协同安全能力 共建情报生态

# 威胁情报生态大会

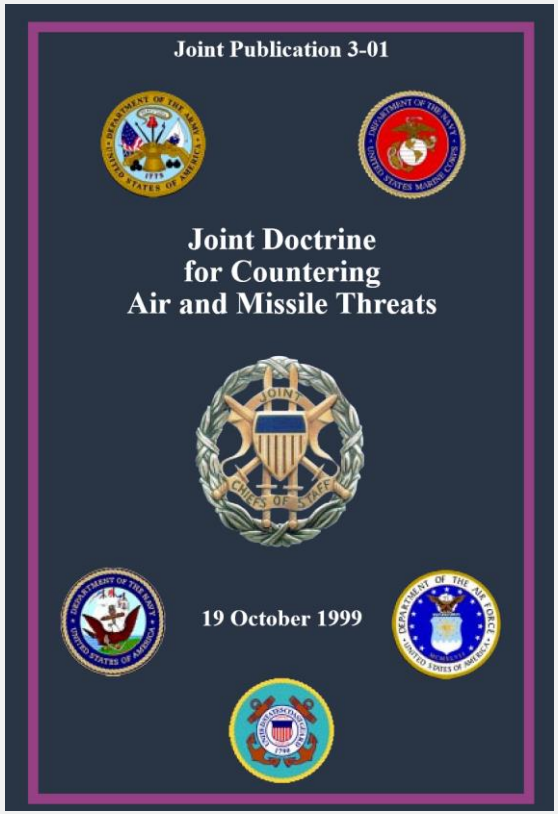
杨大路 天际友盟CEO

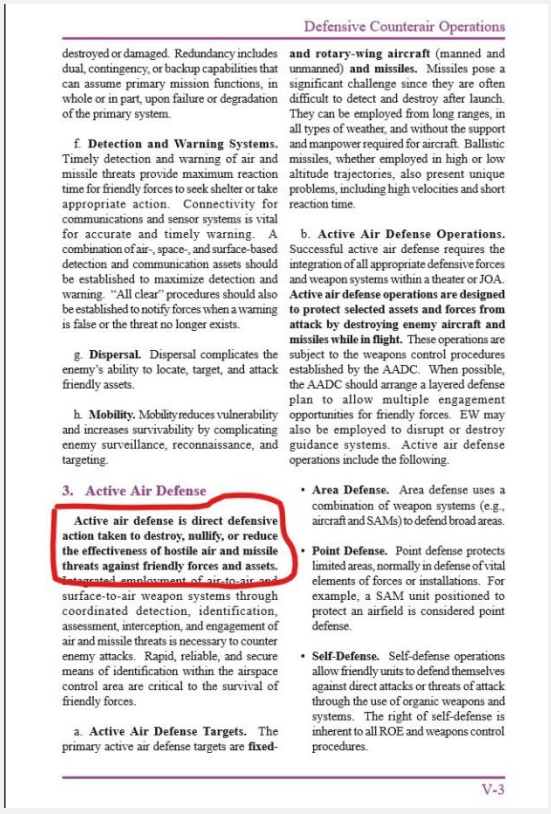
# 利用外部情报平台，构建主动防御体系

北京天际友盟信息技术有限公司
领先的数字风险解决方案提供商

# 目录
CONTENT

# 主动防御概念的缘起



Defensive Counterair Operations

destroyed or damaged. Redundancy includes dual, contingency, or backup capabilities that can assume primary mission functions, in whole or in part, upon failure or degradation of the primary system.

f. **Detection and Warning Systems.** Timely detection and warning of air and missile threats provide maximum reaction time for friendly forces to seek shelter or take appropriate action. Connectivity for communications and sensor systems is vital for accurate and timely warning. A combination of air-, space-, and surface-based detection and communication assets should be established to maximize detection and warning. "All clear" procedures should also be established to notify forces when a warning is false or the threat no longer exists.

g. **Dispersal.** Dispersal complicates the enemy's ability to locate, target, and attack friendly assets.

h. **Mobility.** Mobility reduces vulnerability and increases survivability by complicating enemy surveillance, reconnaissance, and targeting.

### 3. Active Air Defense

**Active air defense is direct defensive action taken to destroy, nullify, or reduce the effectiveness of hostile air and missile threats against friendly forces and assets.** Integrated employment of air-to-air and surface-to-air weapon systems through coordinated detection, identification, assessment, interception, and engagement of air and missile threats is necessary to counter enemy attacks. Rapid, reliable, and secure means of identification within the airspace control area are critical to the survival of friendly forces.

a. **Active Air Defense Targets.** The primary active air defense targets are **fixed-and rotary-wing aircraft** (manned and unmanned) **and missiles.** Missiles pose a significant challenge since they are often difficult to detect and destroy after launch. They can be employed from long ranges, in all types of weather, and without the support and manpower required for aircraft. Ballistic missiles, whether employed in high or low altitude trajectories, also present unique problems, including high velocities and short reaction time.

b. **Active Air Defense Operations.** Successful active air defense requires the integration of all appropriate defensive forces and weapon systems within a theater or JOA. **Active air defense operations are designed to protect selected assets and forces from attack by destroying enemy aircraft and missiles while in flight.** These operations are subject to the weapons control procedures established by the AADC. When possible, the AADC should arrange a layered defense plan to allow multiple engagement opportunities for friendly forces. EW may also be employed to disrupt or destroy guidance systems. Active air defense operations include the following.

