XDef 2019

对话·交流·合作　　前沿·实用·人才

第八届全国网络与信息安全防护峰会

网络安全威胁捕获与追踪关键技术分析

杨传安

首席架构师 绿盟科技

OUTLINE

提纲

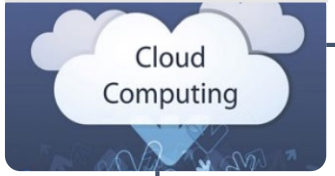
- 01 网络安全攻防的新形势
- 02 体系化防御运营中威胁hunting的价值
- 03 威胁Hunting系统建设思路及关键技术

01

网络安全攻防的新形势

新ICT和网络威胁的变化

云计算
打破网络边界, NFV深化ICT融合



移动
无处不在流动的信息和数据

大数据
海量数据管理，机器学习技术

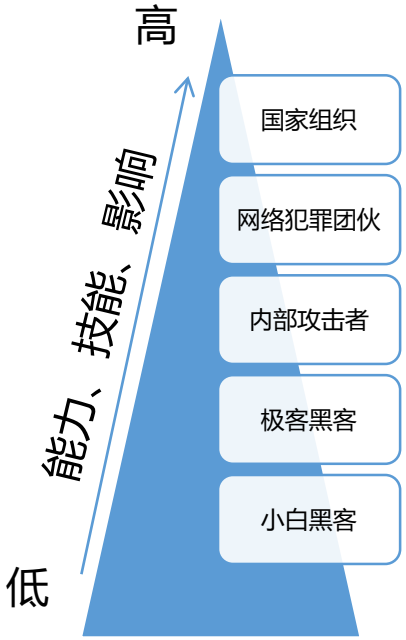
物联网
万物互联，IT&OT融合

云-网-数据-环境的数字化融合

网络**威胁泛化**

网络攻击的变化 – 能力金字塔 vs 技术平民化

攻击能力金字塔



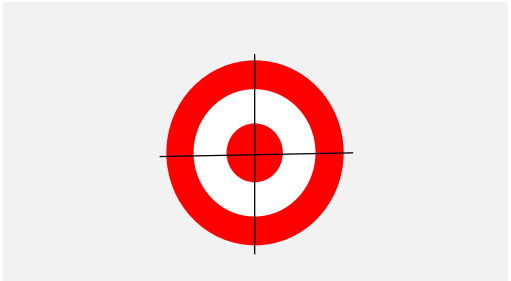
