情报驱动的安全体系建设

吴云坤　360企业安全集团总裁

数字化转型下的网络安全五大变化

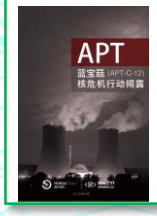
变化的战场

从 网络与系统
到 “云大物移工”

变化的对手

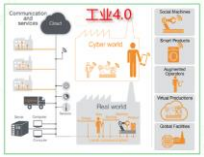
从普通网络犯罪
到组织与国家对抗

变化的武器与战术



勒索蠕虫
高级威胁APT
供应链攻击
……

变化的打击目标



从瞄准网络与系统
到瞄准数据与业务应用

变化的指挥监管

信息安全技术
网络安全等级保护基本要求

Information security technology —

Baseline for classified protection of cybersecurity

护网2016
护网2017
护网2018

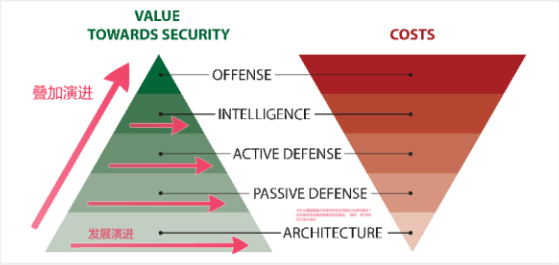
国家战略
法律法规
实战演练

新一代信息化系统安全防护面临的主要问题

- 云计算、大数据等新技术应用改变了信息化和业务环境，带来了新的安全威胁，传统安全技术无法有效应对；
- 传统安全防护手段过多依赖局部、单点防护的低位手段，缺乏基于数据的威胁分析、发现等中高位的安全能力；
- 普遍缺乏全天候、全方位态势感知和安全运营能力和体系。

从被动的威胁应对和标准合规的规划模式，走向面向能力的规划模式

基础结构安全 Architecture	被动防御 Passive Defense	积极防御 Active Defense	情报 Intelligence	进攻性防御 Offense
在系统规划、建立和维护的过程中充分考虑安全防护	在无人员持续介入的情况下，附加在系统架构之上可提供持续的威胁防御或威胁洞察力的系统	分析人员监控和响应网络内部威胁并学习完善防御体系的过程	收集数据、将数据利用转换为信息，并将信息生产加工为评估结果，以填补已知知识缺口的过程	以法律反制措施等形式针对进攻者采取的自我防卫行动



01

网络安全滑动标尺模型

建立了一个分类框架，将网络安全防御相关的各类工作都纳入框架中整体考虑，解决"淘汰演进"迷思给业界带来的长期困扰，从更系统化的"叠加演进"视角考虑整合的防御体系，并更加强调防御能力的"操作化"。

