TianJi Partners

从信息到情报，从溯源到协同

北京天际友盟信息技术有限公司　谢　涛

什么才是威胁情报?

What can be called Threat Intelligence?

TianJi Partners

“威胁情报是基于证据的知识，包括场景、机制、指标、含义和可操作的建议。这些知识是关于现存的、或者是即将出现的针对资产的威胁或危险的，可为主体响应相关威胁或危险提供决策信息。”

----Gartner，2013年。

关于威胁情报，你说的和我说的是同一个吗？

什么才是威胁情报?

What can be called Threat Intelligence?

TianJi Partners

对抗产生情报需求

对威胁的具现化

威胁情报的时间窗口

威胁情报的知识属性

关注威胁，即“知彼”

什么才是威胁情报?

What can be called Threat Intelligence?

决策维度：多维结合，最终判断，处置策略，需实际落地，容错率极低

情报维度：深度加工，准确性高，时效性强，与场景贴合，应用频次高

信息维度：基于数据，初步加工，准确性差，时敏性不高，多作为参考

数据维度：原始数据，未做加工，数据量大，利用难度大、应用频次低

如何运用威胁情报?

How to use Threat Intelligence?

TianJi Partners

在引入威胁情报之前，我们需要考虑以下几个问题：

- 多源、可信源、有效源？
- 外部情报还是内部情报？
- 实时情报还是历史情报（信息）？
- 机读情报、人读情报还是画像情报？
- 威胁情报、资产情报、漏洞情报还是事件情报？
- 情报怎么接入？给谁用？怎么用？

如何运用威胁情报?

How to use Threat Intelligence?

TianJi Partners

应用模式一：基于信息关联检索的威胁溯源平台

- **实现方式**：由情报服务商在云或本地建立溯源知识库，将情报及其他基础信息（如Whois、PDNS、地理位置等）按指定格式入库，用户可对IP、域名、URL、文件Hash等进行快速查询，获取相关信息。
- **适用场景**：用户通过WAF、IDS、SOC等发现可疑威胁或事件后，借助这种溯源来辅助对威胁、事件的真实性、严重性的判断，并开展对威胁线索的扩展关联分析。
- **适用客户**：有WAF、IDS、SOC等检测和事件分析设备，安全人员有一定的分析能力，对应急响应要求较高，例如各大银行、电信运营商、互联网企业、大型央企等，或是第三方安全机构和科研院校。
- **使用方法**：数量少靠人工做界面查询，数量多靠接口做批量查询。
- **注意事项**：云SaaS模式需要考虑网络可达，本地化部署则需要考虑数据更新的问题；界面查询相比接口查询能获取更多的关联信息。

如何运用威胁情报?

How to use Threat Intelligence?

TianJi Partners

应用模式二：基于匹配机制的情报分析平台

- **实现方式**：由情报服务商在云或本地建立情报分析平台，用户将自己的DNS解析记录、设备告警、文件样本、资产信息等数据发至情报分析平台，在平台将情报与用户数据进行命中匹配，并反馈结果。
- **适用场景**：失陷主机检测（DNS解析记录、资产信息等）、安全事件响应（文件样本、设备告警）。
- **适用客户**：缺乏专业安全设备和分析人员，需要依赖外力来发现威胁，且能接受自身数据交给他人。例如部分小型互联网企业和传统中小型企业等。
- **使用方法**：可离线或在线上传数据，分析结果以界面或接口形式反馈。
- **注意事项**：对情报质量和数量要求较高，必然会存在漏报；功能与SOC、流量分析有重合；产品形态较重，性能要求高；仅能发现线索，无法形成分析和响应的闭环。

如何运用威胁情报?

How to use Threat Intelligence?