技术平民化，获取更容易（软件，计算资源，攻击工具）

网络攻击的变化 – 攻击意图多样化

粗暴简单攻击

金钱导向

有组织网络犯罪

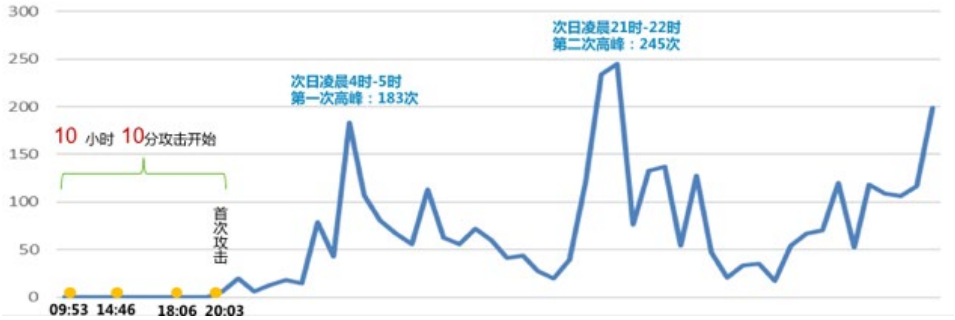


定向APT

敏感数据泄露

国家/区域组织

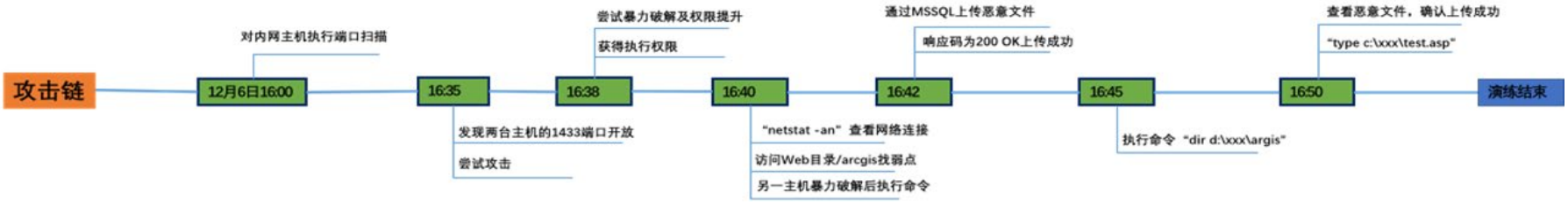
从**攻击活动**威胁看安全防御面临的挑战



数据来源：绿盟安全运营服务Struct2漏洞应急响应

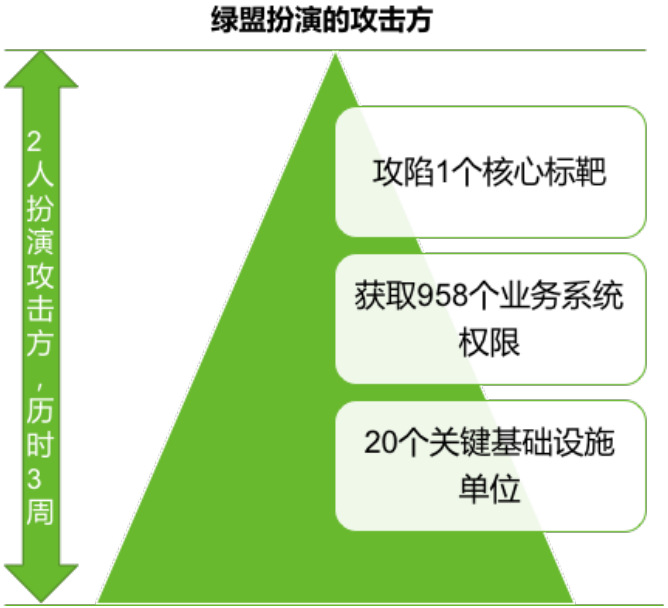
利用紧急漏洞的攻击行为
10小时被监测到

从扫描到非法获取主机权限
只用了8分钟

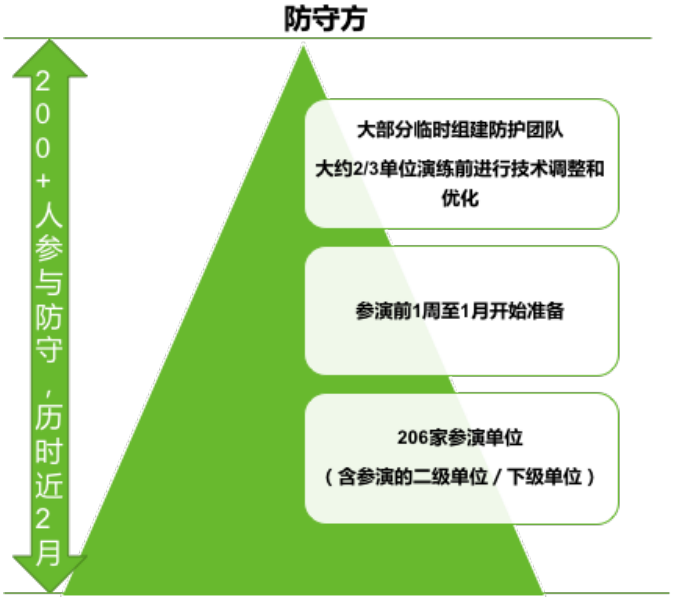


从安全演练观察防护现状

关键信息基础设施单位的安全防护能力并没有达到理想状态



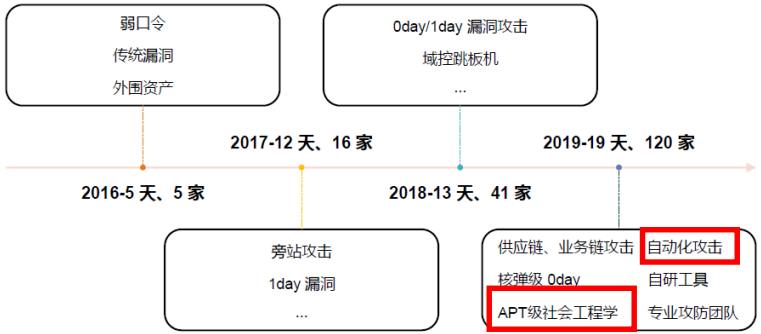
从安全演练看关键信息基础设施单位防护现状：人员、安全能力、技术方案规划和计划欠缺、