成熟度模型

先左后右
夯实基础
逐步提高成熟度

互为依托
相互联动
协同形成整体能力

非割裂连续体

面向能力的体系化同步建设模式

面向能力的体系化同步建设模式
VS
面向检查的合规点建设模式 & 面向威胁的应对建设模式

关键点1：关口前移，与信息化同步规划与建设的综合防御能力体系

偏静态的
综合防御能力体系

深度结合、全面覆盖

关键点2：威胁情报是构建积极防御能力体系的关键

场景1：威胁情报提供了新型的检测能力

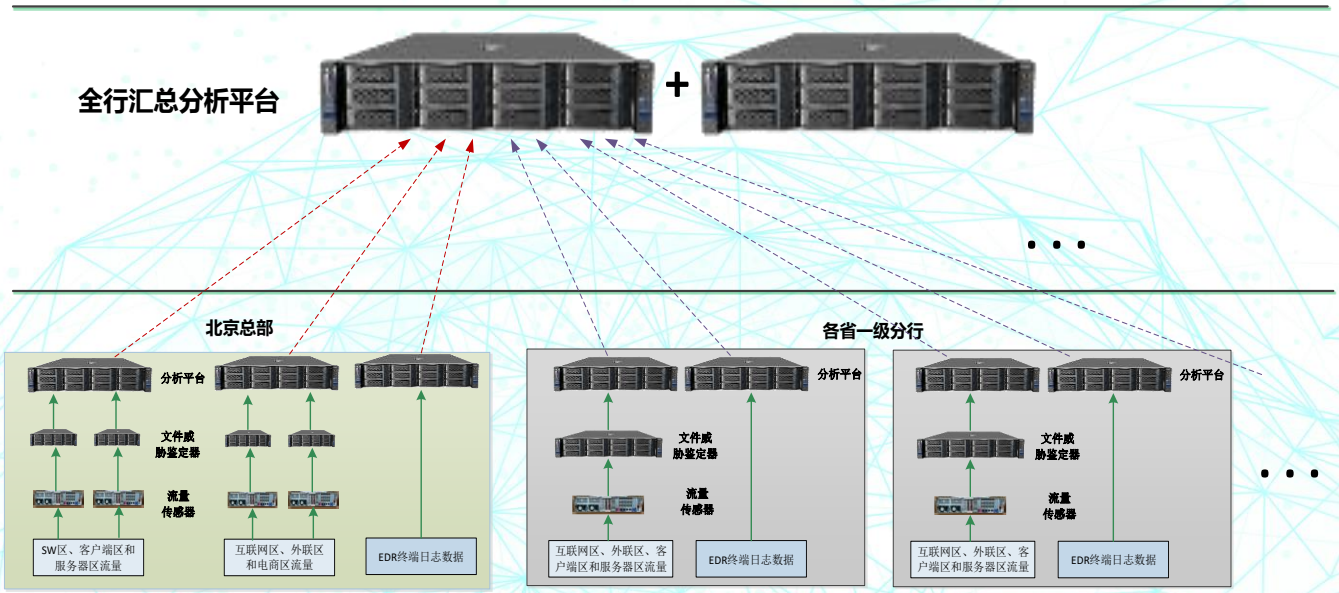
基于威胁情报的高位视角，提供新型的检测能力。
情报的精准、具备指导响应活动的上下文特性，保障了事件可以被及时处置。