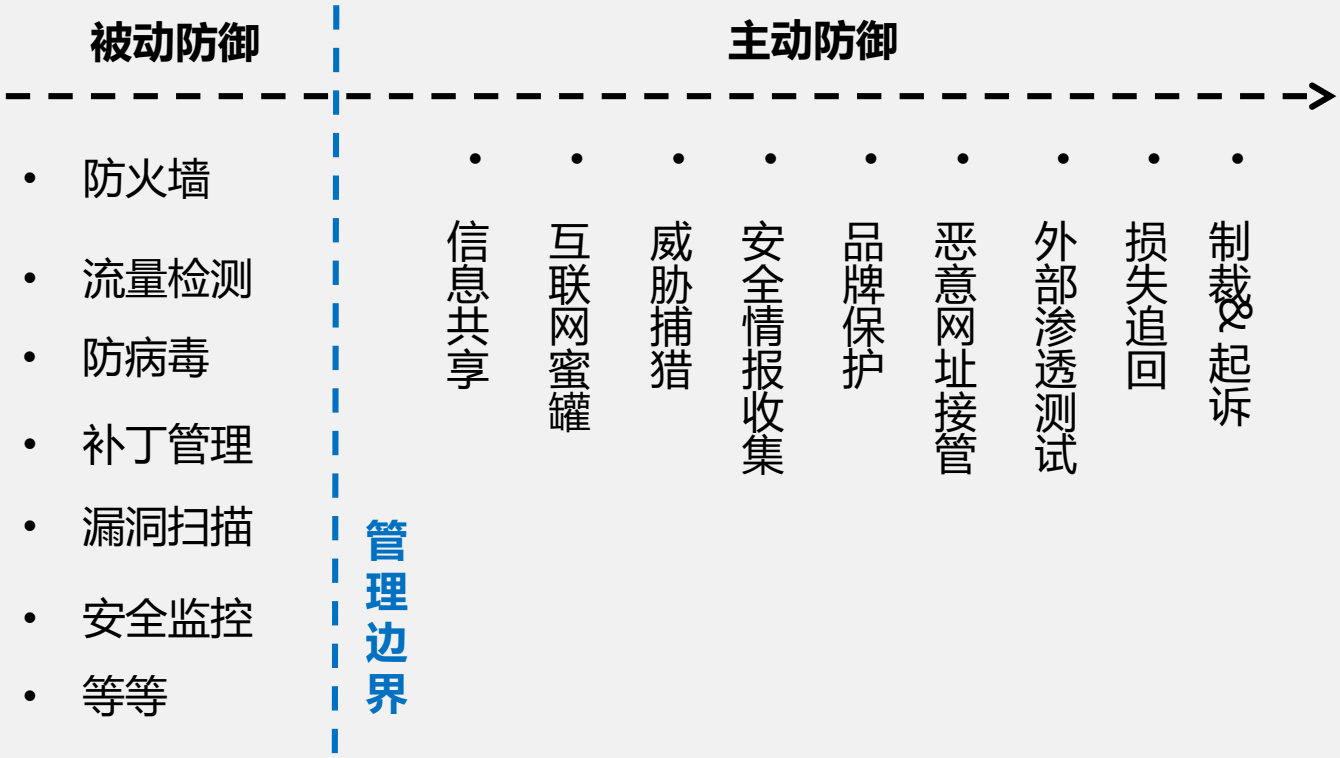
- **Area Defense.** Area defense uses a combination of weapon systems (e.g., aircraft and SAMs) to defend broad areas.
- **Point Defense.** Point defense protects limited areas, normally in defense of vital elements of forces or installations. For example, a SAM unit positioned to protect an airfield is considered point defense.
- **Self-Defense.** Self-defense operations allow friendly units to defend themselves against direct attacks or threats of attack through the use of organic weapons and systems. The right of self-defense is inherent to all ROE and weapons control procedures.

V-3

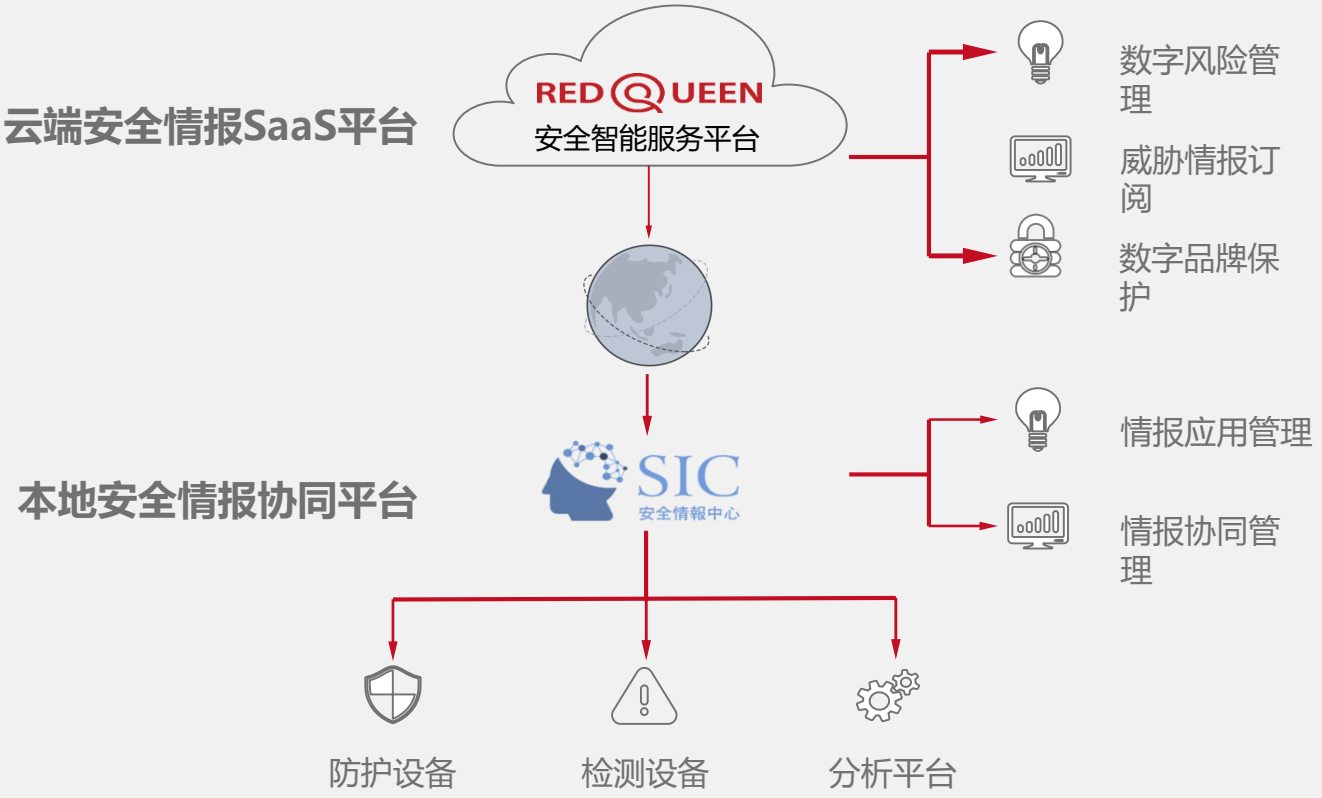
美军在《Joint Publication 3-01》出版物中首次提出了主动防御的概念

