威胁情报：信息 OR 情报？

十年攻防，一朝成盾

情报学的争论
LIS VS IS

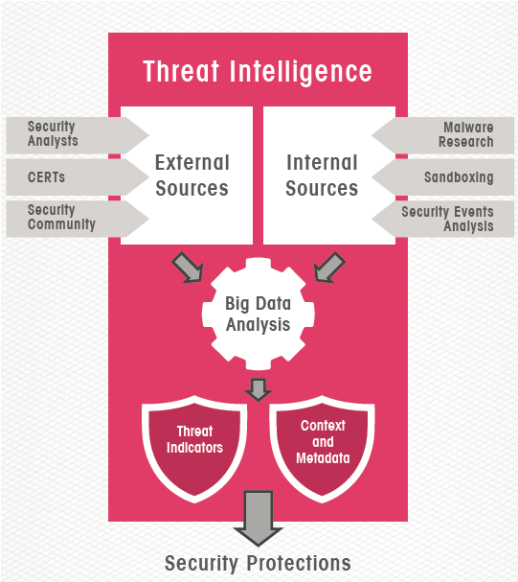
	LIS	IS
情报本质的定义	情报是针对特定用途有传递价值的信息或有传递价值的知识	信息是原料，情报是产品；信息是客观事物的反映，情报是人脑思维的产物。即情报是组织对环境变化的感知和响应。 认为Information派只是资讯学、不是情报学；
`现状	国家层面认知：1992年科委将科技情报司改名科技信息司	美英大学要么关闭LIS学院，要么转为IS学院

