网络空间威胁对抗与态势感知研讨会
暨 第六届安天网络安全冬训营

内部资料

下一代威胁检测引擎
——赋能威胁情报

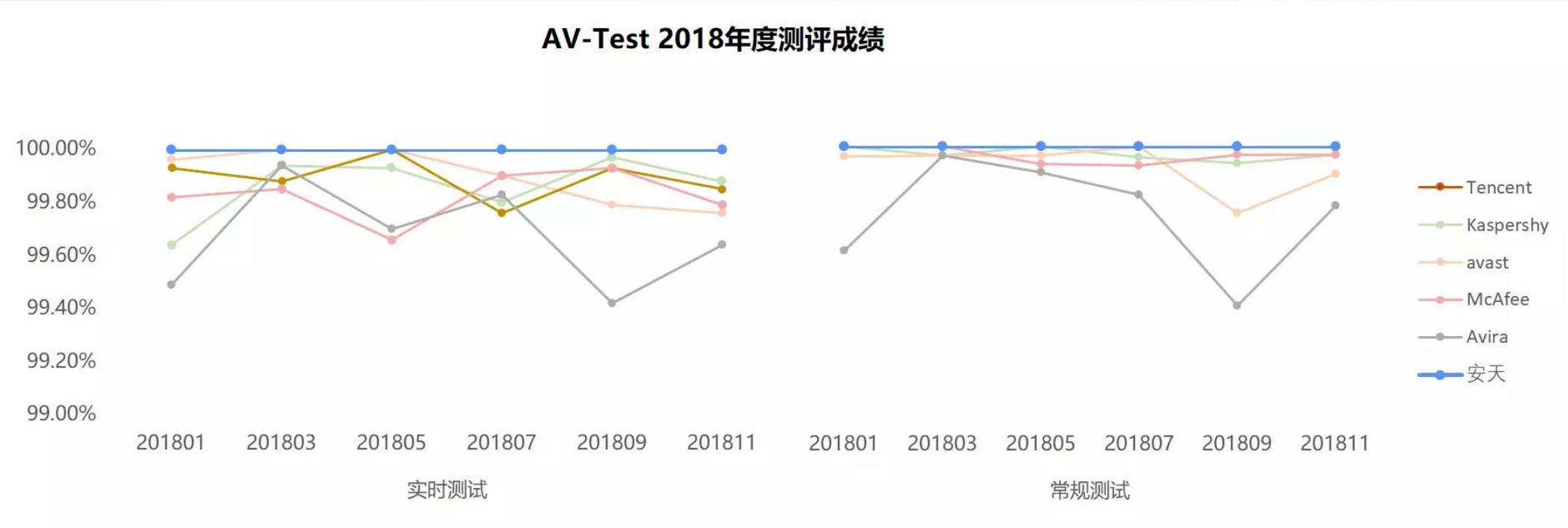
安天基础引擎研发部

战术型态势感知指控积极防御
协同响应猎杀威胁运行实战化

提纲

- 威胁检测引擎简介
- 安天下一代威胁检测引擎
- 赋能威胁情报

安天这一年在威胁检测引擎的取得一些成绩



安天这一年在威胁检测引擎的取得一些成绩

安天包揽国家应急中心网络安全引擎两项大赛第一名

探海获奖证书

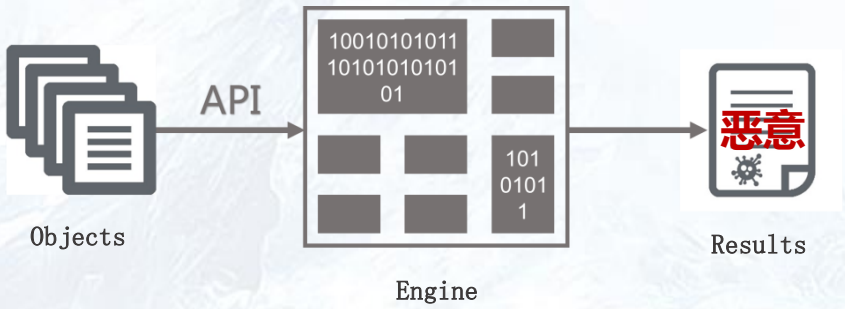
追影获奖证书

01 威胁检测引擎简介

什么是威胁检测引擎?

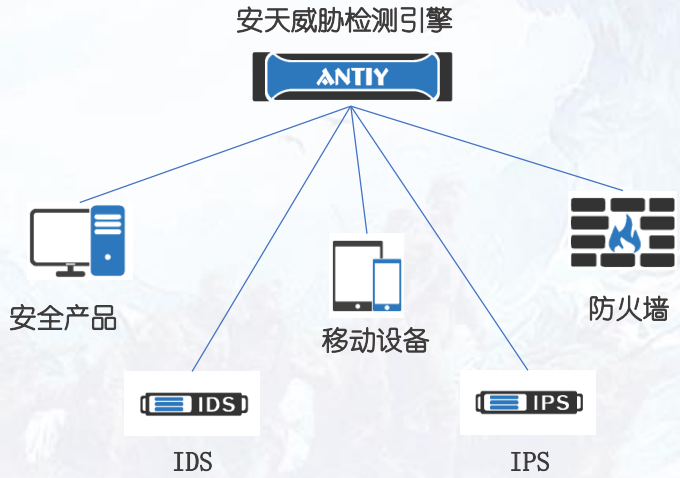
威胁检测引擎的定义:

一组依靠可维护规则的数据结构 通过接口调用能够对输入对象进行病毒检测处理的程序模块的统称。就像汽车的发动机是汽车的核心动力来源一样，威胁检测引擎为威胁检测产品提供着核心的鉴定能力，只要将待检测对象传入引擎，引擎即能输出对该对象的鉴定结果。



威胁检测引擎的应用:

威胁检测引擎不仅可以支持传统主机反病毒产品，还可以应用到移动设备、防火墙、UTM、网闸等各种安全产品和网络设备中。



安天AVLSDK 威胁检测引擎

AVL SDK可嵌入式反病毒引擎（简称AVL SDK）

由安天公司自研的反病毒引擎产品，提供全套的可调用API（应用编程接口），为网络安全产品扩展反病毒能力提供简单优质的解决方案。

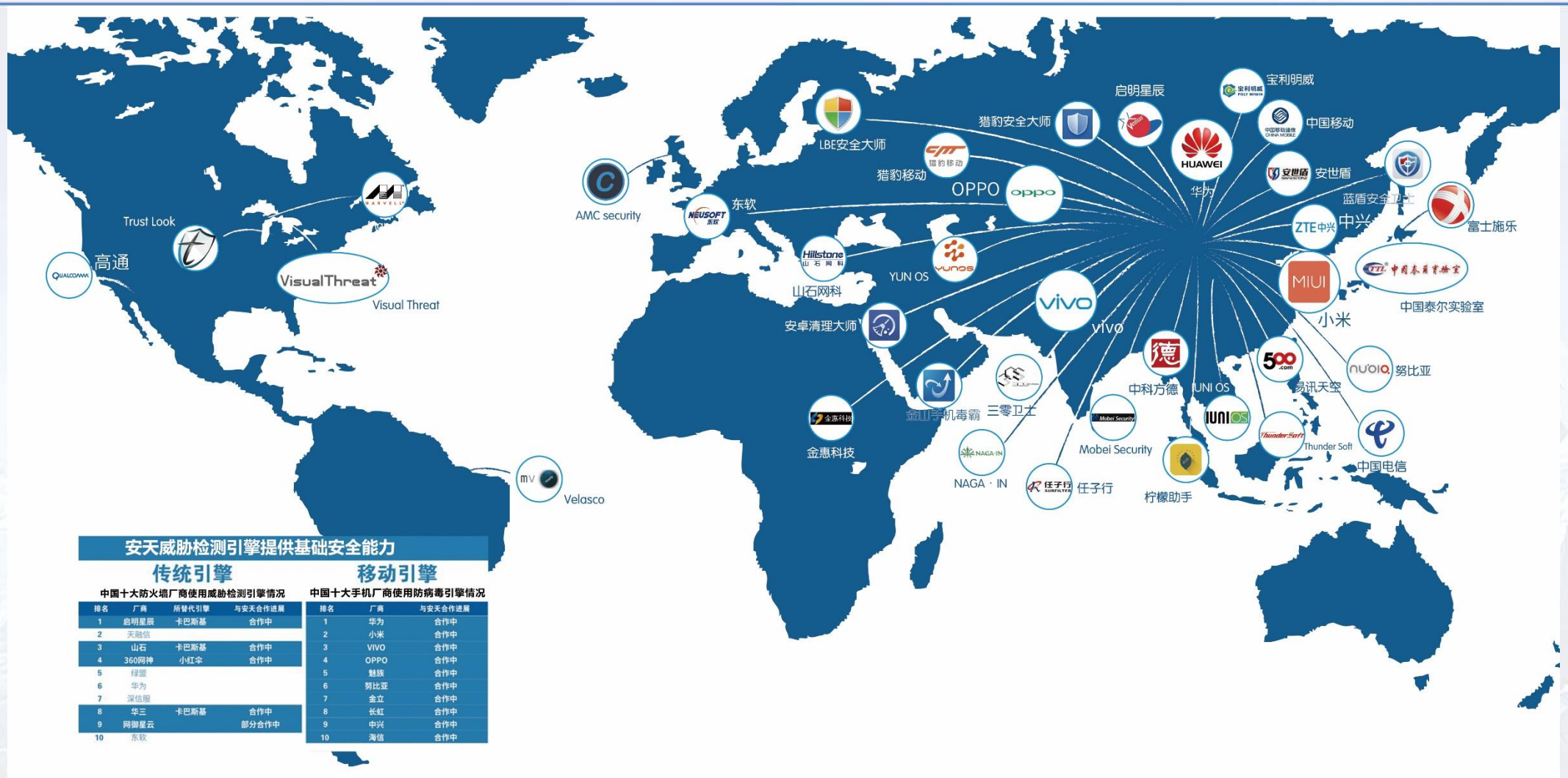
检测能力

- ✓ **检测病毒家族**
  可检测三万余家族，近一千万变种以及数以亿计的恶意代码
- ✓ **检测病毒类型**
  可检测蠕虫、病毒、木马、黑客工具、流氓软件、风险程序等多种类型
- ✓ **支持检测对象**
  可检测多种格式文件和信标（IP、DOMAIN、URL）

产品特性

- ✓ **全规则高速引擎**
  具有海量的病毒检测规则，且检测速度极快，约为其他引擎产品的2-5倍。
- ✓ **跨平台可移植性**
  支持POSIX标准，可应用于各类系统平台（如Windows、Linux、Android、以及国产操作系统等）、硬件平台（如Intel、Arm、X86、MIPS、嵌入式以及国产硬件平台等）中。
- ✓ **灵活版本定制化**
  用户可根据不同需求定制不同的引擎版本。
- ✓ **易于集成**
  对接口简单调用即可使产品具有反病毒能力。
- ✓ **检测方法简便**
  待测对象传给AVL引擎即可得到详细检测结论。

安天引擎合作伙伴



安天威胁检测引擎提供基础安全能力

传统引擎

中国十大防火墙厂商使用威胁检测引擎情况

排名	厂商	所替代引擎	与安天合作进展
1	启明星辰	卡巴斯基	合作中
2	天融信		
3	山石	卡巴斯基	合作中
4	360网神	小红伞	合作中
5	绿盟		
6	华为		
7	深信服		
8	华三	卡巴斯基	合作中
9	网御星云		部分合作中
10	东软		

移动引擎

中国十大手机厂商使用防病毒引擎情况

排名	厂商	与安天合作进展
1	华为	合作中
2	小米	合作中
3	VIVO	合作中
4	OPPO	合作中
5	魅族	合作中
6	努比亚	合作中
7	金立	合作中
8	长虹	合作中
9	中兴	合作中
10	海信	合作中

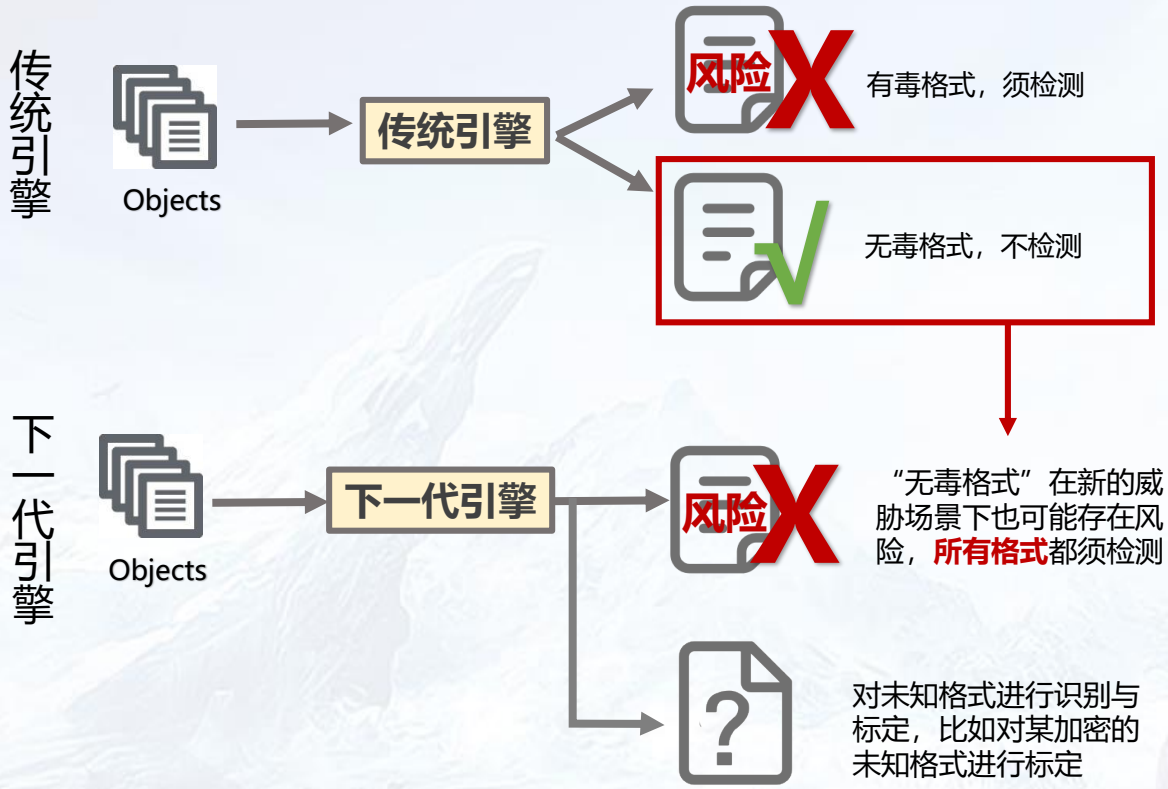
02 安天下一代威胁检测引擎

更深入的识别与解析
更多样的输入输出对象
更广泛的应用场景

传统威胁检测引擎 vs 下一代威胁检测引擎

	传统威胁检测引擎	下一代威胁检测引擎
工作模式	以自身规则检测载荷的安全与否，对部分文件提供授信能力	立足于攻击方可以获得防御方引擎并可以绕过引擎的假想下来设计
输入对象	单一输入对象	多种输入对象 (网络层次、本地层次)
工作能力	鉴定器	识别器、拆解器、鉴定器、分析器

具有更深入的识别解析能力



✓ 格式识别能力

可识别文件格式：268类，342余种（包含小版本）

- 可执行文件 42
- 包裹 43
- 文档 28
- 媒体文件 36
- 软件关联格式 133
- 脚本 9
- 文本格式 21
- 其它格式 7
- 图片文件 23

✓ 编译器与壳识别能力

- 1. 可识别编译器：>500 （包含小版本）
- 2. 可识别壳： >3000（包含小版本）

具有更深入的识别解析能力

✓ 面临挑战

- **传统引擎**在格式解析上已初步具备相应能力，但主要为内部检测能力服务的，不具备输出能力，不能为威胁情报和关联检索提供基础要素。

✓ 应对挑战

- **下一代引擎**对格式解析能力做了几点强化：
- 1、扩大了需要解析的格式范围
- 2、增加了重点格式的解析深度
- 3、传统威胁检测引擎中的格式解析是服务与内部流程的，不能为威胁情报和关联检索提供原料，下一代检测引擎可以把这种能力从内部转化为对外部产品的输出

✓ 格式解析能力

- 文档类：DOC，XLS，PPT，PDF，RTF …
- 媒体文件：SWF 等
- 可执行文件：Microsoft.PE，Microsoft.MSIL，Linux.ELF 等
- 包裹：压缩包，自解压包，安装包等共计40类

具有更深入的识别解析能力

✓ OFFICE

- 文档说明：标题，主题，标记，类别，备注…
- 文档来源：作者名，公司，版本号，管理者，创建内容时间…
- 文档内容：夹带文件，宏代码…

✓ BinExecute/Microsoft.PE

a）静态向量

- 行为标签（共162项）：
  对抗，传播，控制
  隐藏，窃取，欺骗
  …
- API（51类）：
  模块相关，网络相关
  文件相关，进程相关
  窗口相关，内存相关