采取直接防御行动，摧毁、消除或降低攻击对我方资产威胁的有效性

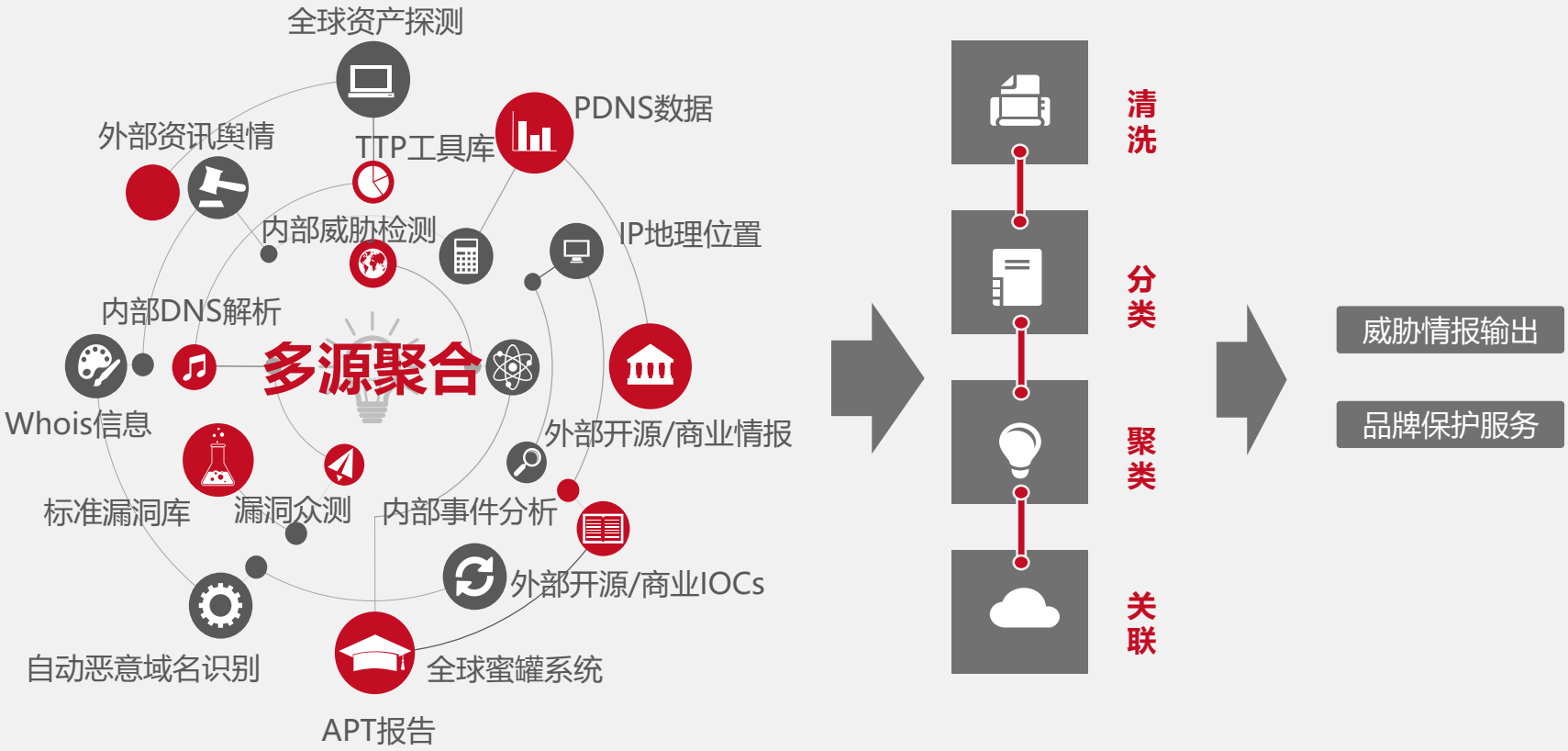
# 主动防御手段举例


被动防御
主动防御
防火墙
流量检测
防病毒
补丁管理
漏洞扫描
安全监控
等等
管理边界
信息共享
互联网蜜罐
威胁捕猎
安全情报收集
品牌保护
恶意网址接管
外部渗透测试
损失追回
制裁&起诉