TianJi Partners

应用模式三：基于订阅分发机制的情报协同平台

- **实现方式**：由情报服务商在云或本地建立情报协同平台，以订阅方式将实时情报发送至NGFW、WAF、IDS、SOC、EDR、流量检测等安全设备（已具备情报模块），安全设备将情报按需入库，并根据自身功能进行基于情报的检测、分析和处置。
- **适用场景**：防护、检测、响应的各类安全场景，以及情报共享交换和企业内部安全通报等衍生场景。
- **适用客户**：主要基于情报服务商和设备厂商的合作，对用户要求不高。
- **使用方法**：以接口形式分发情报，设备将情报加入黑库或灰库进行检测和分析。
- **注意事项**：产品形态较轻，和其他安全产品功能上没有重叠；情报应用均由用户本地的安全设备自行完成，无需上传数据；设备需要升级以具备解析情报的能力，且需要考虑统一的情报标准。

如何运用威胁情报?

How to use Threat Intelligence?

TianJi Partners

➢ 联盟情况

国内首个威胁情报联盟，2015年10月成立，11家成员企业。

➢ 联盟宗旨

以安全威胁情报为核心，打造平等互惠的新生态圈模式，共谋共策，推进威胁情报的标准制定及应用推广。

➢ 合作理念

“联合”、“共享”、“协作”、“共赢”。

➢ 合作模式

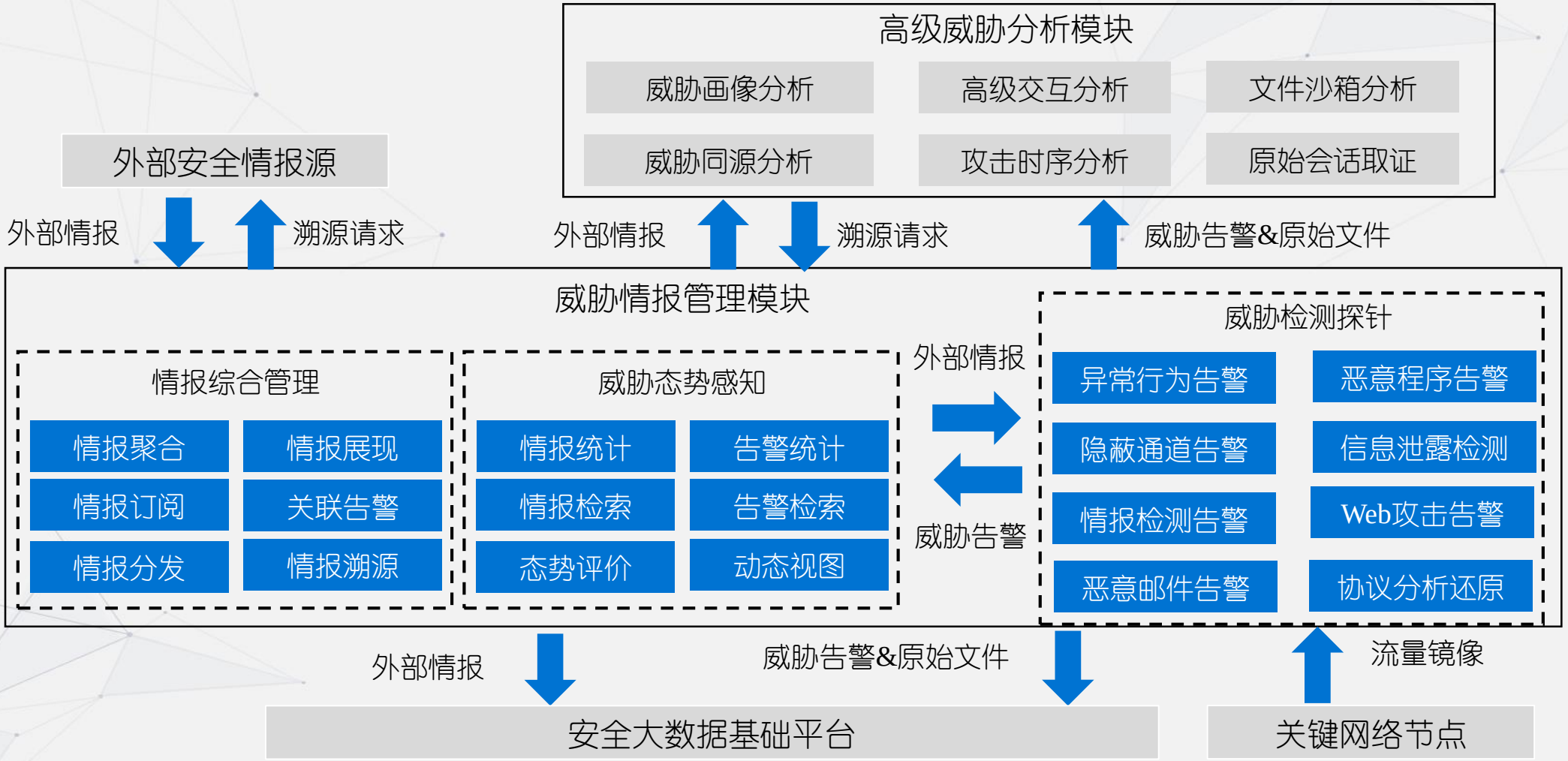
技术合作：关键基础设施共建，对内情报信息共享，对外产品联动协同。

服务合作：服务支持体系共建，服务人员集中培训，服务内容统一管理。

市场合作：解决方案整体打包，市场推广互通协作，客户资源信息共享。

如何运用威胁情报?

How to use Threat Intelligence?

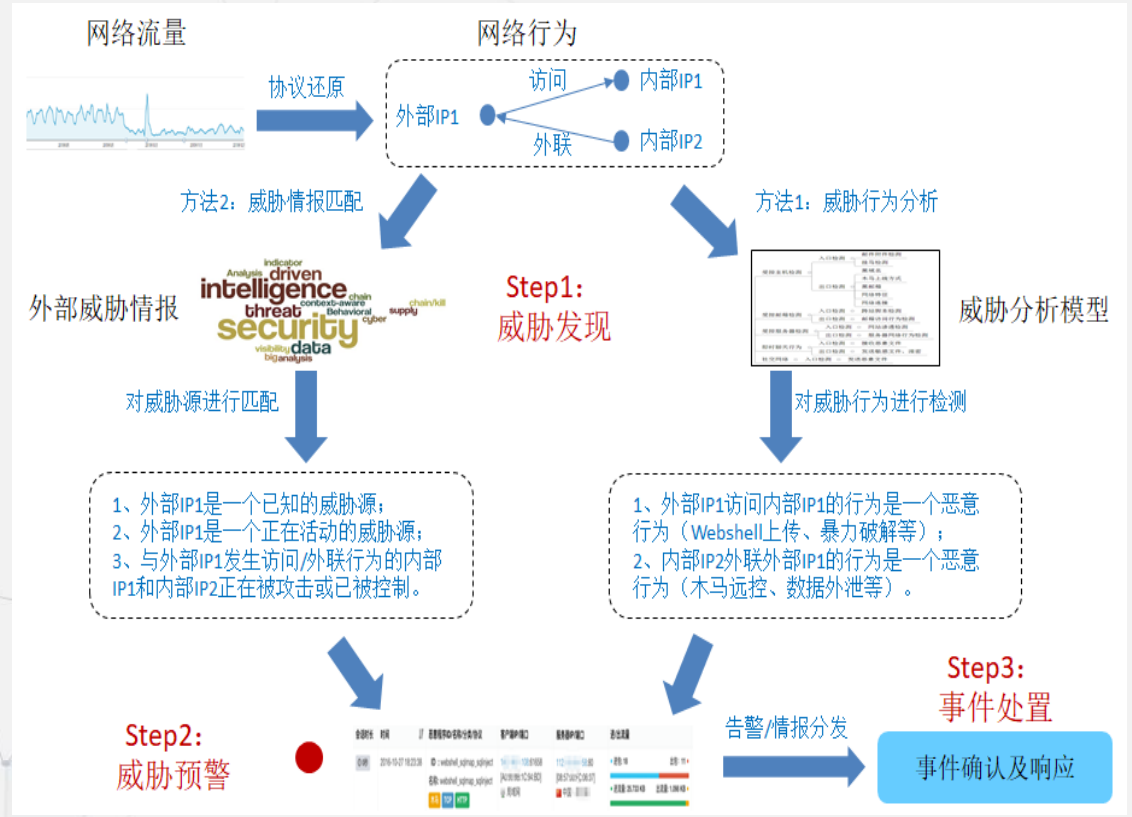


如何运用威胁情报?