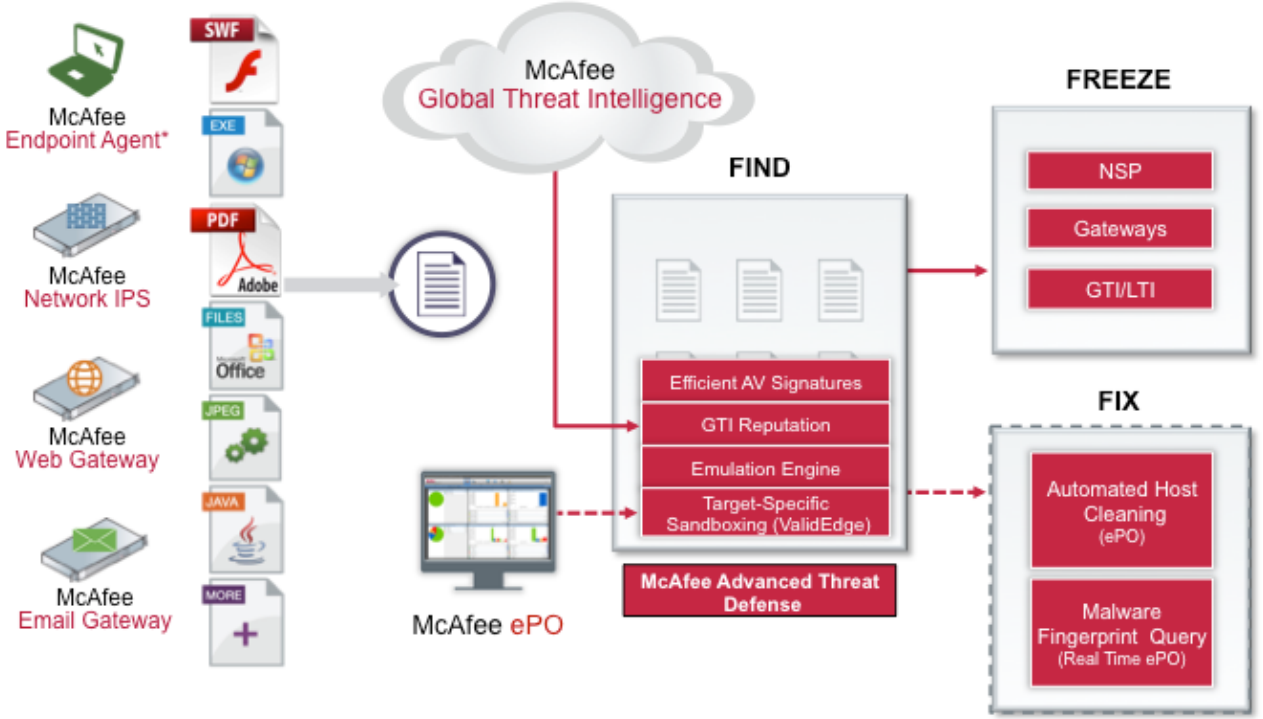
现代情报学

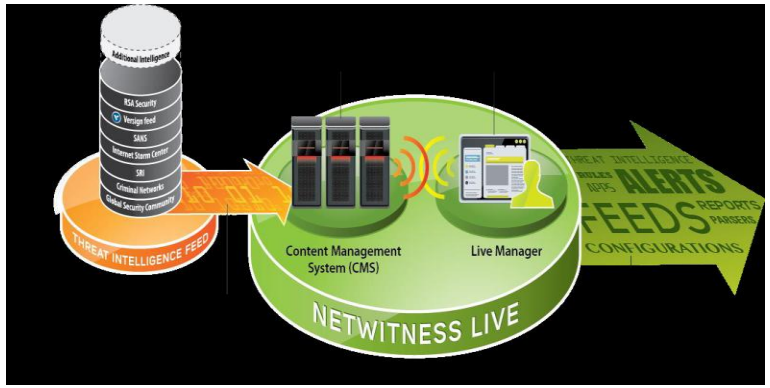
竞争情报 ，情报与安全信息

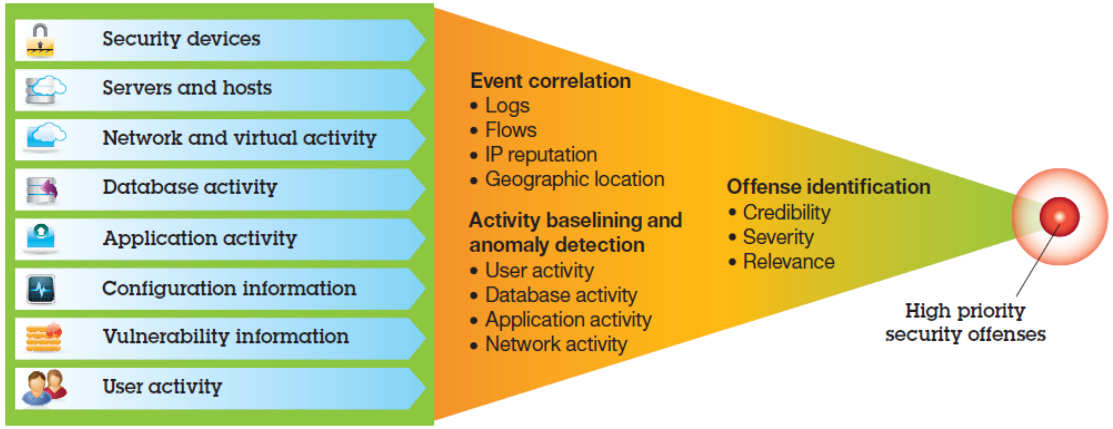
	传统情报学	竞争情报	情报与安全信息
使命	对特定目标提供有价值的知识与信息	赢得竞争优势、降低风险	赢得对抗优势、降低风险
核心目标	发现有价值的知识与信息	预测、决策	预测、决策、取证
核心工作	发现知识组织关联	信息序化、信息分析、学习系统	信息序化、信息分析、学习系统、模拟验证系统 特别关注组织和人的关系描述、人的行为与意图分析
特定属性	知识性、可传递性	信息性（包含知识）、可传递性	信息性（包含知识）、可传递性
		隐蔽性、价值选择性、对抗性、预测&决策性、时效性	隐蔽性、价值选择性、对抗性、预测&决策性&可举证性、时效性