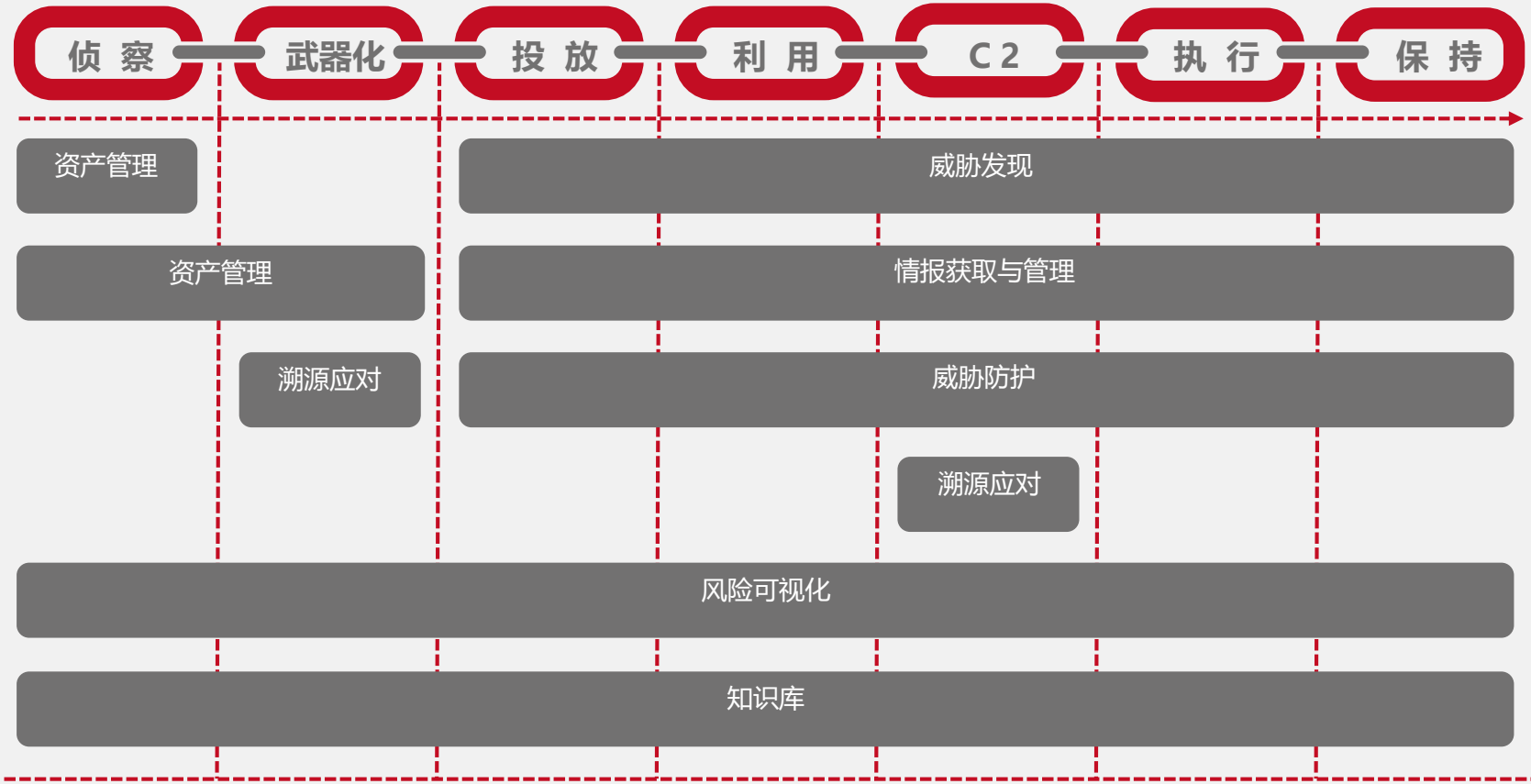
# 安全威胁情报平台


云端安全情报SaaS平台
RED QUEEN
安全智能服务平台
数字风险管理
威胁情报订阅
数字品牌保护
本地安全情报协同平台
SIC
安全情報中心
情报应用管理
情报协同管理
防护设备
检测设备
分析平台

# 基于数据管理能力的情报提供和处置服务



# 基于“Kill Chain”攻击视角防护的情报应用



# 基于最佳实践的情报订阅模式

## 国际最佳实践：基于标准化的“情报市场”订阅模式


ICS 35.040
L80

GB

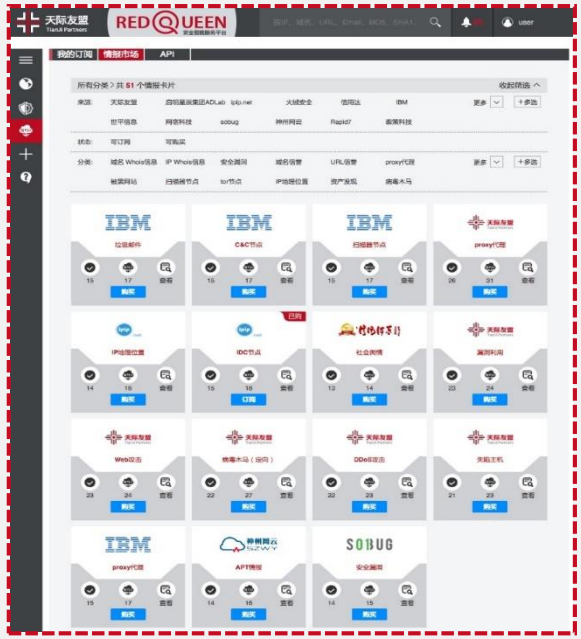
中华人民共和国国家标准

GB/T 36643—2018

信息安全技术 网络安全威胁信息格式规范

Information security technology —Cyber security threat information format

2018-10-10


# 云端&本地结合的威胁知识库

**重点一**

形成安全信息溯源知识库，，对结构化和非结构化的各类安全信息按照规定的数据结构进行统一解析入库，并进行分类存储并管理。

**重点二**

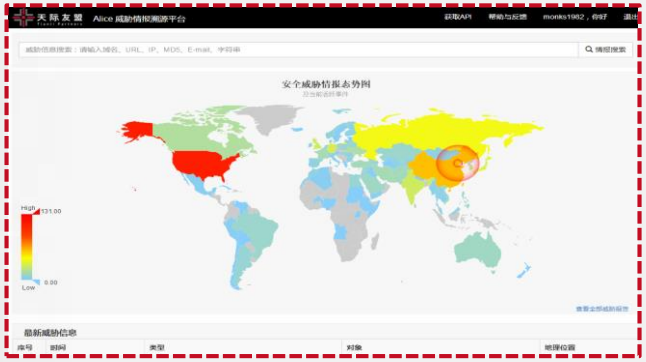
设计关联分析算法模型，构建可视化关联分析模块，实现对IP、域名、URL、文件Hash、Email等的可视化溯源检索能力。