对出局流量进行检测，及时发现内部被APT团伙、木马、蠕虫控制的主机

对业务服务器访问日志检测，主动发现异常IP访问，如：资产漏洞探测、爆库、自动化攻击等

检测流量中文件传输，以及主机上进程启动等信息，发现恶意文件，并进行攻击链分析

实例：威胁情报应用于某国有银行未知威胁检测系统



现状与挑战：

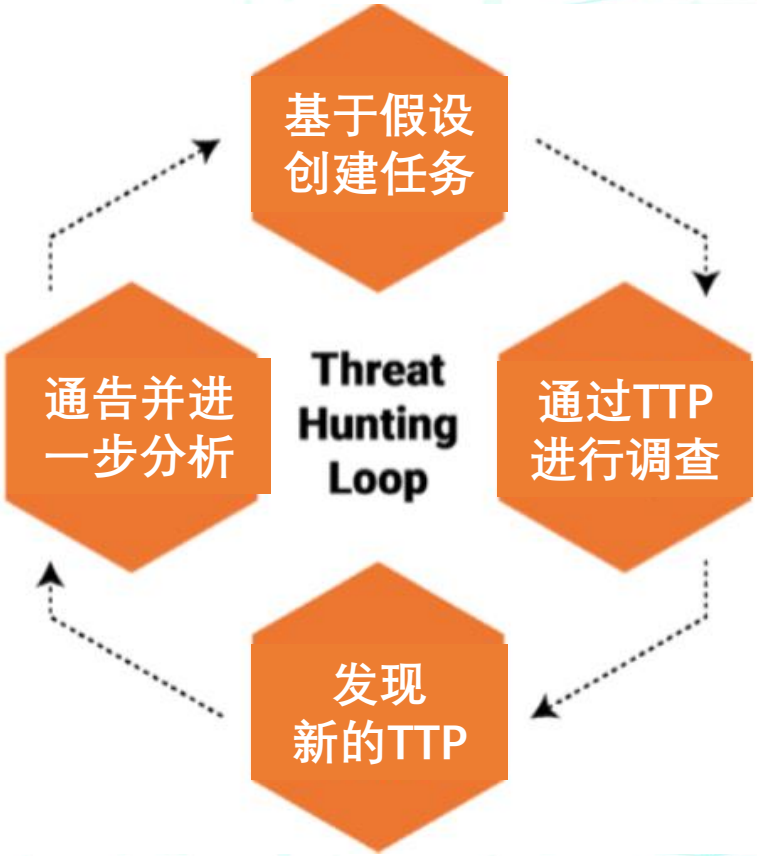
- 已经通过部署专业的防火墙、IPS、防病毒软件、终端安全软件等安全防护手段，能够针对主流威胁实现防护。
- 基于特征检测的传统安全防御手段只能识别已知威胁，以APT为代表的高级威胁使得传统的“依靠特征检测的方法”失效