威胁情报现状
产业界在延续LIS的定义









威胁情报现状

用户的期待：获得或赢得竞争&对抗

单纯的防御已不能应对威胁

我的弱点

我的优势

我的行动

对手弱点

对手能力

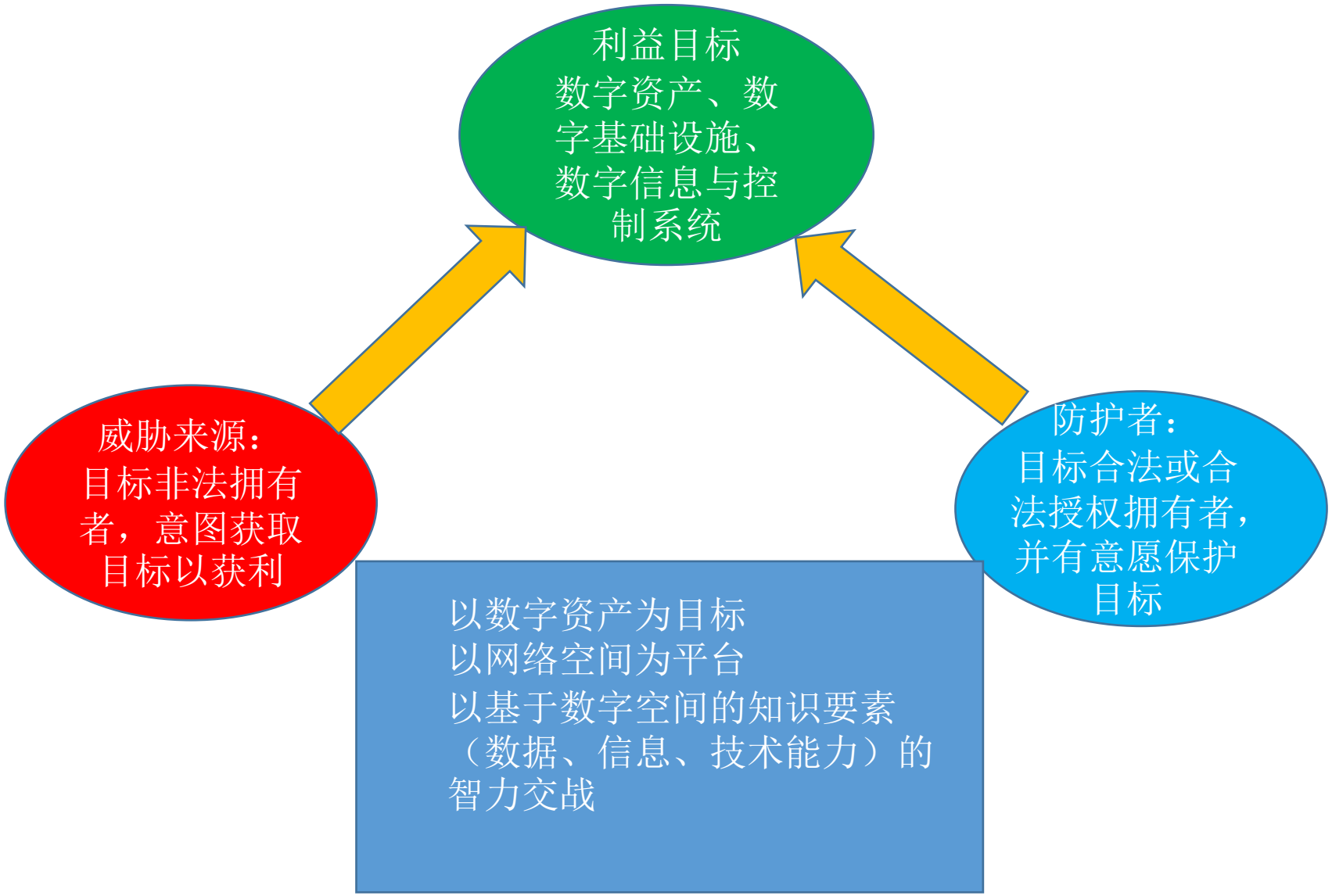
对手行动

核心目标

主要对手？

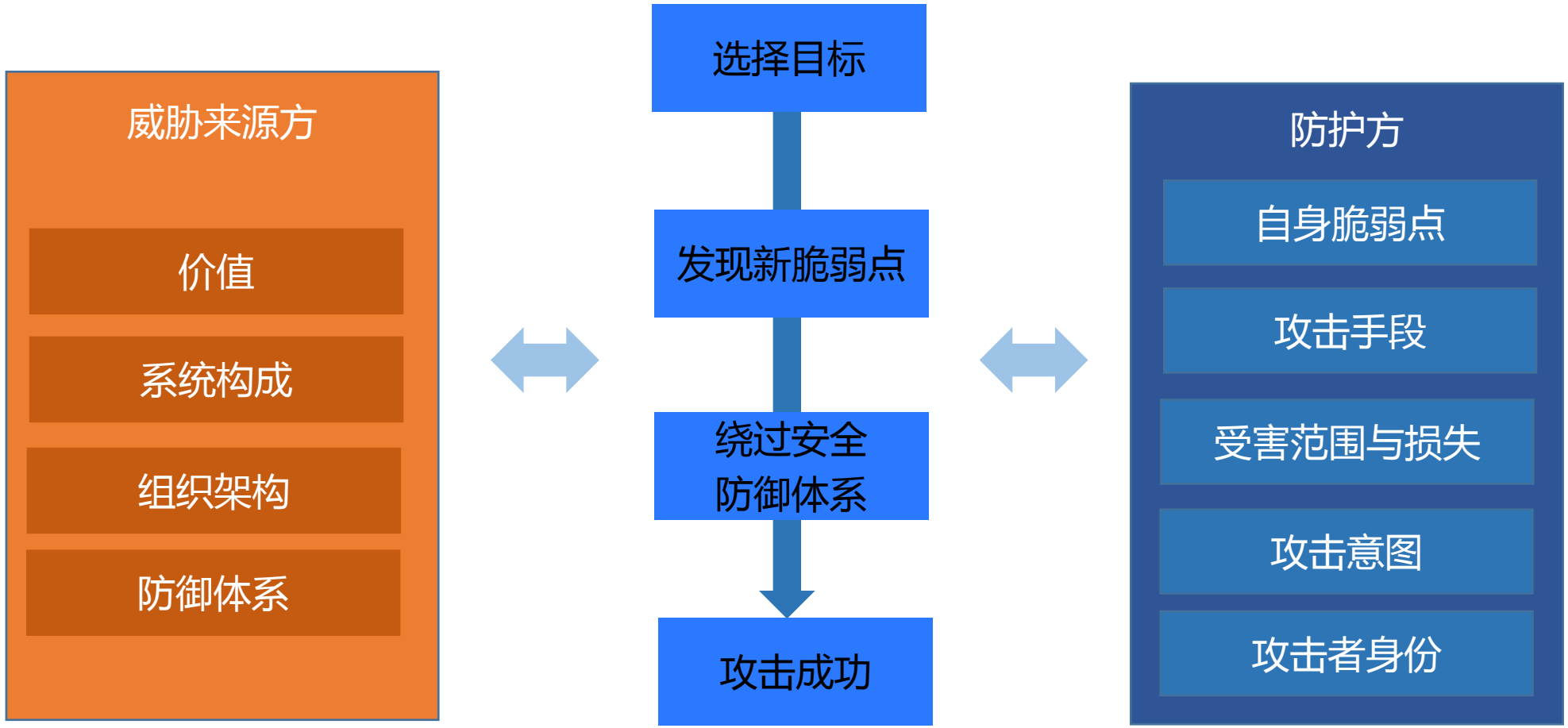
威胁本质

网络空间的威胁来自对抗



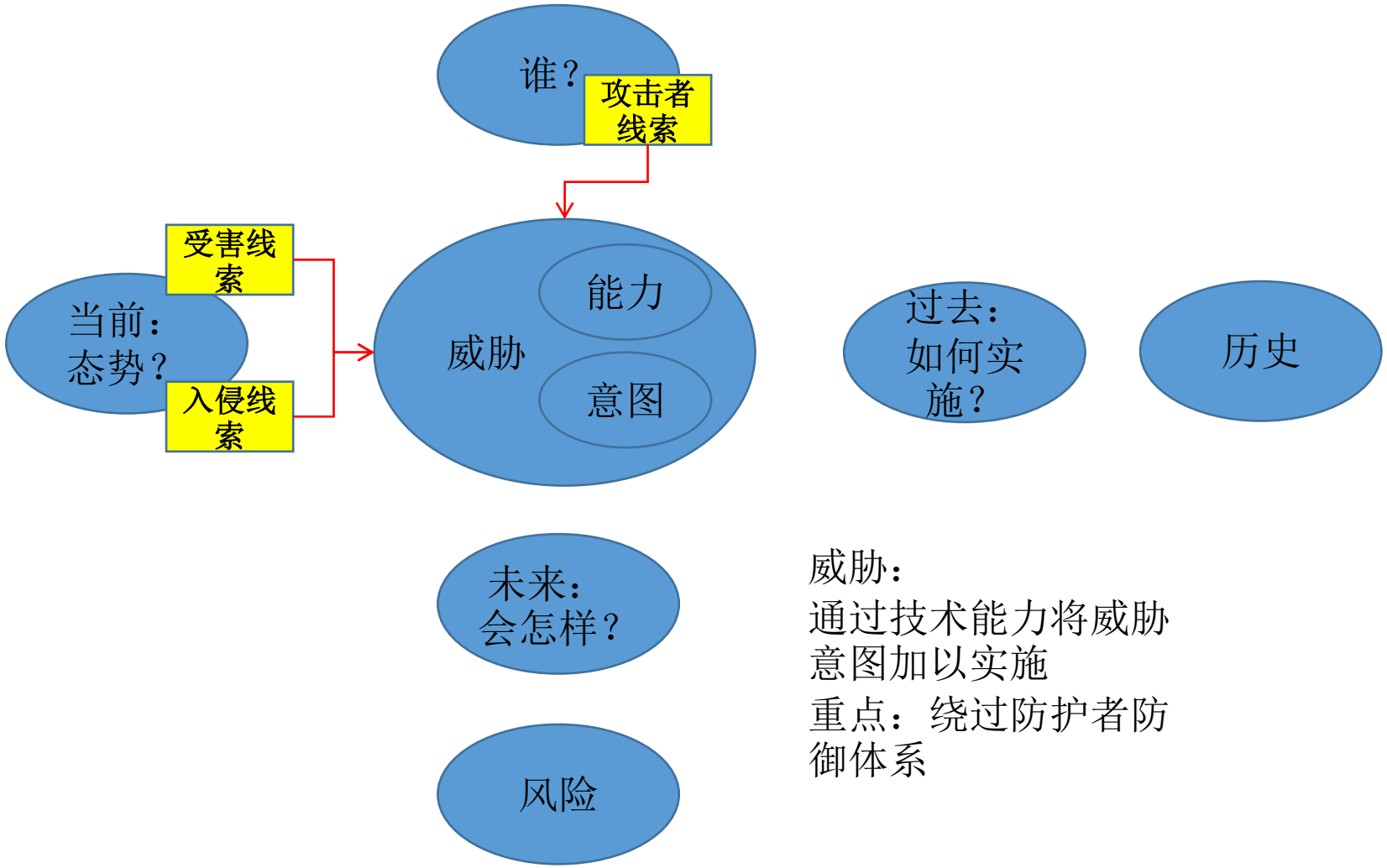
对抗本质

人或组织之间：智力、知识和情报、能力、资源的全方位对抗



单点的防御者威胁情报视角