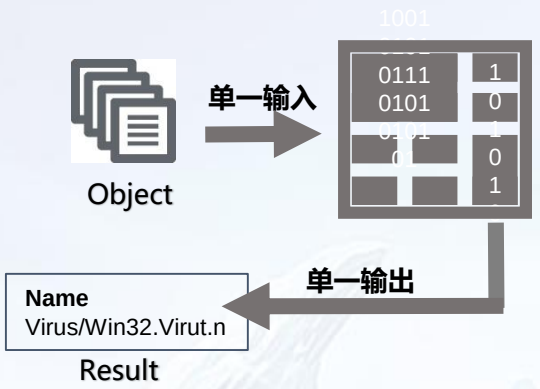
b）远控静态配置解密

- IP，URL
- MAIL，DOMAIN

b）数字签名

- 证书信息：颁发者，使用者，有效期，算法 …
- 签名信息：证书链，签名人名字，签名时间
- 判定标签：伪造，吊销，过期，证书不完整

具有更多样的输入输出对象

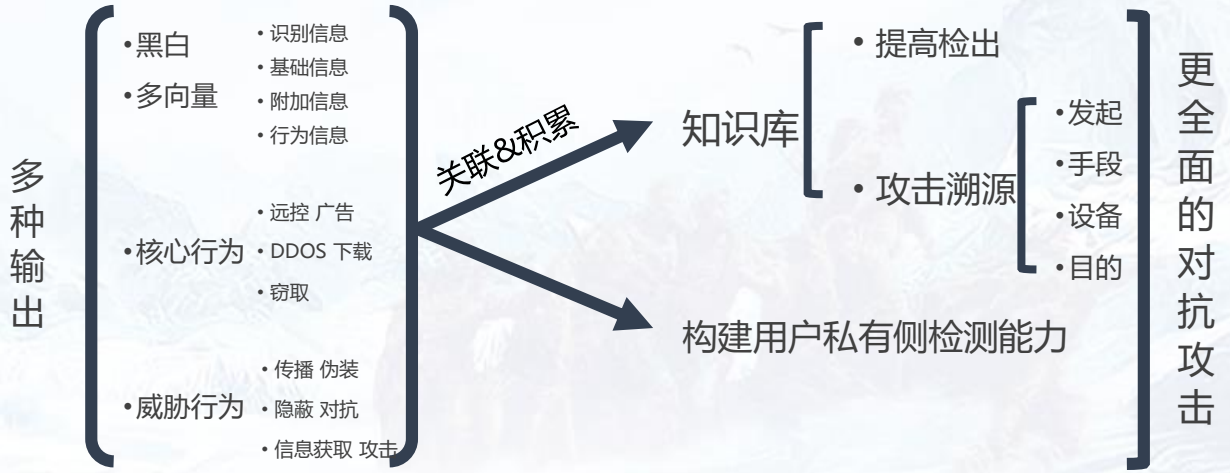


✓ **传统引擎**

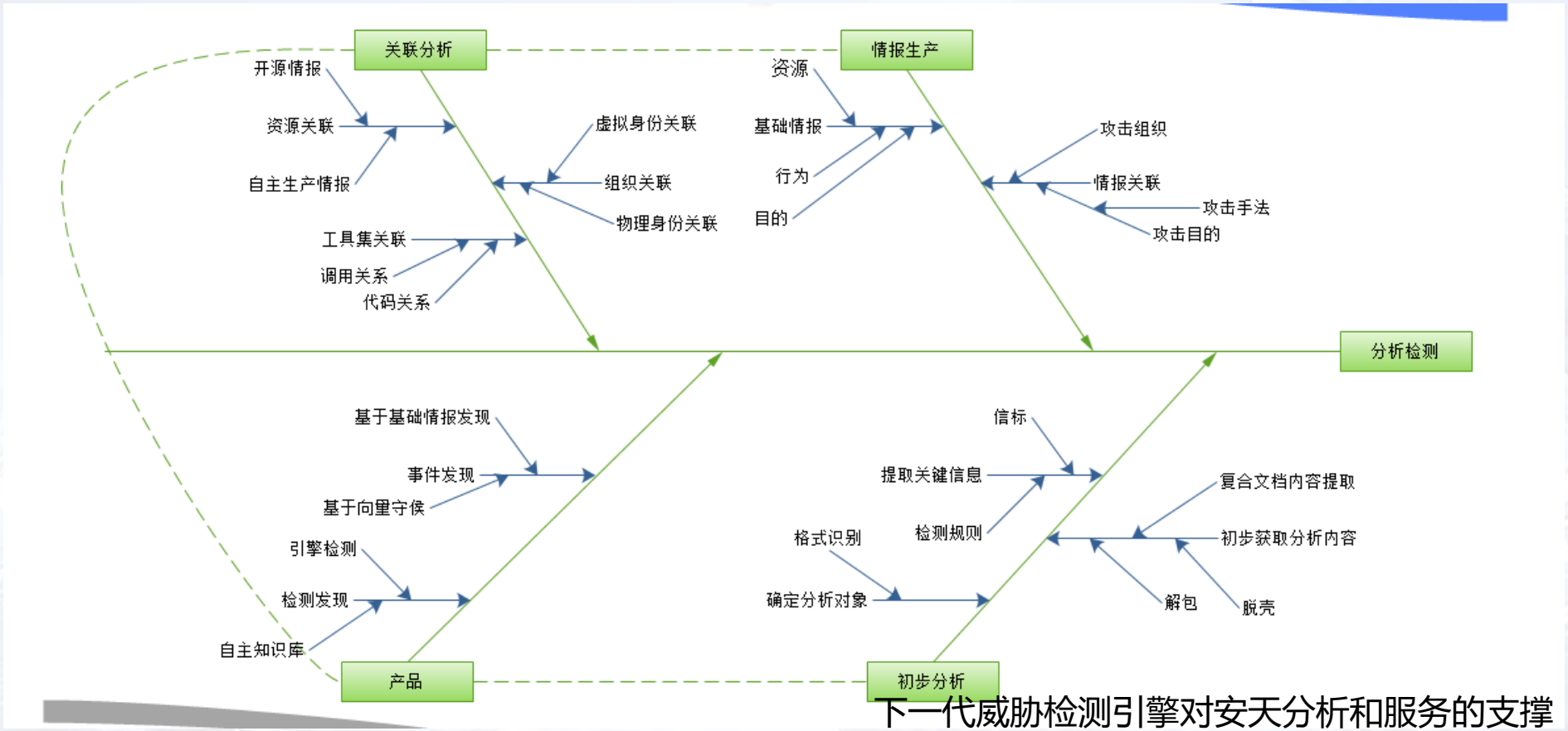
主要是以单一对象为输入，以单一结果为输出。而随着威胁的进一步演进和泛化，威胁检测已不能仅仅停留在对单一对象进行鉴定上。