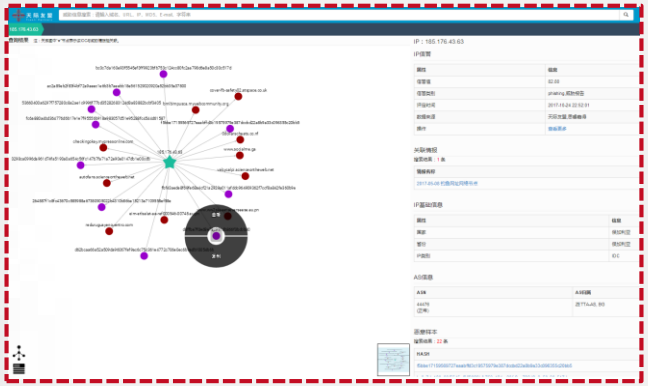
**重点三**

设计异步数据扩展机制，根据溯源请求和结果，通过定制数据接口，以异步方式从其他平台扩展和补充缺失信息入库。

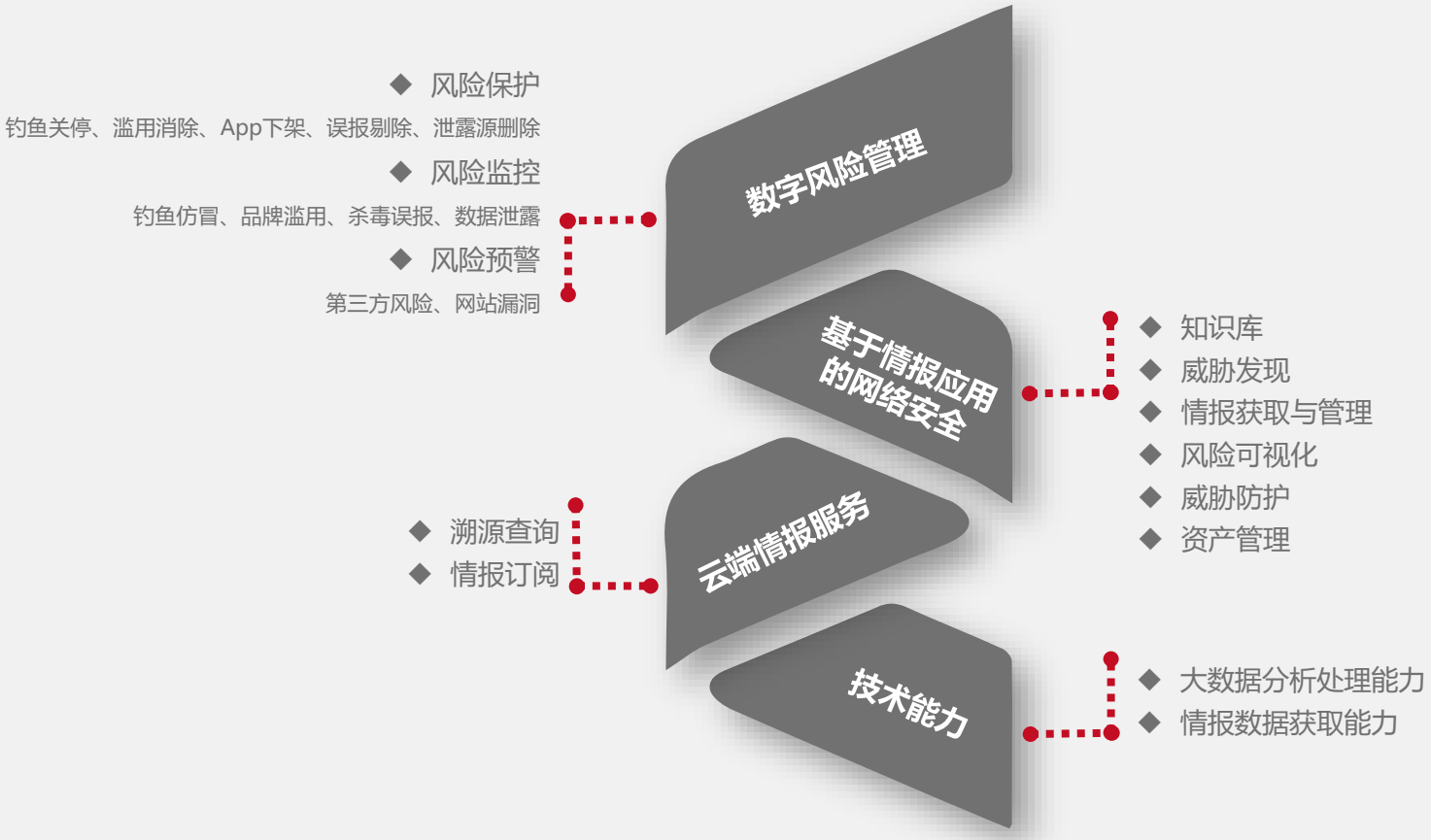
**重点三**

设计相应的溯源查询接口，支持单条查询和批量查询，并实现基于Web界面调用的溯源能力共享。



# 威胁情报平台能力成长路线



# 利用情报平台快速构建主动防御体系



01

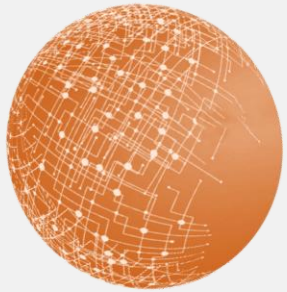
企业现有安全能力结合情报平台，快速构建主动防御体系

02

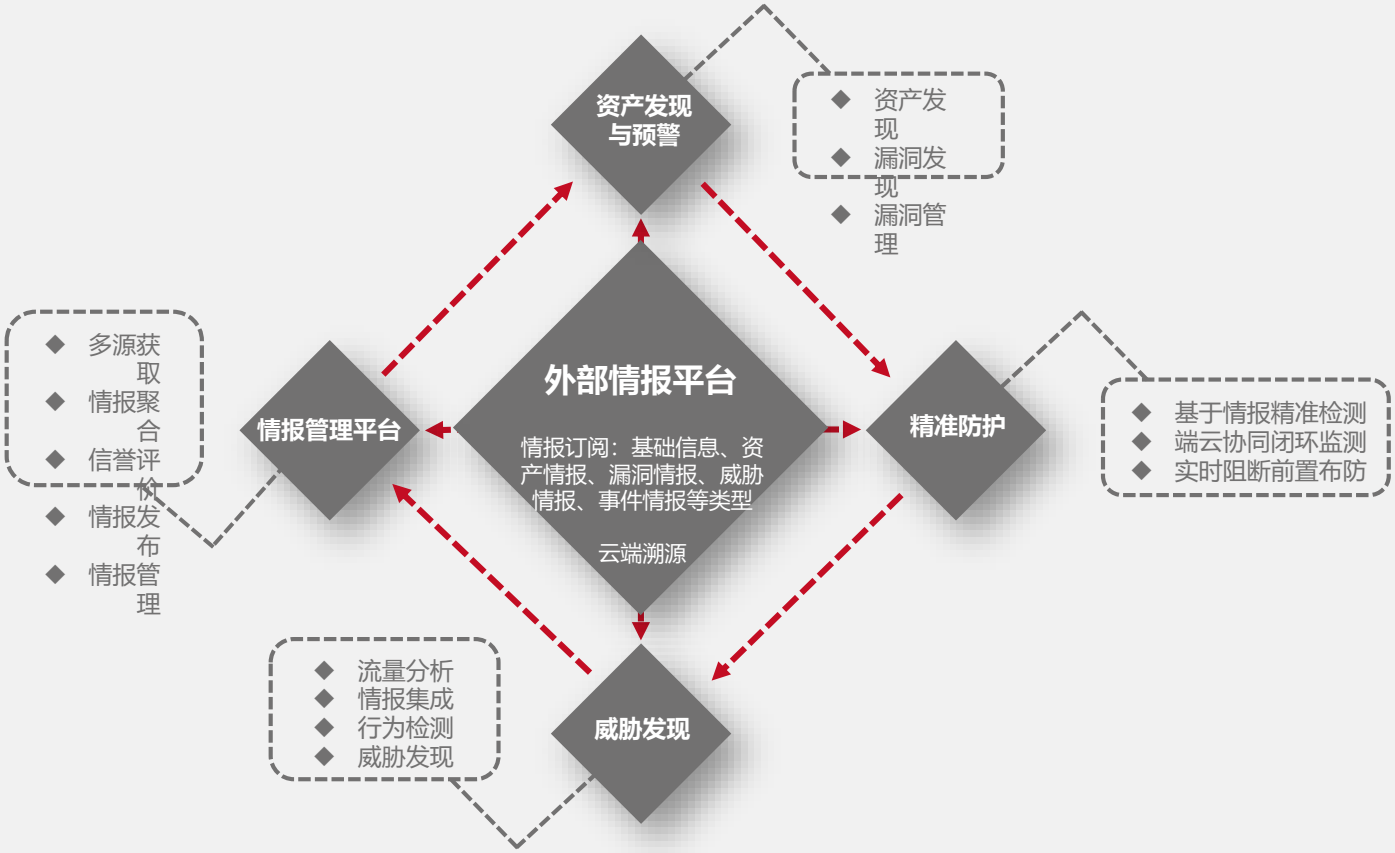
厂商现有产品对接情报平台，构建具备主动防御能力的产品解决方案

03

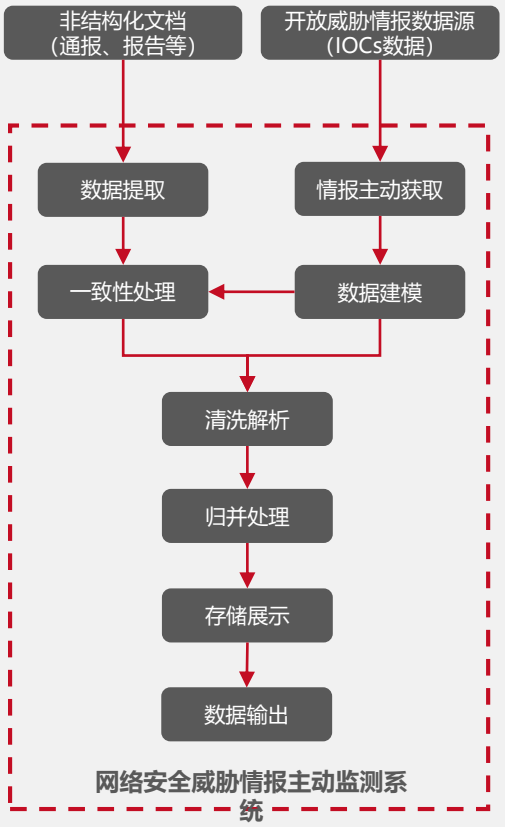
重点行业通过建设行业级情报平台，实现行业间情报共享能力



# 情报平台在企业的典型应用场景



# 情报平台在企业的典型应用场景




## 关键技术

1）智能爬虫技术：实现开放威胁情报的主动获取。

2）基于自然语义识别的信息提取技术：实现对非结构化文档的威胁信息提取。

3）威胁信息表达模型：参考国标、STIX标准，实现统一的情报数据建模。