实现了更敏捷的未知威胁检测能力

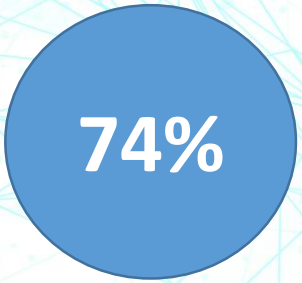
- 以威胁情报形式打通攻击定位、溯源与阻断多个工作环节，帮助建行从源头上解决安全问题；
- 增强了终端对于威胁事件的深度可见性，更敏锐的去检测到高级威胁，并提升的事件响应的能力；
- 通过基于大数据挖掘分析的恶意代码智能检测技术，提升了检测恶意代码的能力。

场景2：威胁情报是安全狩猎的基础

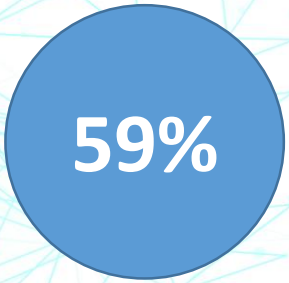
安全狩猎的前提是基于特定攻击者的技战术手法（作战情报，TTP）提出假设，并通过数据分析调查验证假设，成功的狩猎会发现新的TTP和之前未关注的攻击面。



发现之前未检测到的威胁



减少攻击面

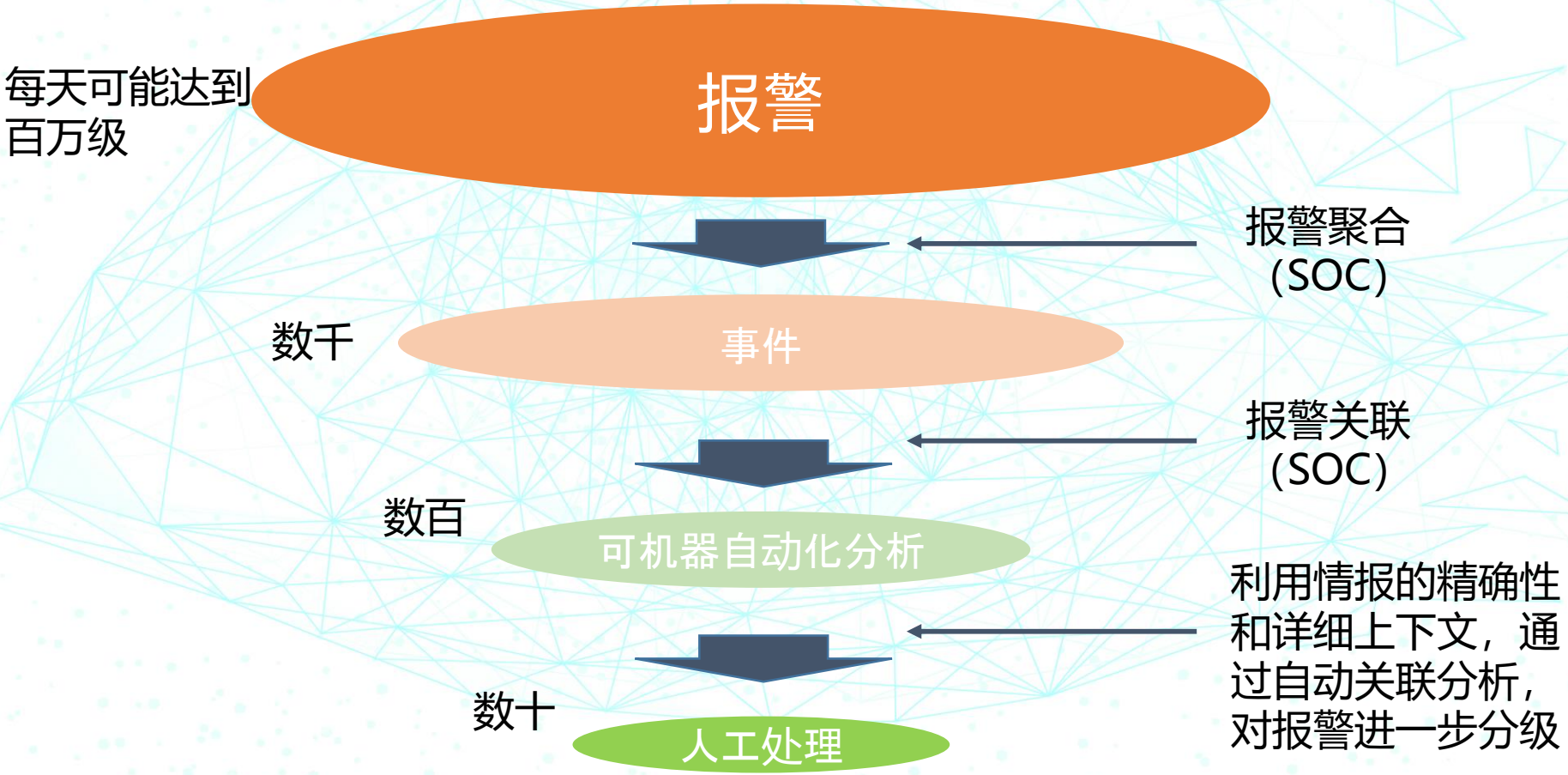


提升响应的速度和精度

来源: “Threat Hunting: Open Season on the Adversary,” Robert M. Lee, SANS Institute, 2016