✓ **下一代威胁检测引擎**

多种输入对象，多种输出结果。威胁检测多样化。



具有更广泛的应用场景



下一代威胁检测引擎对安天分析和服务的支撑

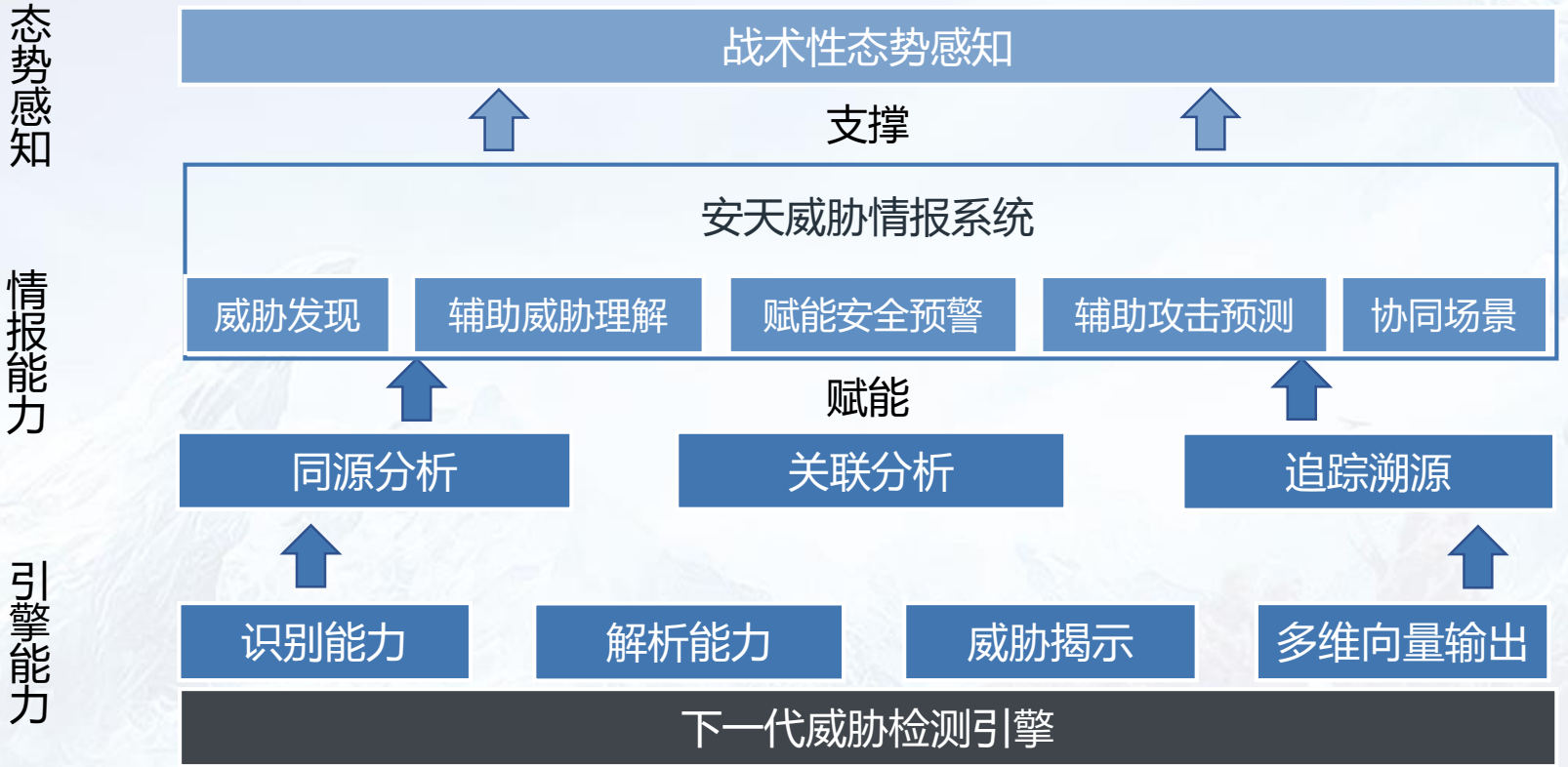
3 赋能威胁情报

情报采集

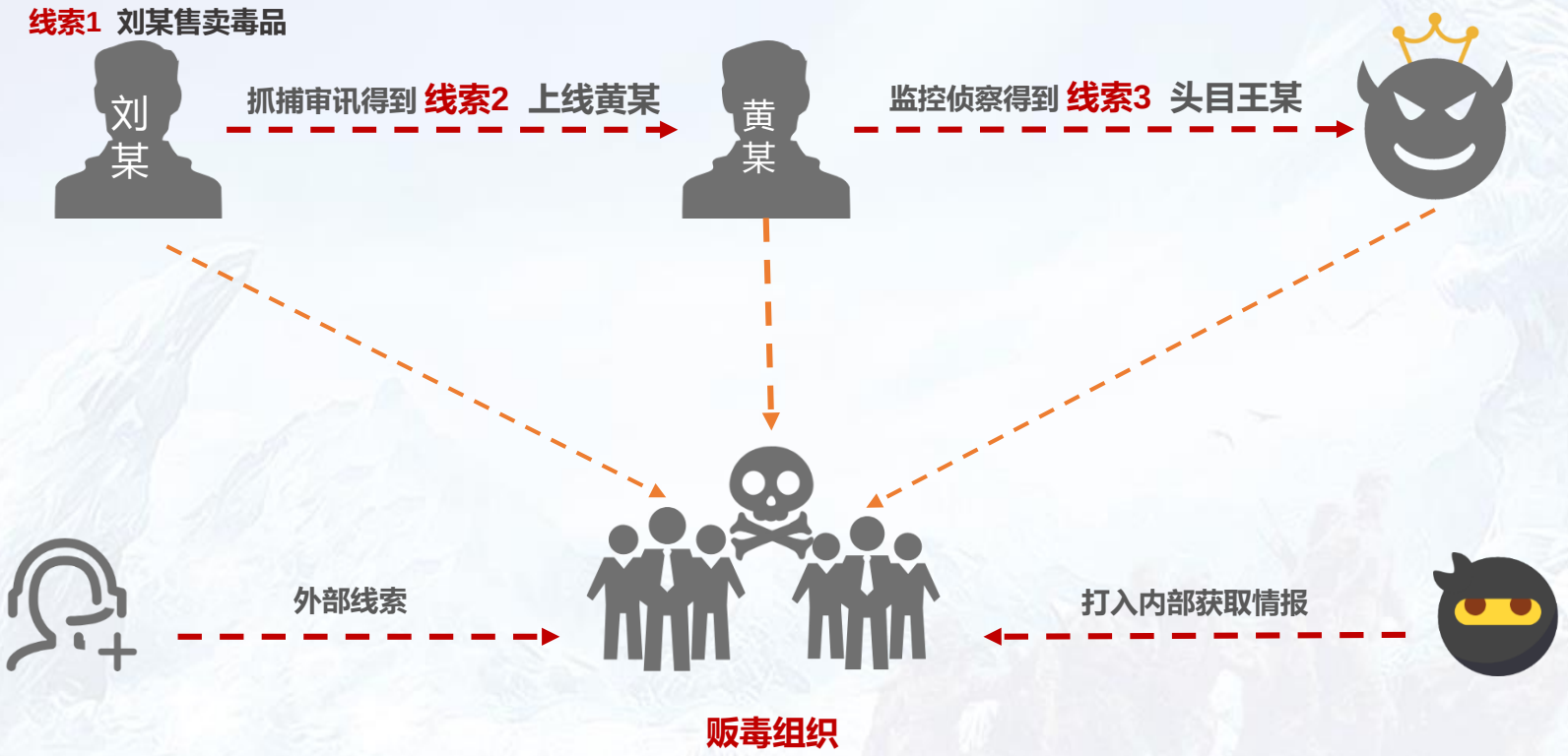
情报生产

情报应用

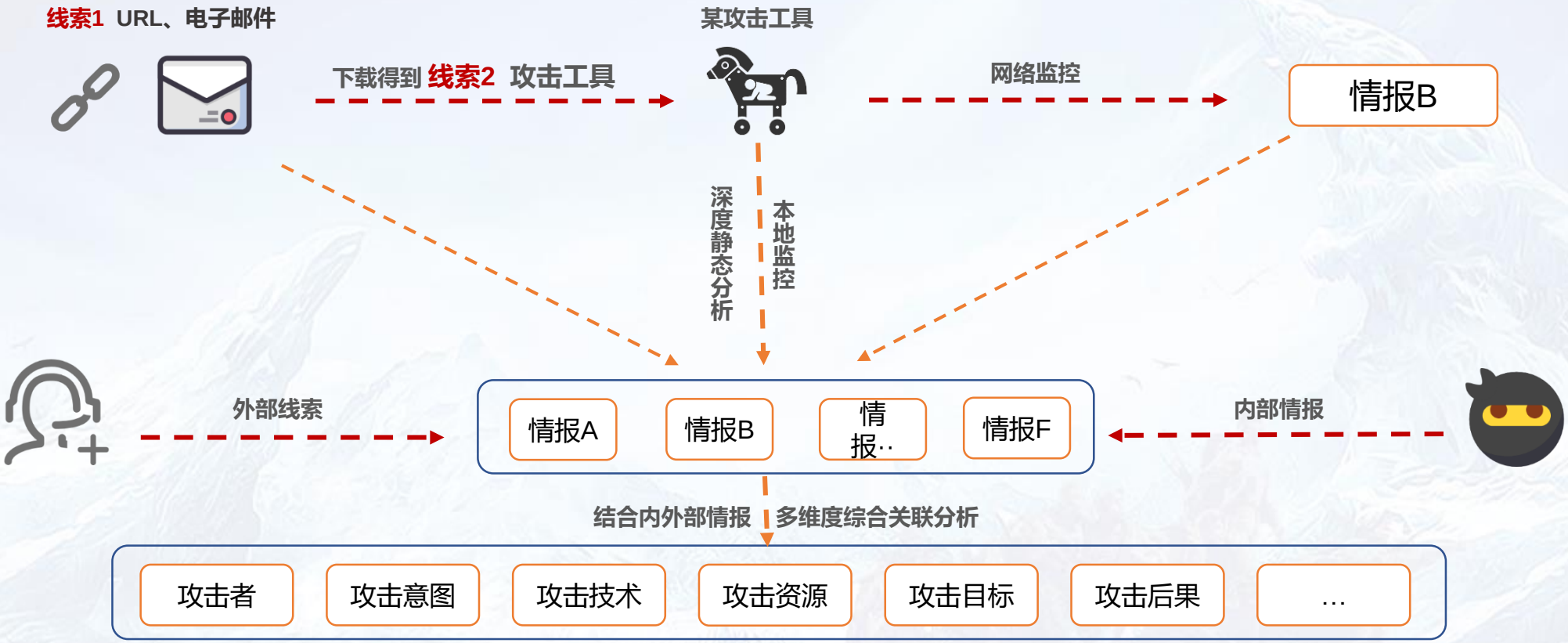
下一代威胁检测引擎赋能威胁情报、支撑态势感知系统



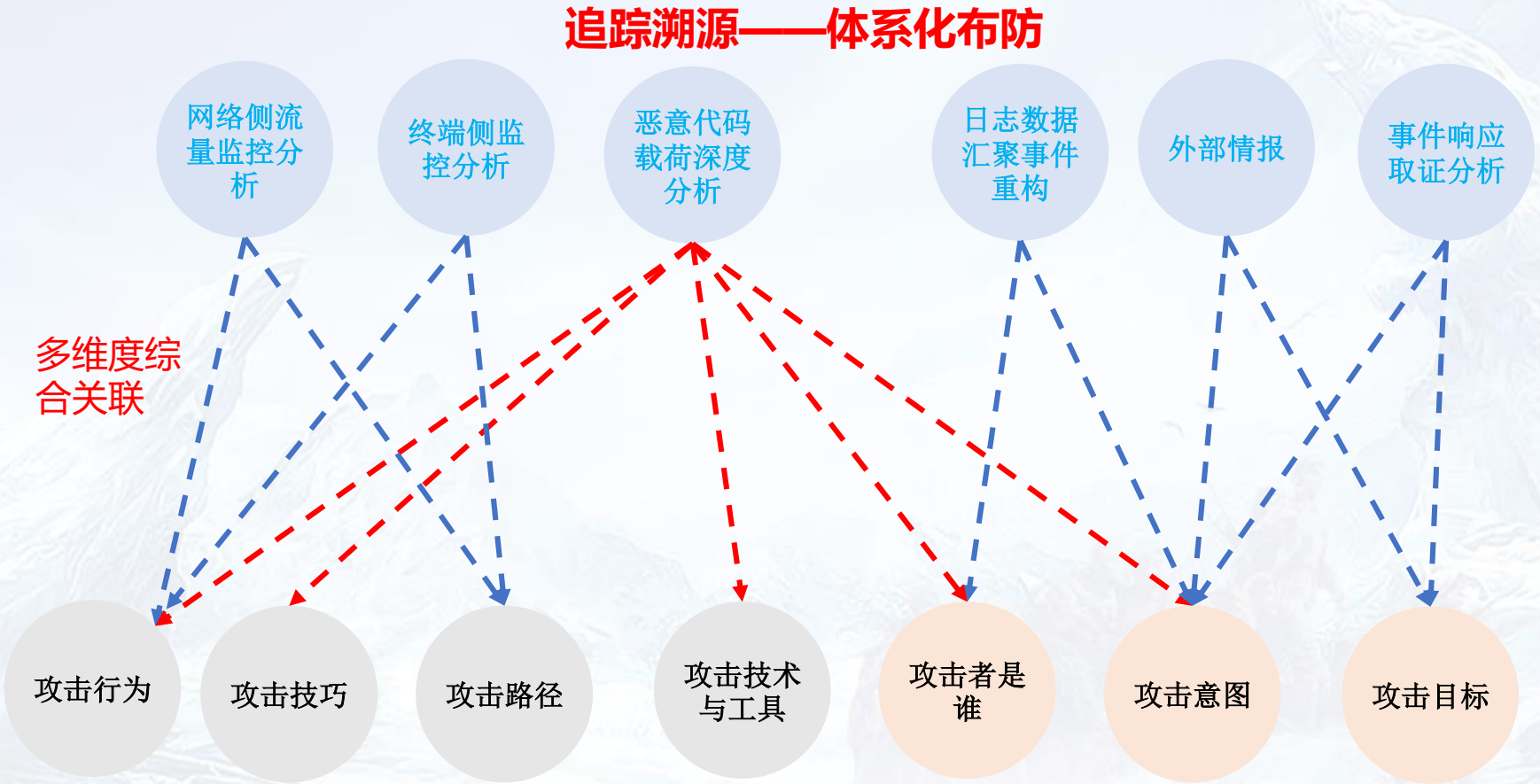
威胁情报在现实破案中的应用