## 关键技术

1）接入84个开放威胁情报源并可灵活扩展，输入支持TXT、CSV、JSON等多种格式，情报输出支持STIX2.0格式。

2）前端探测Proxy自动或随机切换，支持身份认证配置。

3）具备数据源日志追踪、“热”接入与“热”推出功能。

4）支持从HTML、DOC、PDF等文档提取威胁信息。

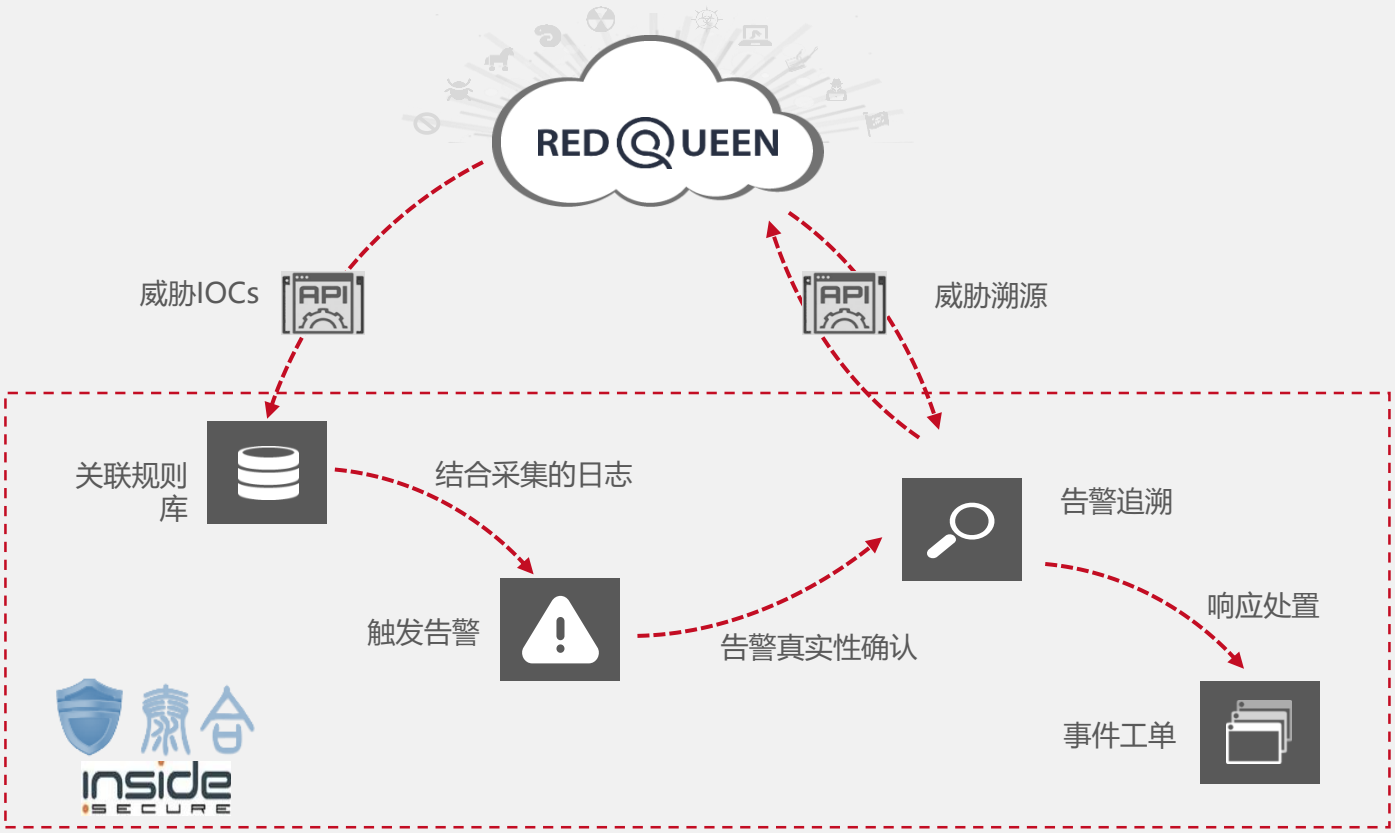
5）可提供不少于1000条的黑客组织或团伙威胁情报信息。

## 预期效果

1）丰富的威胁情报数据源，辅助对事件、团伙的监测与分析。

2）实现对非结构化文档的自动信息提取，改变人工处理模式，提升工作效率。

# 情报平台与安全产品的典型结合场景



# 情报平台与安全产品的典型结合场景

外部情报
分发至本地

SIC
安全情报中心

情报输出

| | | |
|---|---|---|
| 钓鱼网址 | 恶意软件 | 恶意邮件 |
| 色情、赌博 | 勒索软件 | C&C节点 |
| proxy代理 | 木马软件 | 僵尸网络 |
| tor节点 | 垃圾邮件 | 扫描器节点 |

**上行流量**

- 钓鱼、色情、赌博等站点的违规外联
- 与C&C、TOR、僵尸网络等相关的可疑外

...

**下行流量**

- 过滤恶意、垃圾邮件
- 阻断外部扫描行为
- 切断恶意软件、勒索软件

...