场景3：威胁情报为报警分析带来了革命性变化

安全运营中关键问题是报警量过大，无法及时处置关键事件；SOC基于本地数据，无法获取威胁类型及攻击者意图等信息，威胁情报催生的新产品解决最终解决了问题



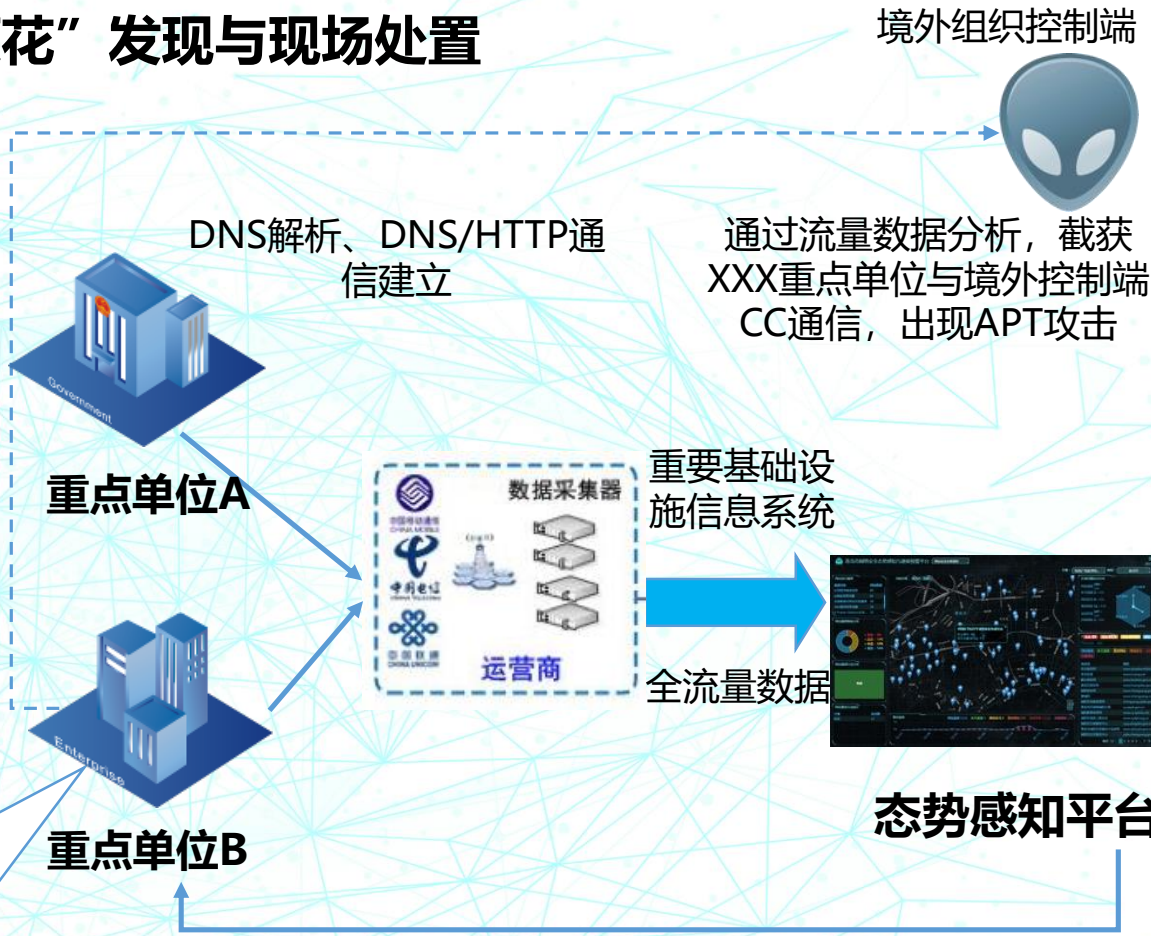
场景4：利用威胁情报进行事件响应

事件响应过程中，利用战术情报IOC，快速判定攻击影响面，并利用攻击者技战术特点（TTP），进行攻击链回溯分析。

实例：事件响应专业工具利用威胁情报做现场处置

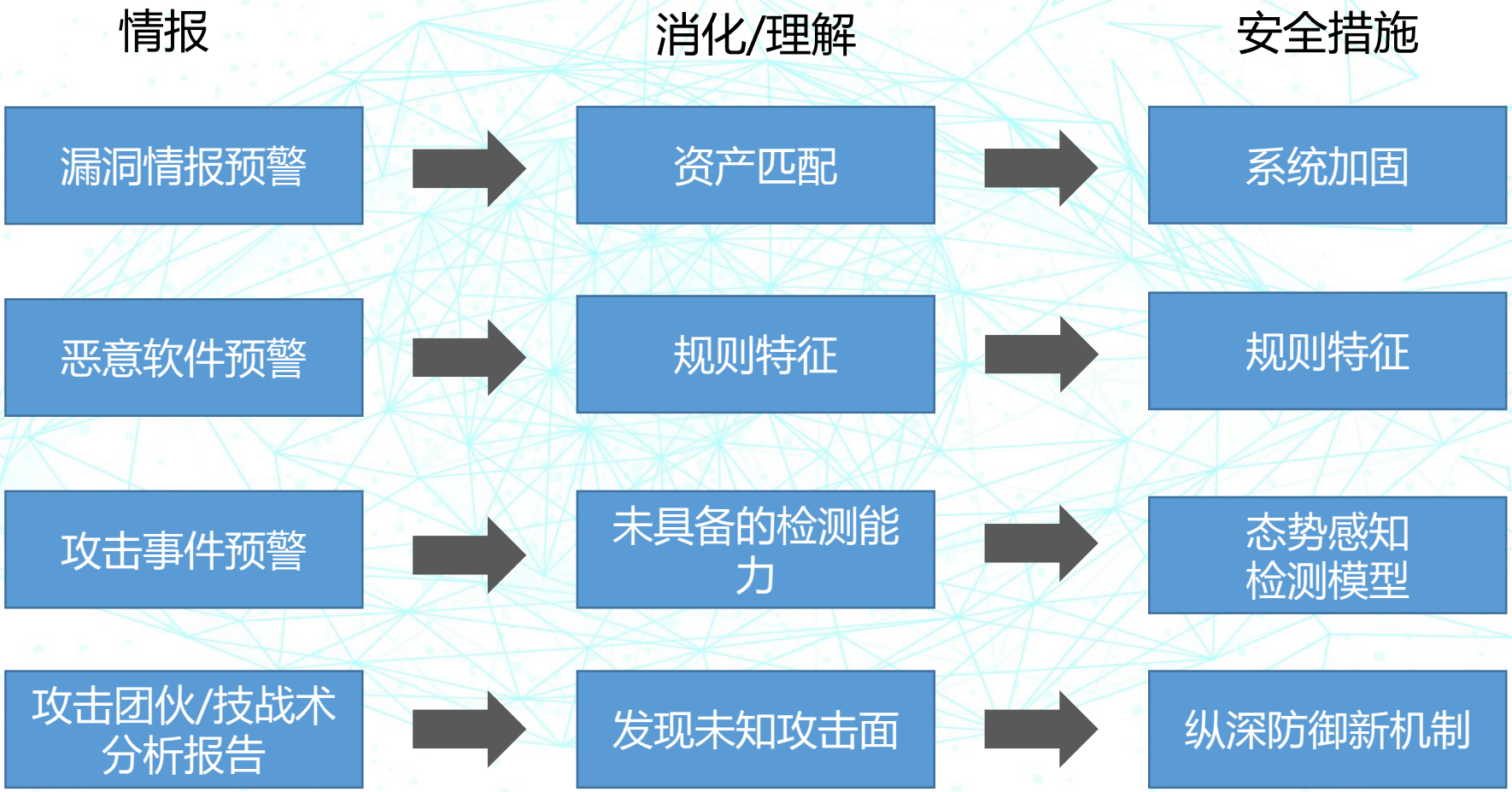
XX市XXX能源央企的“海莲花”发现与现场处置