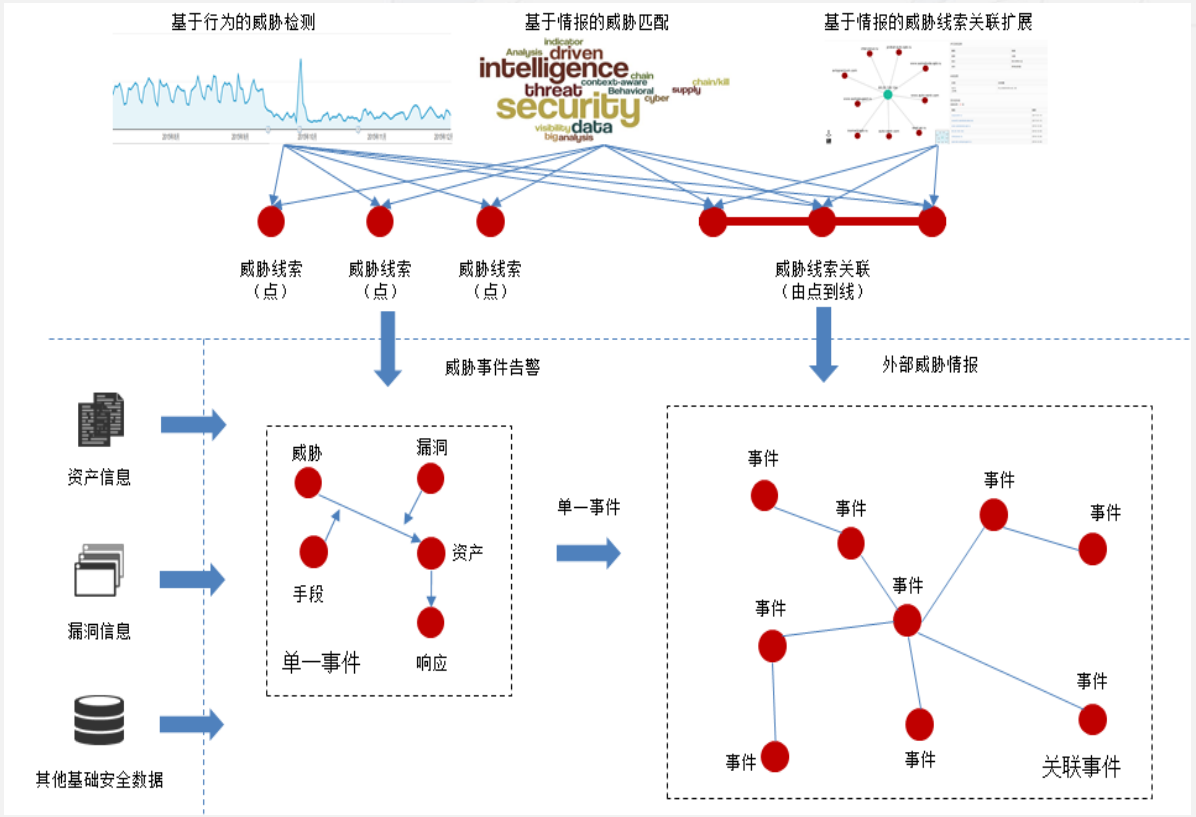
How to use Threat Intelligence?

TianJi Partners

基于情报协同的高级威胁检测



结合情报的事件关联分析



TianJi Partners

WE ARE JUST ON THE WAY

THANK YOU