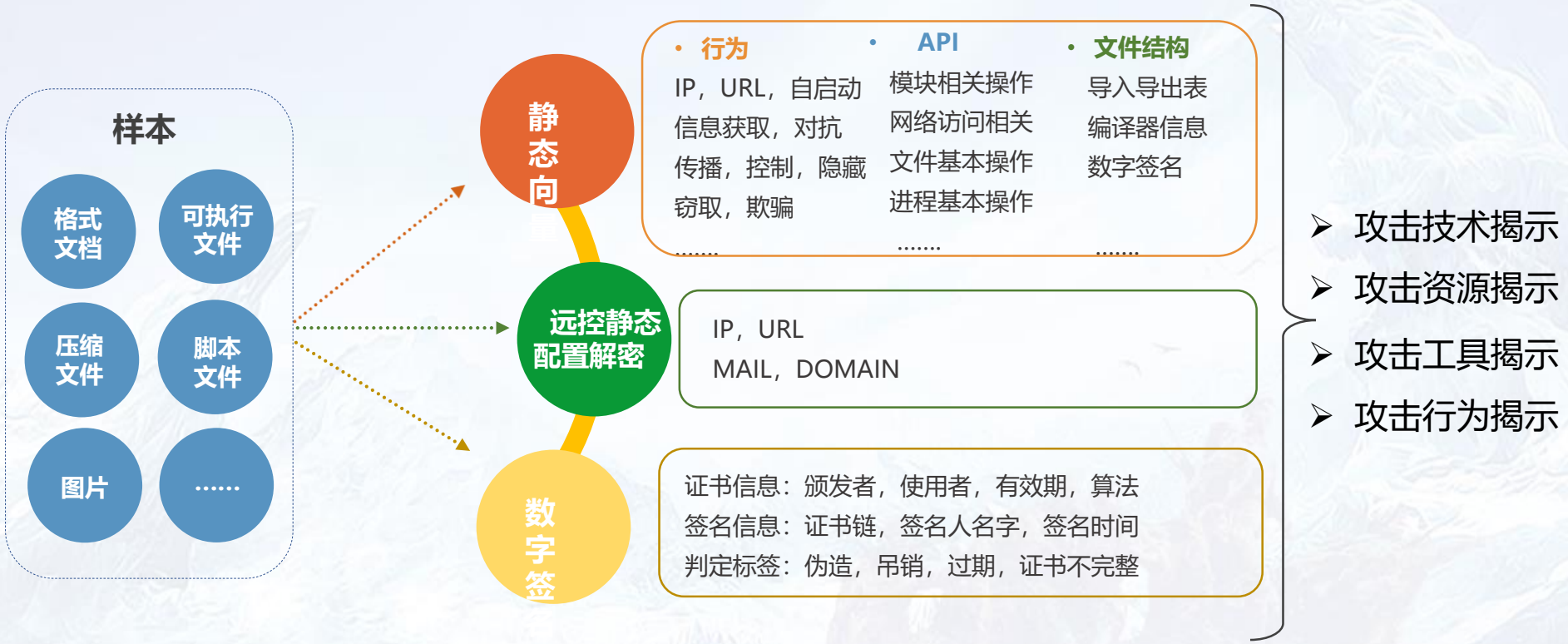
威胁情报在网络溯源中的应用



威胁情报在网络上的追踪溯源



应用于情报采集与生产


样本
格式文档
可执行文件
压缩文件
脚本文件
图片
……
静态向
远控静态配置解密
数字签
• 行为
IP，URL，自启动
信息获取，对抗
传播，控制，隐藏
窃取，欺骗
……
• API
模块相关操作
网络访问相关
文件基本操作
进程基本操作
……
• 文件结构
导入导出表
编译器信息
数字签名
……
IP，URL
MAIL，DOMAIN
证书信息：颁发者，使用者，有效期，算法
签名信息：证书链，签名人名字，签名时间
判定标签：伪造，吊销，过期，证书不完整
攻击技术揭示
攻击资源揭示
攻击工具揭示
攻击行为揭示