- 发现“海莲花” 及“摩柯草” APT攻击；APT攻击有内网横向移动；
- 涉及众多的终端，及2台服务器，已被定位。



场景5：基于情报进一步完善防御体系

利用情报机制，可以进一步完善积极防御、纵深防御乃至基础架构安全



从IOC转化成为监测特征，从TTP转化成为态势感知的心智模型，从漏洞情报转化成为资产匹配筛选模板

态势感知消化威胁情报后在积极防御、纵深防御乃至基础结构安全发挥作用

从覆盖全环境/情报发现者环境的威胁情报，做减法匹配到实际的具体信息化环境（资产、配置、拓扑等）

威胁情报的真正应用是通过积极防御中的态势感知，作用于纵深防御和基础结构安全。

关键点3：威胁情报能力构建，需要从生态开始

从生产高质量威胁情报，到使用威胁情报完善安全体系，充满各种挑战，难以依赖单方面的力量，需要构建完整的生态。

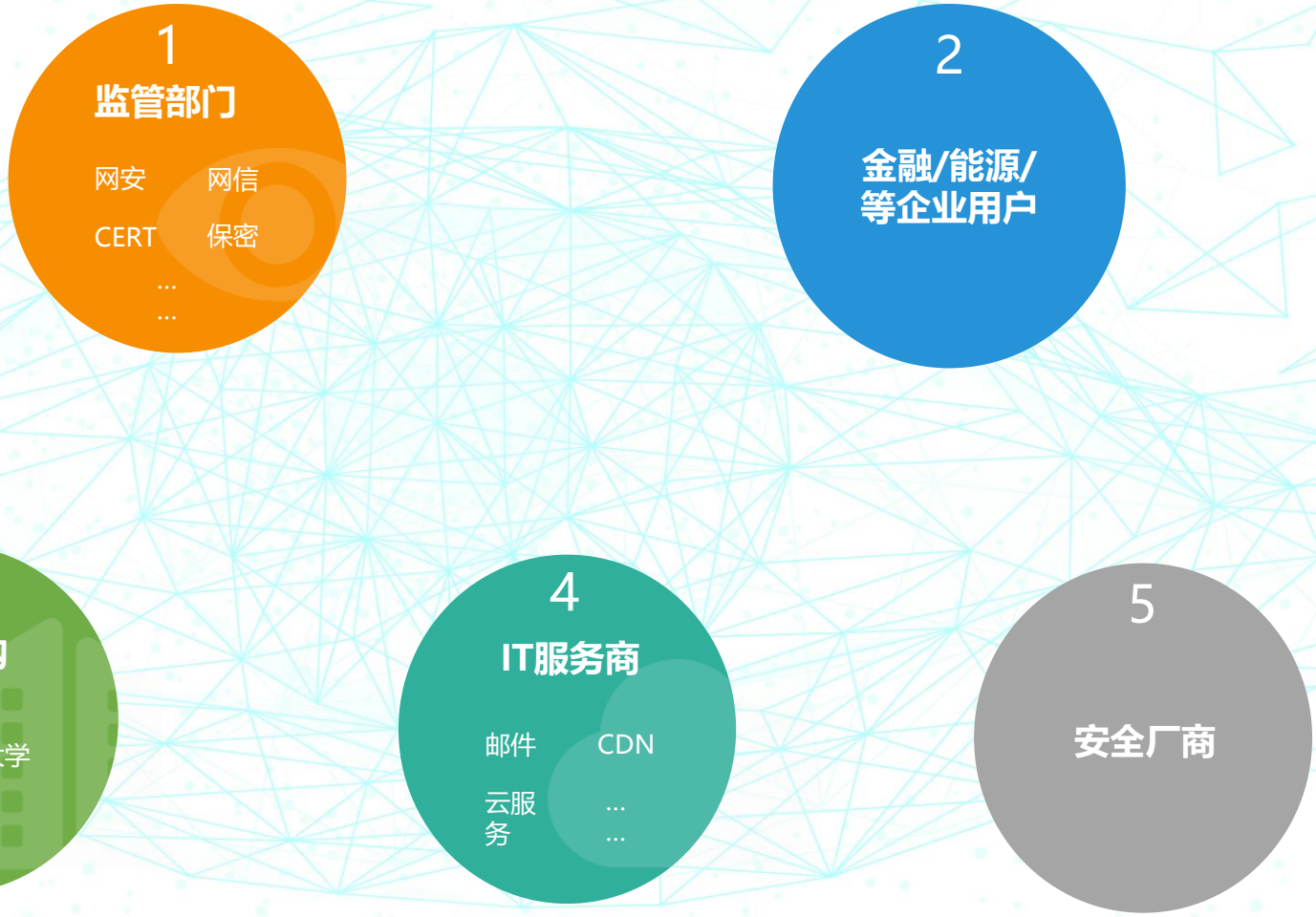
1. 任何厂商都难以提供完整覆盖面的威胁情报（不同行业、地域，不同类型的威胁情报），情报生产需要形成生态（安全厂商、行业企业、IT服务商）；

2. 重大事件预警，需要借助监管部门力量，才能推动整体上的快速响应（监管部门、安全厂商、行业企业）；

3. 预警情报的消化/理解到形成安全措施，需要多种安全能力：产品能力（规则、模型）、事件响应能力（加固）、解决方案能力（防御新机制），用户和厂商之间需要建立生态；