数据来源：某规模化安全演练活动

攻击侧能力升级在持续

绿盟战队演练后总结

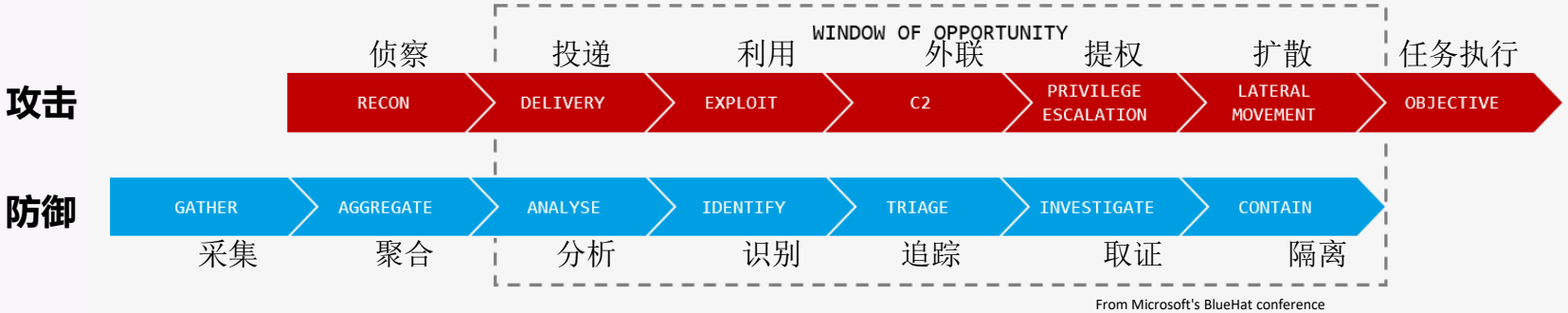


专业攻击服务(国外红队)

防御侧思路需要根本变化

BlueTeam 防御攻击链

攻防对抗的机会窗口



From Microsoft's BlueHat conference

威胁新范式理念的普遍接受

- 无法阻断所有攻击/You can’ t prevent all attacks.
- 网络将会被攻陷/Your network will be compromised.
- 百分百的安全不存在/One hundred percent security doesn’ t exist.