线索-〉现状-〉监测-〉溯源-〉预测



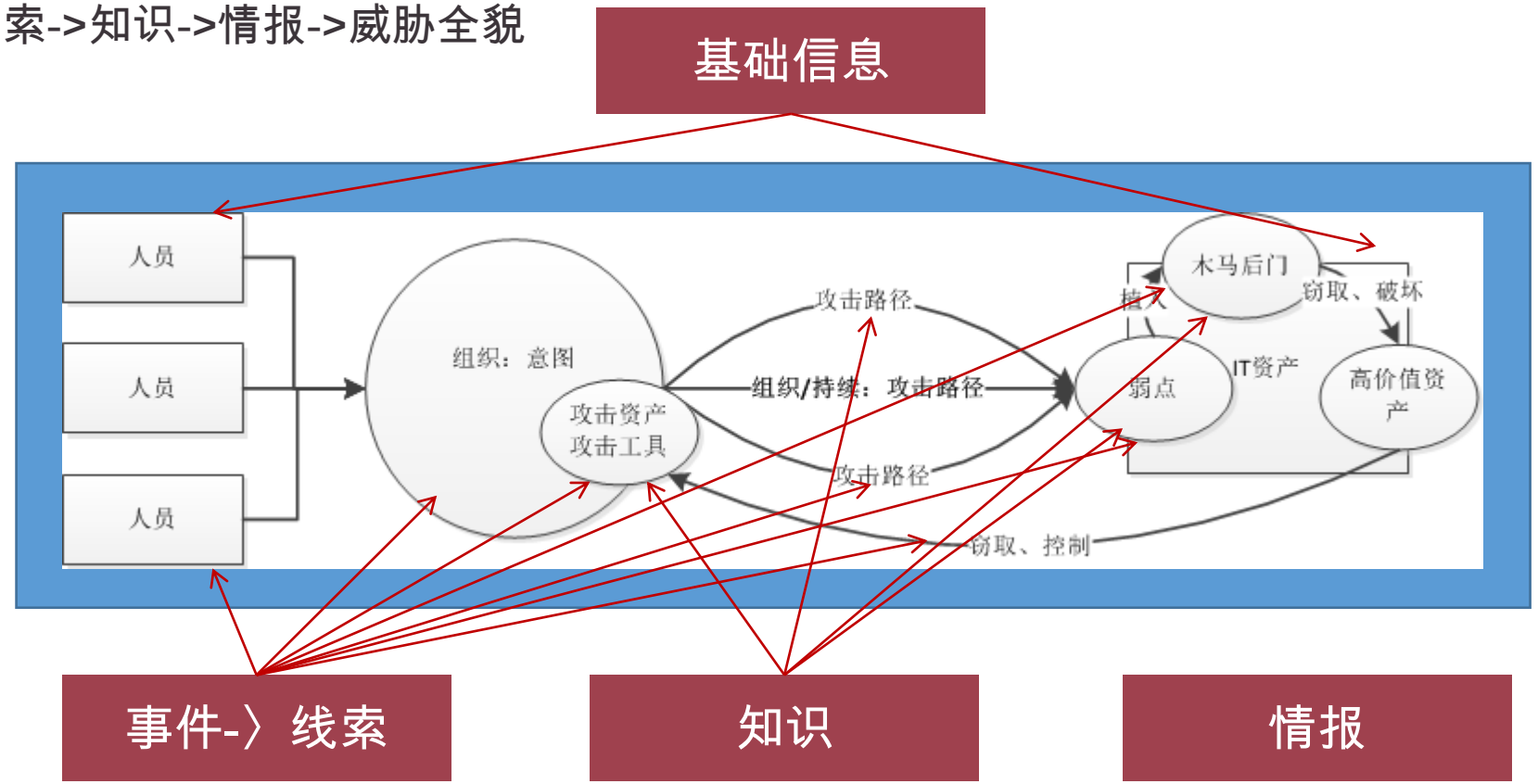
威胁：

通过技术能力将威胁意图加以实施

重点：绕过防护者防御体系

全景视角的威胁情报

基础信息|线索->知识->情报->威胁全貌



还原事实：描述或补全对全景描述的重要未知细节（过去、现在、谁）

分析原因：分析攻击者意图、拥有的资源能力、防御者的弱点

着眼未来：对威胁进行预测、评估长远趋势、风险、提出应对策略

阿里威胁情报体系
大数据场景

情报：威胁场景

情报：威胁态势

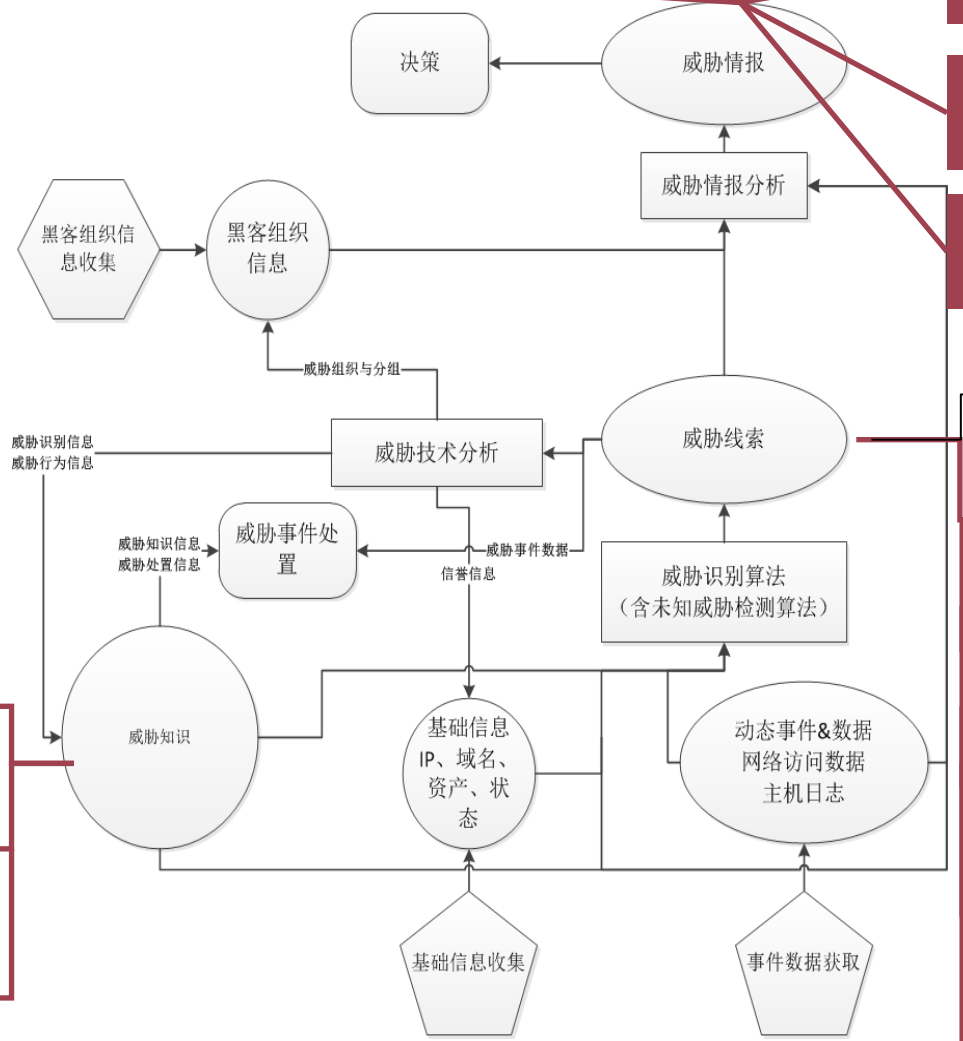
情报：威胁来源

情报：威胁意图

情报：威胁能力

