工所CNTIC工作组