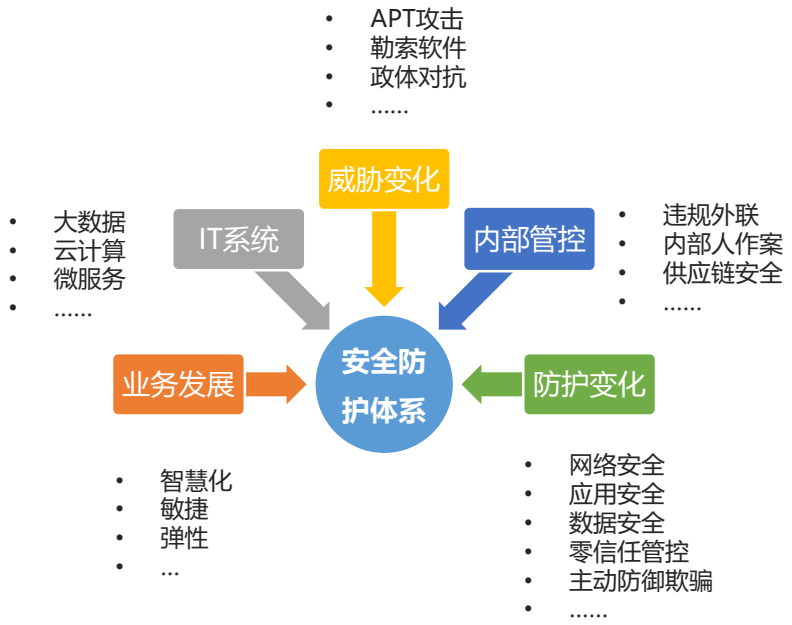
From security Intelligence

02

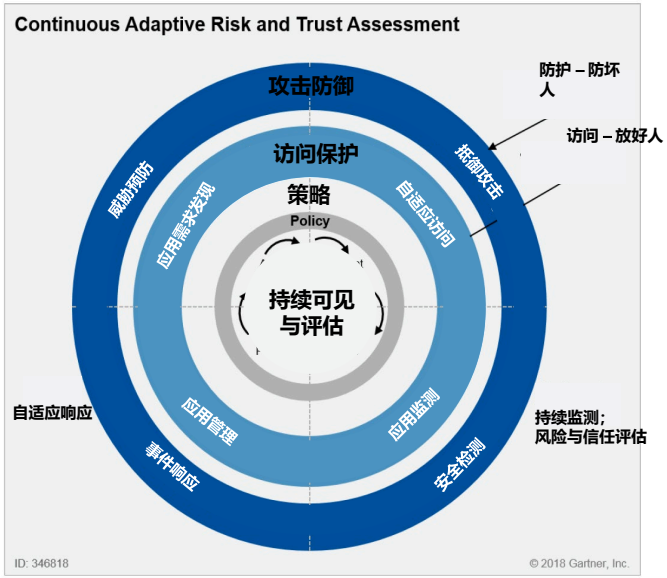
体系化防御运营中威胁hunting的价值

体系化的防御实践

设计驱动要素



理念参考模型



Source: Gartner (March 2018)

Gartner CARTA

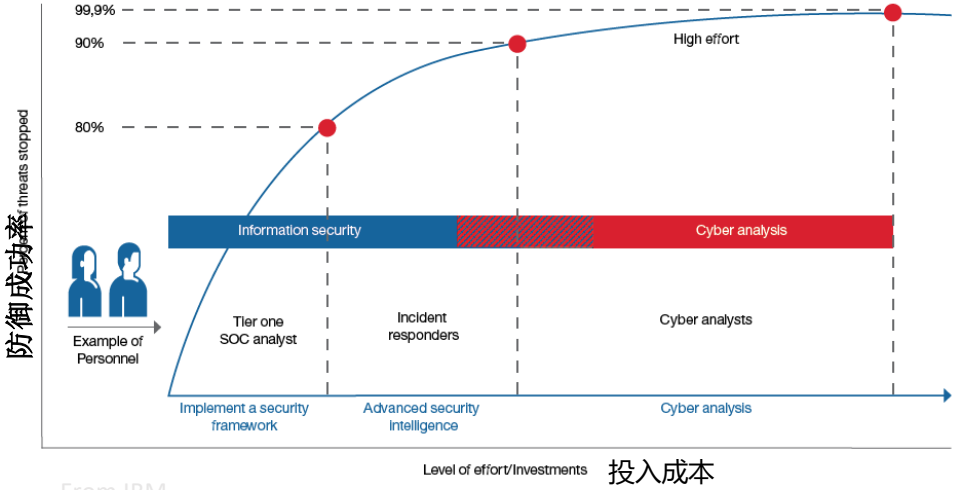
持续自适应风险与信任评估

防御能力和运营成熟度

要求提升主动对抗防御能力
威胁捕获&追踪Threat Hunting

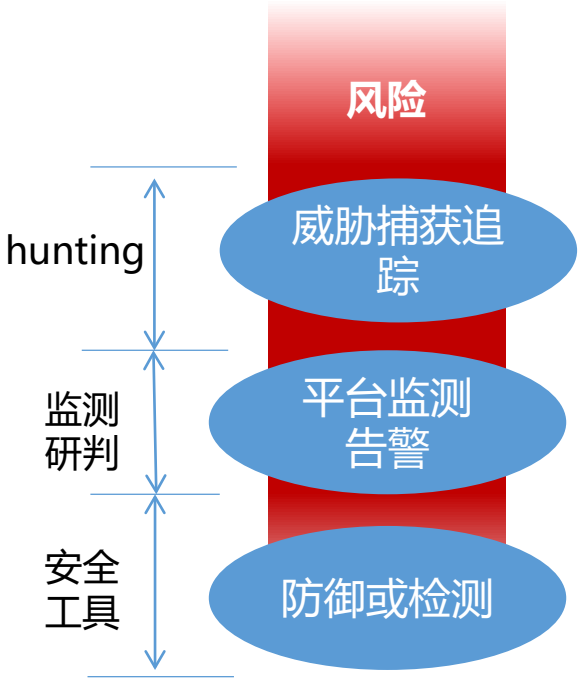
网络安全防御项目发展模型

From FireEye



From IBM

威胁捕获与追踪(Threat Hunting)



威胁追踪是一种迭代的方法，用于搜索、识别和了解进入防御者网络的攻击者。

Cyber threat hunting. *Cyber threat hunting is an* ***active cyber defence activity***. *It is "the process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions."*