情报：威胁风险

情报：威胁预判



知识：威胁识别

知识：威胁处置

知识：威胁DNA

线索：泄露事件

线索：弱点暴露

线索：恶意样本

线索：入侵事件

线索：黑客动向

线索：受害|恶意

我们希望的威胁情报体系
对齐语义，理解阿里的威胁情报理念

- 威胁知识： 描述识别威胁、威胁DNA、威胁处置的信息
- 威胁情报： 发现或分析出来的描述威胁要素相关的信息；目的是补全威胁全景相关的信息。用于深入分析和追溯威胁。包括
  - 威胁场景（过去）：攻击者历史上如何发起攻击，并逐步渗透达到现在的态势
  - 威胁态势（现在）：那些IT资产会受到攻击影响，攻击者已经入侵成功的IT资产、攻击者动用的工具与资源、攻击者目前正在发起什么攻击或攻击准备，攻击者已经拿走了什么重要资产（损失、意图猜测）
  - 威胁能力：基于过去和现在，可以评估能力：组织性、持续性、技术手段、规模
  - 威胁来源：追溯出背后具体的数字犯罪组织、数字犯罪成员；如果可以还能关联更多其它的威胁，分析更大的威胁场景、威胁态势、威胁能力
  - 威胁意图：基于以上信息（目标/组织性/能力/造成的损失），可以评估威胁者意图
  - 威胁预测：评估或获取到攻击者/组织可能采取的下一步行为
  - 威胁风险：判断攻击者/组织长期的行为，可能的损失，威胁的风险
- 威胁线索情报：被发现的当前看起来孤立的威胁的单一信息，一般来源于具体事件中的发现；通过威胁线索与各类知识、信息、事件的关联分析，可以获得更多威胁全景的信息
- 基础信息情报： 描述出IT资产、人员的信息，用于更好关联分析黑客组织、威胁场景、态势、能力、意图
- 事件&数据： 动态实时发现在数字世界的交互类数据，从中依据威胁的知识或异常准则或者线索识别出威胁线索

威胁情报语义定义

基础信息、事件、线索、知识、情报

	基础信息	事件	线索（威胁事件）	知识	情报
静态|动态	静态	动态	动态，可关联静态	静态	动态
叙述|指导	叙述	叙述	叙述	指导	叙述
威胁信息			微观	微观	微观+宏观
对应行动				应急	决策
信息要求			视威胁情况选择公开或保密	公开	根据决策在一定范围公开
价值性			对特定目标	所有目标	特定目标
主观客观性	客观	客观	客观	客观	带一定主观