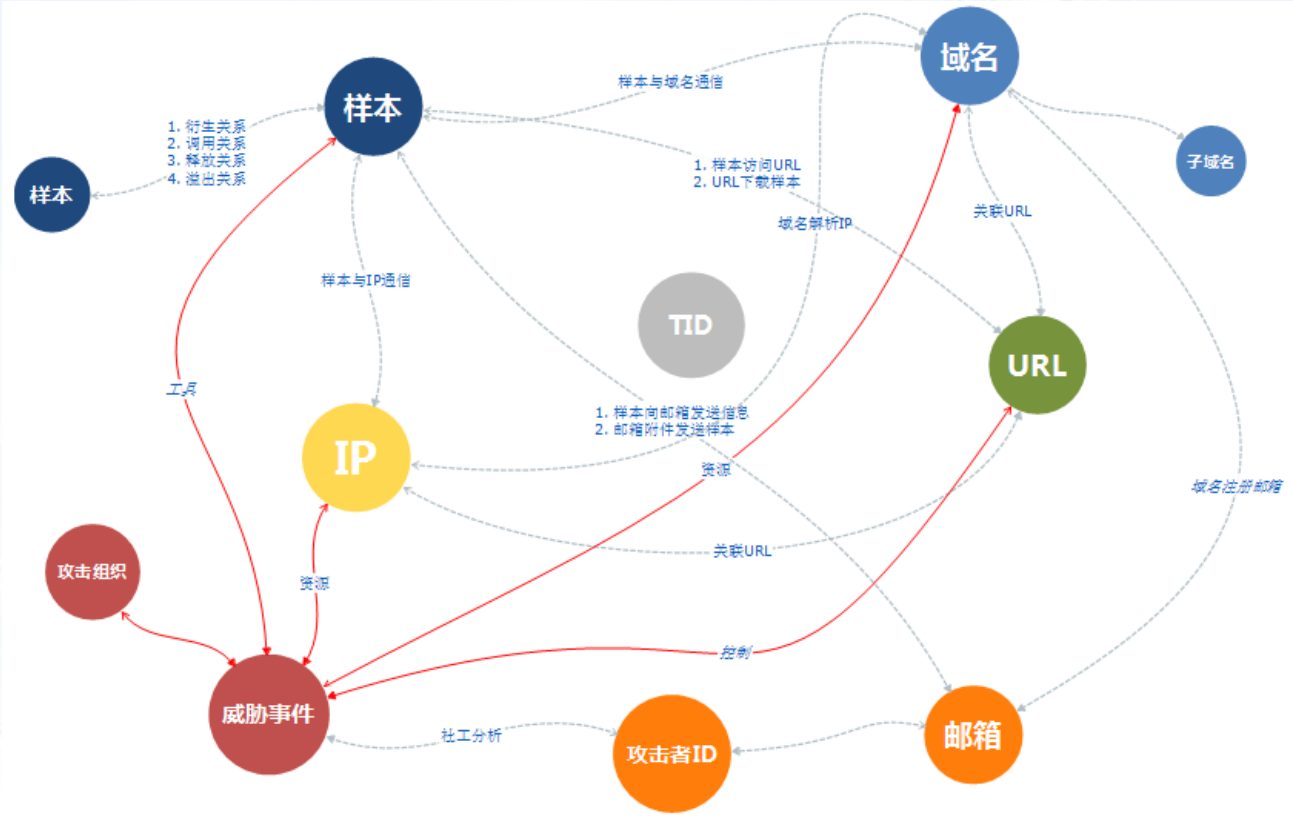
应用于多源数据汇聚整合

- **多源数据的汇聚整合**

应用于关联分析

- **关联分析模型**

对已知APT事件进行**基因提取**，**前端网络捕获**域名、ip、url path、端口、网络特征等属性，**后端挖掘**模糊哈希、代码段哈希、导入表哈希，文件名、文件大小、版本信息、时间戳、字符串信息、pdb路径信息、数字签名信息、互斥量信息、衍生文件、注册表键值、shellcode等属性,结合**威胁情报库**和**网络基础信息库**，实现对象间威胁关联的深度分析。



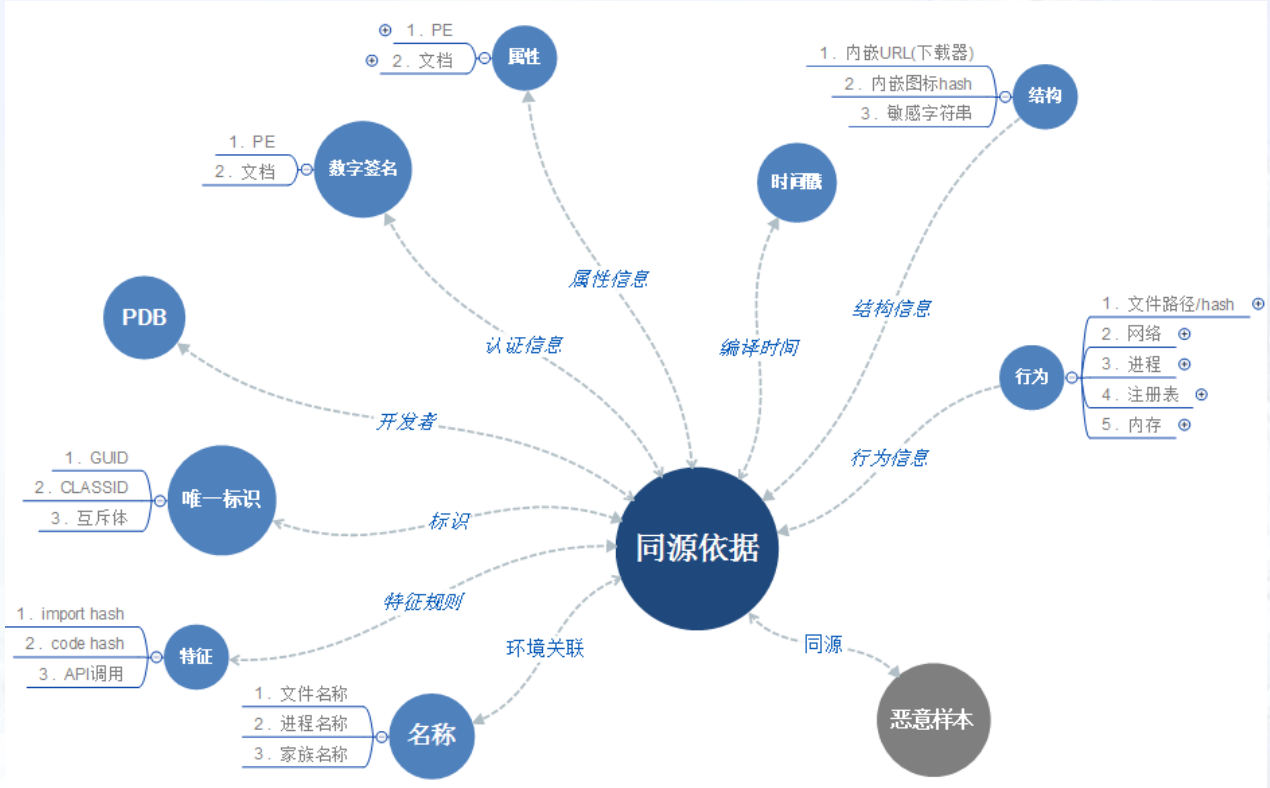
应用于同源分析

- **恶意样本同源性分析**

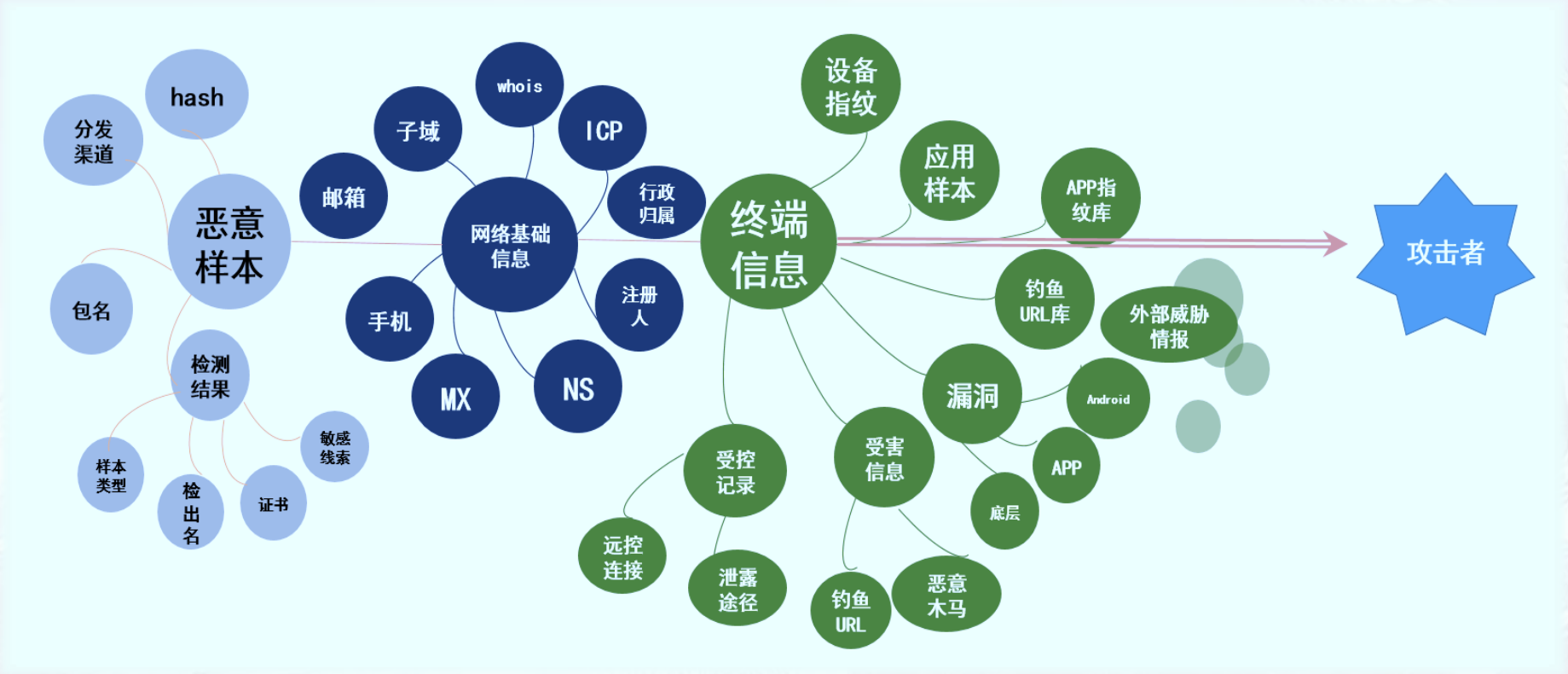
通过研究多个特征维度上的恶意代码的关联模型和分类、聚类模型，充分揭示恶意样本之间的同源性。