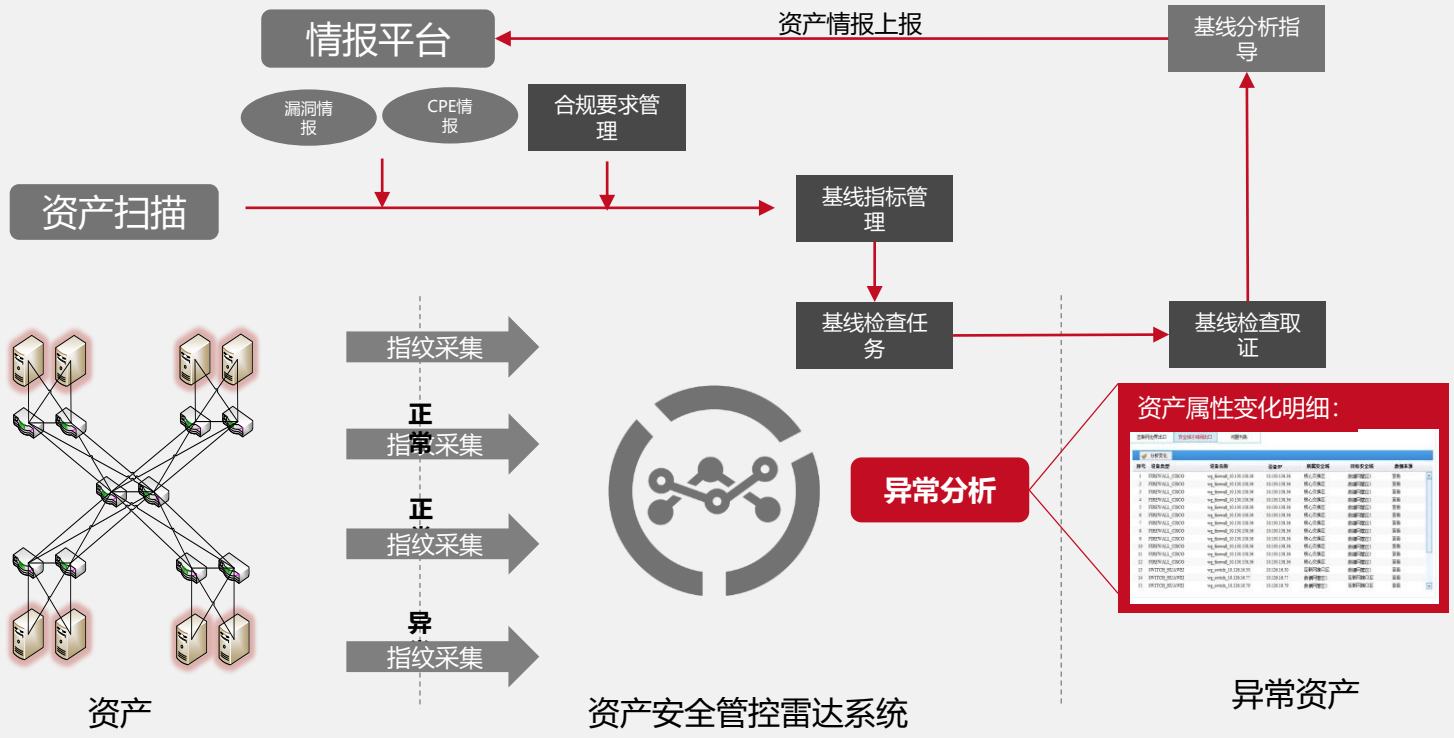
NGFW

1、实现外部情报与本地上/下行流量日志的命中匹配；

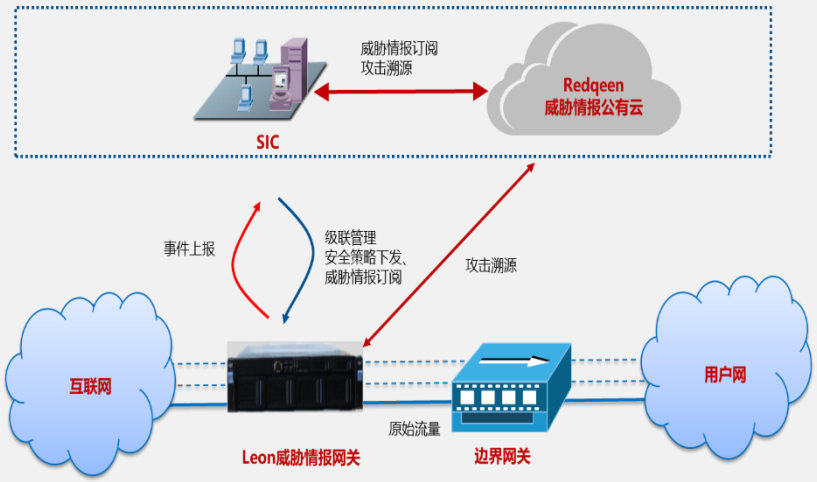
2、根据命中匹配结果，自动过滤恶意的访问和外联行为。

# 情报平台与安全产品的典型结合场景

# 情报平台与安全产品的典型结合场景



# 情报平台与安全产品的典型结合场景




**检测** 提供高价值威胁情报驱动的全面检测能力

**分析** 与SIC协同，判定网络威胁并还原攻击场景

**溯源** 提供基于域名、IP、URL、Email地址等威胁信息的溯源分析查询

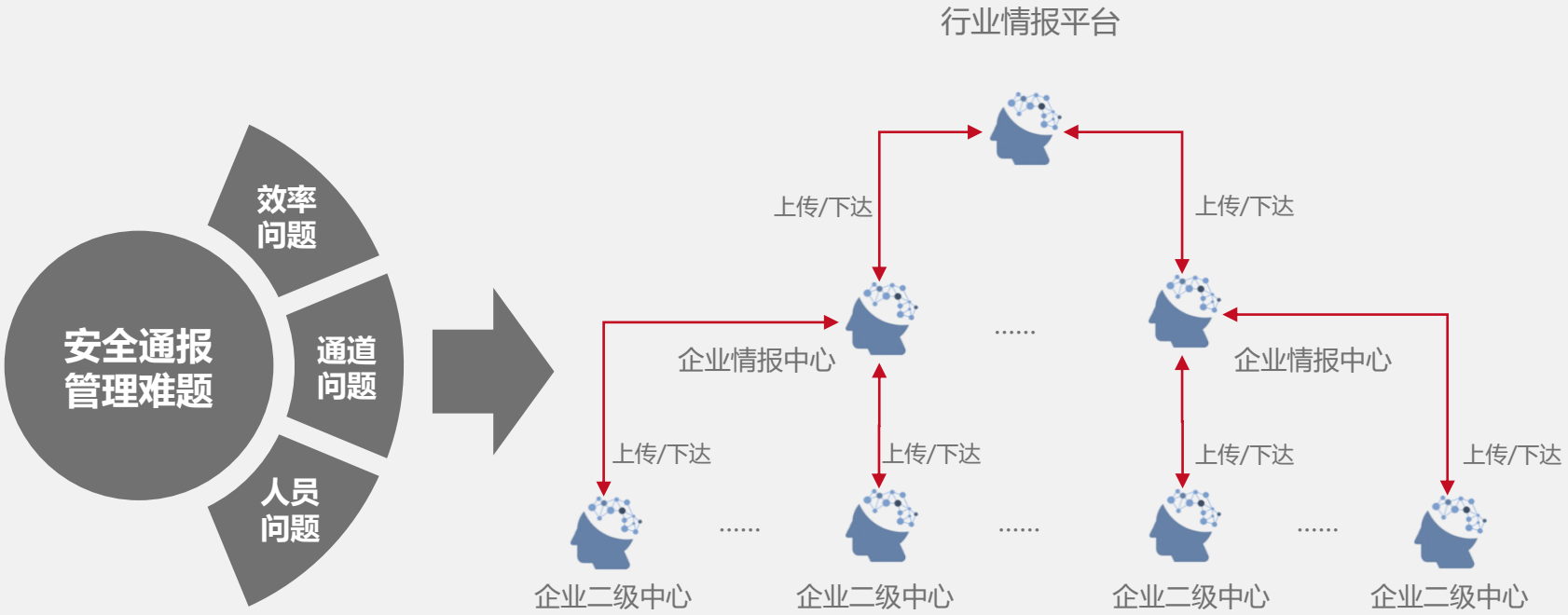