阿里威胁情报与CI、ISI

	竞争情报	情报与安全信息	阿里威胁情报
使命	赢得竞争优势、降低风险	赢得对抗优势、降低风险	赢得对抗优势、降低风险
核心目标	预测、决策	预测、决策、取证	预测、决策、取证
核心工作	信息序化、信息分析、学习系统	信息序化、信息分析、学习系统、模拟验证系统 特别关注组织和人的关系描述、人的行为与意图分析	信息序化、信息分析、学习系统、模拟验证系统 关注组织和人的关系描述、人的行为与意图分析 大数据是核心能力
特定属性	信息性（包含知识）、可传递性	信息性（包含知识）、可传递性	信息性（包含知识）、可传递性
	隐蔽性、价值选择性、对抗性、预测&决策性、时效性	隐蔽性、价值选择性、对抗性、预测&决策性&可举证性、时效性	隐蔽性、价值选择性、对抗性、预测&决策性&可举证性、时效性
	现实生活、对手合法对抗	现实生活，对手非法对抗	虚拟世界、对手非法对抗

LIS定义威胁情报的好处

知识与信息可以产品化输出

	威胁知识	威胁情报
信息来源	单一数据	综合数据，包括业务
面向对象	运维与响应人员	高层决策人员
使用限制	无价值选择性，可复制输出	有价值选择性，不能复制输出
	较精确，可以指导处置	有一定推测性，需要决策
	弱隐蔽性&保密性&时效性	强隐蔽性&保密性&时效性
结论	可产品化复制输出	只能定制化服务输出
用户需要		

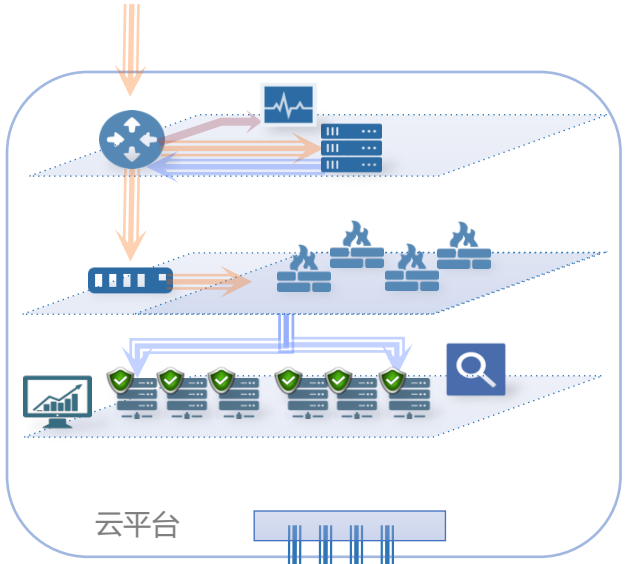
阿里威胁情报为什么要以IS定义为目标

- 对抗环境下，发现线索/威胁，BLOCK线索/威胁并非好的对抗策略
- 大多数用户不仅仅需要知识，更需要威胁情报，才能获得竞争优势
  - 威胁知识到威胁情报，需要用户具备专业安全能力、大数据分析能力，更多外部数据与信息
- 阿里不是IT时代的产品型公司，而是DT时代的数据服务公司
  - 阿里有更综合的数据，可以支撑威胁情报分析与关联
  - 阿里可以通过云提供可复制的定制化服务模式，以满足IS的各项属性需求，而不是以用户产品形态提供

阿里威胁情报
大数据到安全

高级威胁研究　反欺诈研究
漏洞挖掘　渗透测试
威胁情报分析
智能设备、无线安全研究

安全研究团队

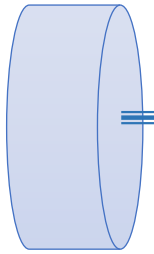


外部威胁
资产价值
脆弱点
安全风险

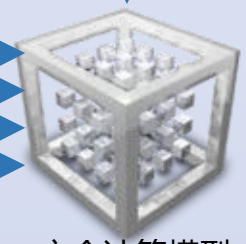
安全策略

安全事件
（人、时间、地点、方法）

安全元数据



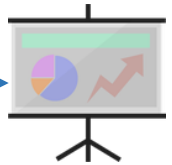
合作方安全信息交换



安全计算模型

大数据
威胁分析平台

大数据团队



当前

过去、未来

威胁情报团队

态势感知

- 风险视图
- 实时展示
- 未知威胁
- 关联分析
- 方案建议

威胁情报

- 安全预测
- 自动策略
- 安全预处理

阿里安全
SECURITY OF ALIBABA

谢谢！

Let’s Talk