分析同源性的依据主要分为以下几类：

家族同源	**开发者同源**
家族名称	PDB
代码段	GUID
API调用序列	互斥量
图标	数字签名
导入表	版本信息
	文件名
攻击资源同源	**工具集同源**
域名	导出表-导入表
IP	进程调用
漏洞	



应用于多源融合关联分析追踪溯源



案例1-赋能揭示攻击者使用技术手段

- 从网络获取的海莲花组织相关信息

年份	国家	行业	恶意软件
2014	越南	网络安全	WINDSHIELD
2014	德国	制造业	WINDSHIELD
2015	越南	媒体	WINDSHIELD
2016	菲律宾	消费品	KOMPROGO WINDSHIELD SOUNDBITE BEACON
2016	越南	银行	WINDSHIELD
2016	菲律宾	技术基础设施	WINDSHIELD
2016	中国	医院	WINDSHIELD
2016	越南	媒体	WINDSHIELD
2016	美国	消费品	WINDSHIELD PHOREAL BEACON SOUNDBITE

网络上搜索到的信息不包含工具载荷的Hash信息

1.工具信息

103.53.197.202	104.237.218.70	104.237.218.72
185.157.79.3	193.169.245.78	193.169.245.137
23.227.196.210	24.datatimes.org	80.255.3.87
blog.docksugs.org	blog.panggin.org	contay.deaftone.com
check.paidprefund.org	datatimes.org	docksugs.org
economy.bloghop.org	emp.gapte.name	facebook-cdn.net
gap-facebook.com	gl-appspot.org	help.checkonl.org
high.expbas.net	high.vphelp.net	icon.torrentart.com
images.chinabytes.info	imaps.qki6.com	img.fanspeed.net
job.supperpow.com	lighpress.info	menmin.strezf.com
mobile.pagmobiles.info	news.lighpress.info	notificeva.com
nsquery.net	pagmobiles.info	paidprefund.org
push.relasign.org	relasign.org	share.codehao.net
seri.volveri.net	ssl.zin0.com	static.jg7.org
syn.timeizu.net	teriava.com	timeizu.net
tonholding.com	tulationeva.com	untitled.po9z.com
update-flashs.com	vieweva.com	volveri.net
vphelp.net	yii.yiihao126.net	zone.apize.net

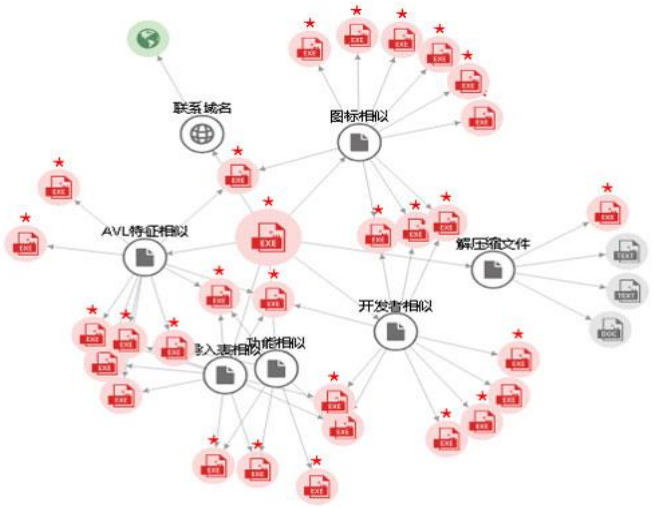
2.C&C信息

案例1-赋能揭示攻击者使用技术手段

案例2-赋能揭示恶意样本载荷的同源

威胁判定说明

恶意　白名单　未知　•点击图标显示节点详情　•右击图标查看菜单操作　•双击释放节点



保存分析模型　导出节点数据

EXE　d11b34685aa209171b0a4b89d06

关联　同源　收藏

威胁判定	Trojan/Win32.Reconyc
格式名称	BinExecute/Microsoft.EXE[:X86]
md5	d11b34685aa209171b0a4b89...