**画像** 对攻击流程、攻击者信息、攻击手段全景再现，进行攻击者画像分析

**响应** 支持报警、阻断、提取威胁情报IOC等响应方式

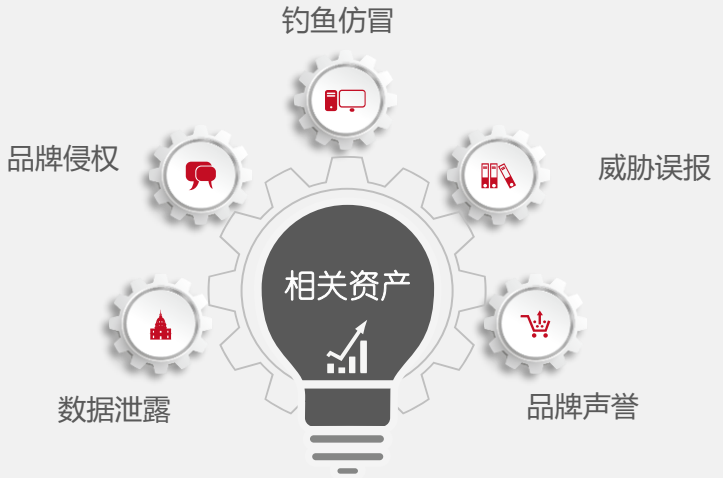
**处置** 对安全威胁进行有效处置

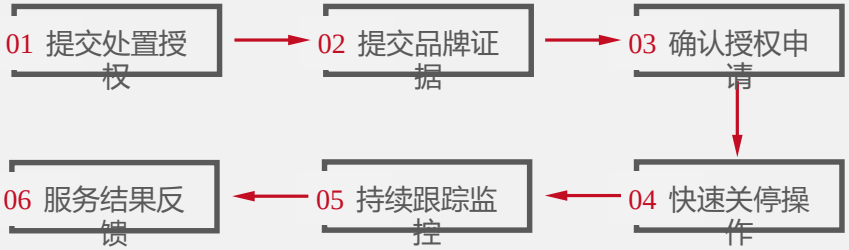
# 情报平台在行业共享中的典型应用

## 建设行业情报平台，构建行业内主动防御体系



# 主动防御体系的最外部环节：数字品牌保护

# 天际友盟，领先的数字风险解决方案提供商

谢 谢！