4. 安全研究机构，需要利用生态获得安全大数据、攻击者的技战术手法等信息，研究新的安全技术或检测模型。（研究机构、行业企业、安全厂商、IT服务商、监管部门）。

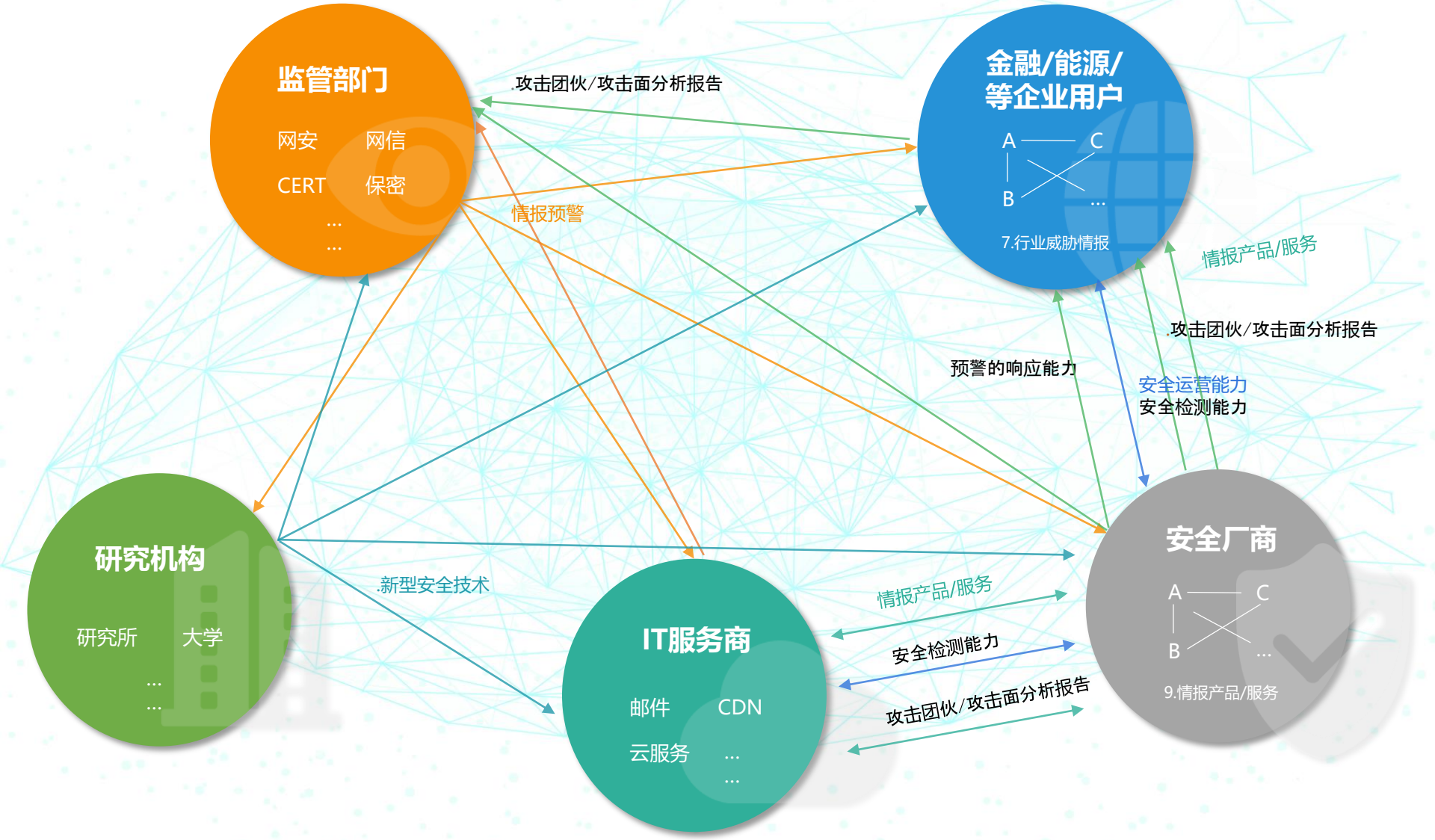
生态建设中的5个关键角色



生态建设中的8个关键产出物

1. 覆盖完整的威胁情报（包括行业化威胁情报）
2. 情报预警（漏洞、恶意软件、攻击事件）
3. 新型情报产品或服务能力
4. 攻击团伙/攻击面分析报告
5. 基于情报的安全运营能力（分析、响应）
6. 基于情报的安全检测能力
7. 基于情报预警的响应能力（加固、新规则、新特征、新模型）
8. 新型安全技术

一个完整的威胁情报生态模型



实例：360威胁情报中心生态赋能实践

帮助更多“生产者”生产威胁情报

帮助“消费者”更好地利用威胁情报

更多生产威胁情报

1 安全厂商

- 开放云端ALPHA情报分析平台（威胁关联分析、深度文件分析）；
- 非商业用途，限量免费使用；

2 行业用户

- 行业威胁情报生产方案；
- 情报分析培训/服务；

3 IT服务商

- 协同、合作特定领域的威胁分析报告

更好地利用威胁情报

1 安全厂商构建产品和服务

- 开放情报API供其在产品、服务中调用：失陷检测、IP情报、文件信誉；
- 开放本地化TIP API接口，协同构建用户侧解决方案；

2 研究机构

- 安全技术研究，协商免费提供需要的数据及情报

TIXA Threat Intelligence eXchange Alliance
威 胁 情 报 交 换 联 盟

威胁情报交换联盟

2017年，由ISC互联网安全大会发起成立的一个旨在推动威胁数据交换共享的联盟组织，目前已经有360威胁情报中心、蓝盾、Coremail、天际友盟等多家信息化和安全组织加盟，联盟成立2年多，进行了多次的情报共享和专项安全报告合作。联盟欢迎更多机构加入，共同推动威胁情报生态建设。

TIXA Threat Intelligence eXchange Alliance
威 胁 情 报 交 换 联 盟

协同安全能力 共建安全生态

谢谢！

360威胁情报中心