标签

CVE-2012-0158　WhiteElephant　APT　CVE-2012-0422　CVE-2012-4792

更多

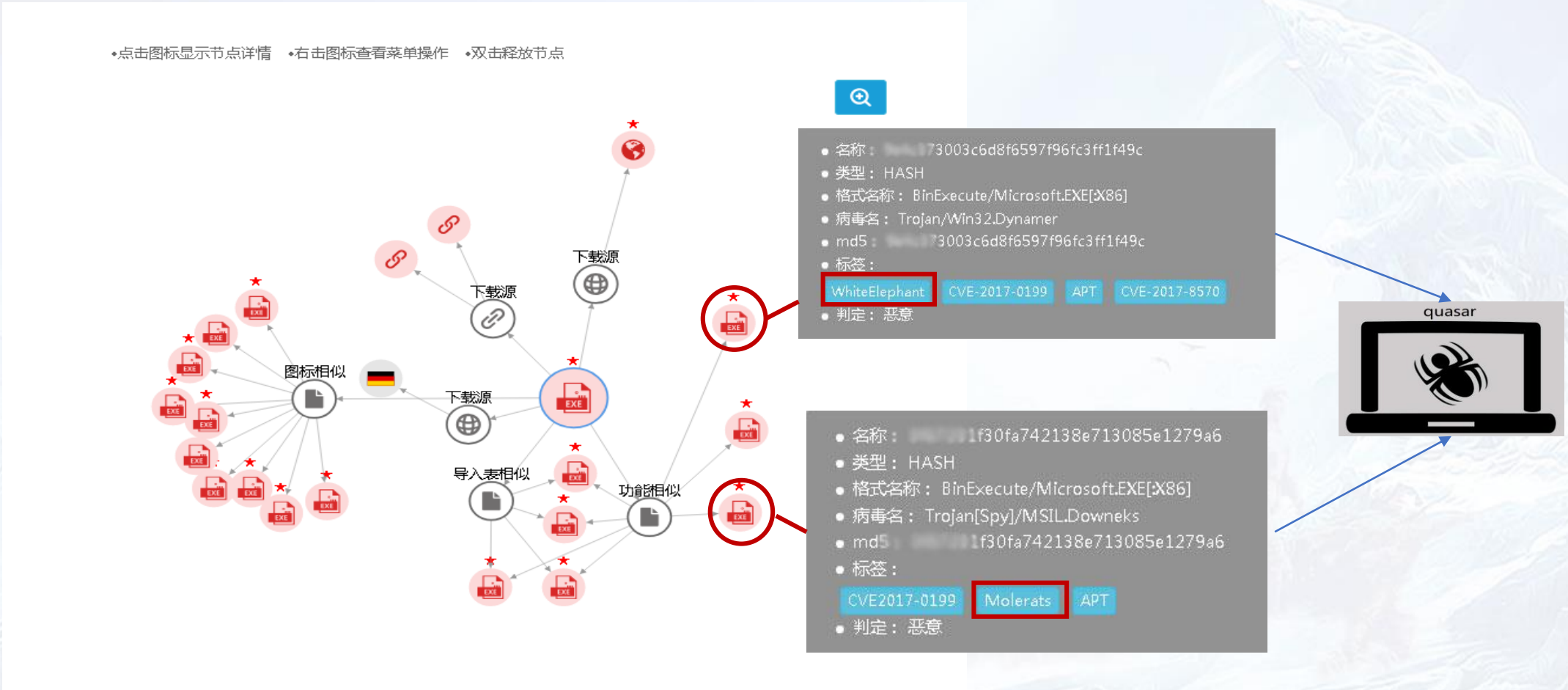
关联

功能相似	6
AVL特征相似	16
联系域名	1
图标相似	61
导入表相似	26
开发者相似	113
解压缩文件	4

案例2-赋能揭示恶意样本载荷的同源

- **基于下一代威胁检测引擎的向量输出能力将白象象群的攻击工具聚合在一起**

案例3-赋能揭示工具集的同源性



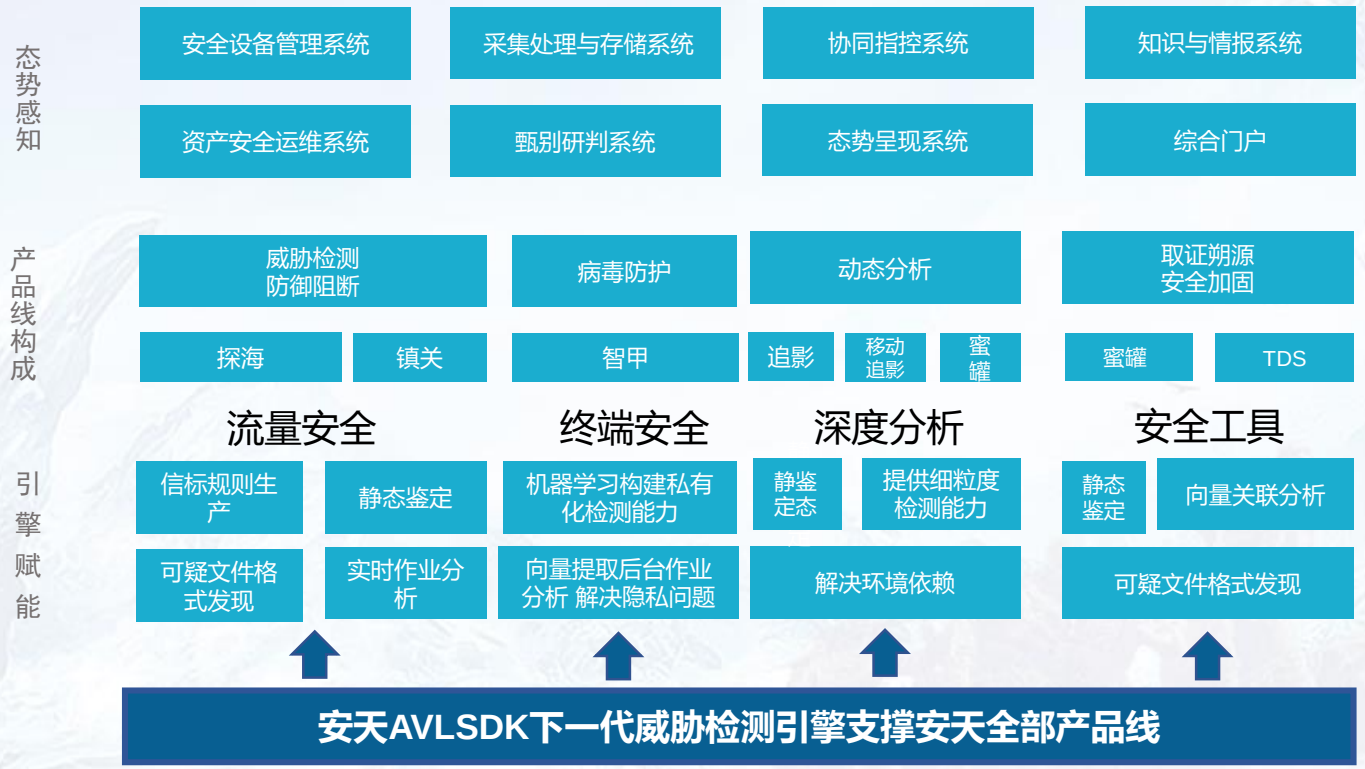
案例4-赋能揭示攻击目的

MD5	url	威胁名称	首次发现时间	攻击目的	格式
****afa1918240421b0a2749c2a3e24e	http://111.90.158.225/d/ft32	RiskWare[RiskTool]/Linux.BitCoinMiner.n	2018/11/6	挖矿	BinExecute/Linux.ELF[:X86]
****cf699252377b4e477357e4bf8e63	http://111.90.158.225/d/ft32	RiskWare[RiskTool]/Linux.BitCoinMiner.n	2018/11/9	挖矿	BinExecute/Linux.ELF[:X86]
****9fc3561e94051998d11381a00bbd	http://111.90.158.225/d/ft64	RiskWare[RiskTool]/Linux.BitCoinMiner.n	2018/11/7	挖矿	BinExecute/Linux.ELF[:X64]
****543e84f19f49bcec27313600845e	http://111.90.158.225/d/ft64	RiskWare[RiskTool]/Linux.BitCoinMiner.n	2018/11/9	挖矿	BinExecute/Linux.ELF[:X64]
****25f47dd6c62077cf52aeb5a759e7	http://111.90.158.225/d/mn32.exe	RiskWare[RiskTool]/Win32.BitMiner.gen	2018/11/6	挖矿	BinExecute/Microsoft.EXE[:X86]
****8045df750419911c6e1bf493c747	http://111.90.158.225/d/ft32	Trojan/Linux.CoinMiner.fd	2018/11/26	挖矿	BinExecute/Linux.ELF[:X86]
****a18d7949bcfc2b0928cfd8683478	http://111.90.158.225/d/ft32	Trojan/Linux.CoinMiner.fd	2018/12/15	挖矿	BinExecute/Linux.ELF[:X86]
****8a6c72c06d1892132d5e1d793b4b	http://111.90.158.225/d/fast.exe	Trojan/Win32.Occamy.c	2018/11/4		BinExecute/Microsoft.EXE[:X86]
****8a6c72c06d1892132d5e1d793b4b	http://111.90.158.225/d/ft.exe	Trojan/Win32.Occamy.c	2018/11/4		BinExecute/Microsoft.EXE[:X86]
****bbef96b8507715dc4d975e7f8f5f	http://111.90.158.225/d/ft.exe	Trojan/Win32.Occamy.c	2018/12/13	刷广告/刷流量	BinExecute/Microsoft.EXE[:X86]
****994a8f2fd5af2961166c8c456b6d	http://111.90.158.225/d/srv.exe	Trojan/Win32.Occamy.c	2018/12/14		BinExecute/Microsoft.EXE[:X86]
****74e871bce1df442b73bf927f1f39	http://111.90.158.225/d/mn64.exe	Trojan/Win32.Satan	2018/11/4		BinExecute/Microsoft.EXE[:X64]
****a336185bc2141f9c92a59a918c26	http://111.90.158.225/d/srv.exe	Trojan/Win32.Satan	2018/11/4		BinExecute/Microsoft.EXE[:X86]
****2bc458d9e94e8fabfc8402cd2b78	http://111.90.158.225/d/srv.exe	Trojan/Win32.Skeeyah.a	2018/11/9		BinExecute/Microsoft.EXE[:X86]
****ee0187c61d8eb4348e939da5a366	http://111.90.158.225/d/conn32	Trojan[Exploit]/Linux.LuckyRansom	2018/11/18	勒索	BinExecute/Linux.ELF[:X86]
****a1dd0b7bb17a816c18cce18cdbc6	http://111.90.158.225/d/conn.exe	Trojan[Exploit]/Win32.ShadowBrokers.ae	2018/11/4		BinExecute/Microsoft.EXE[:X86]
****bbda5f7c02ca179a366232adbb96	http://111.90.158.225/d/conn.exe	Trojan[Exploit]/Win32.ShadowBrokers.ae	2018/11/16		BinExecute/Microsoft.EXE[:X86]
****4b74ee538dab998085e0dfaa5e8d	http://111.90.158.225/d/cry32	Trojan[Ransom]/Linux.LuckyRansom	2018/11/24	勒索	BinExecute/Linux.ELF[:X86]
****4e763a527f3ad43e9c30acd276ff	http://111.90.158.225/d/cpt.exe	Trojan[Ransom]/Win32.Crypmod.aatb	2018/11/24	勒索	BinExecute/Microsoft.EXE[:X86]

- 多平台开发能力 ----------→ 适应不同环境
- 持续不断的维护更新 ----------→ 通过不断维护更新攻击载荷 避免被检测
- 攻击目的多样 ----------→ 以勒索、挖矿为目的

是一个以获取经济利益为主要目的，技术能力强，有组织，有分工的黑客团伙

更广泛的应用场景


态势感知
安全设备管理系统
采集处理与存储系统
协同指控系统
知识与情报系统
资产安全运维系统
甄别研判系统
态势呈现系统
综合门户
产品线构成
威胁检测
防御阻断
病毒防护
动态分析
取证朔源
安全加固
探海
镇关
智甲
追影
移动追影
蜜罐
蜜罐
TDS
流量安全
终端安全
深度分析
安全工具
引擎赋能
信标规则生产
静态鉴定
机器学习构建私有化检测能力
静鉴定态
提供细粒度检测能力
静态鉴定
向量关联分析
可疑文件格式发现
实时作业分析
向量提取后台作业分析 解决隐私问题
解决环境依赖
可疑文件格式发现
安天AVLSDK下一代威胁检测引擎支撑安天全部产品线

总结

- 安天下一代威胁检测引擎具备对载荷深度格式识别、格式解析、威胁揭示能力。
- 基于威胁检测引擎能力生产具备战术性威胁情报，支撑态势感知系统。
- 将下一代威胁检测引擎内嵌安天全系列产品，依托产品能力达成积极防御的，猎杀威胁的目标

网络空间威胁对抗与态势感知研讨会
暨 第六届安天网络安全冬训营

THANKS

扫码关注冬训营动态

战术型态势感知指控积极防御
协同响应猎杀威胁运行实战化

铁流鏖戰