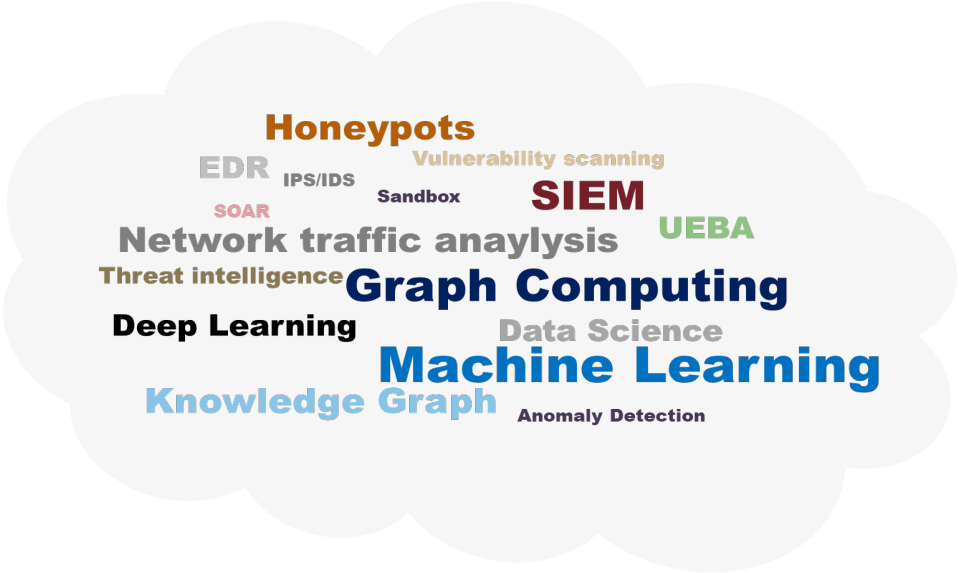
Cyber threat hunting - Wikipedia

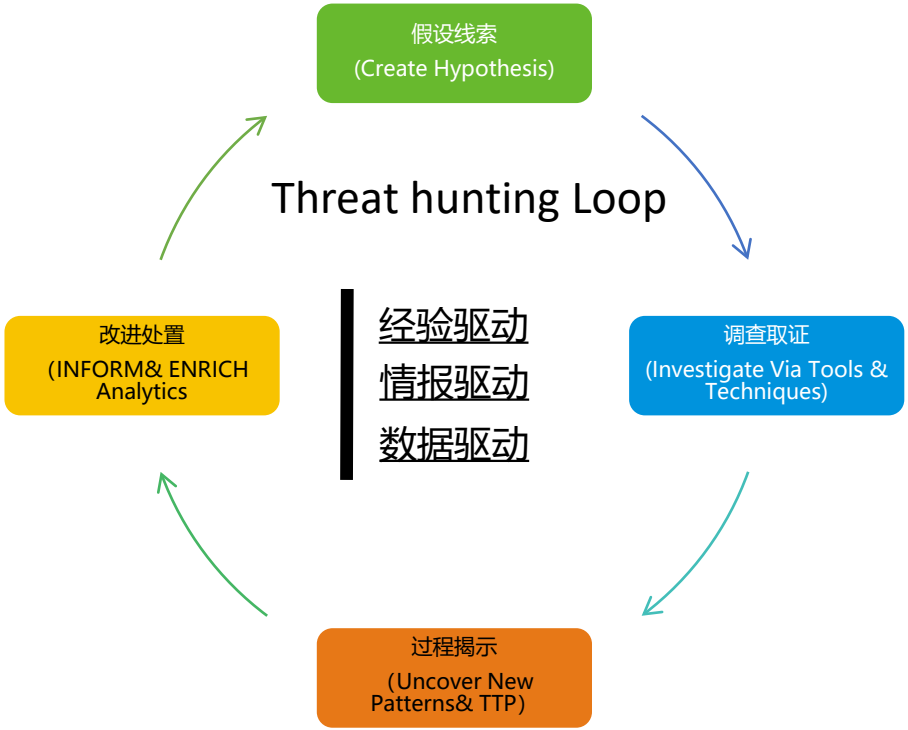
传统威胁分析 vs. 威胁Hunting

传统威胁分析	威胁hunting
基于发生的特定告警	基于假设、线索
被动	主动
依赖SIEM和规则积累，告警自动化归并	基于SIEM和专家知识，线索/评估/关联驱动
已知，根据已知规则发现已知事件	未知→未归编异常 已知→评级和溯源

场景1：检测知识之外的
场景2：挖掘淹没在海量告警之中的
场景3：主动防御潜在的
场景N：...

威胁Hunting处置参考模型





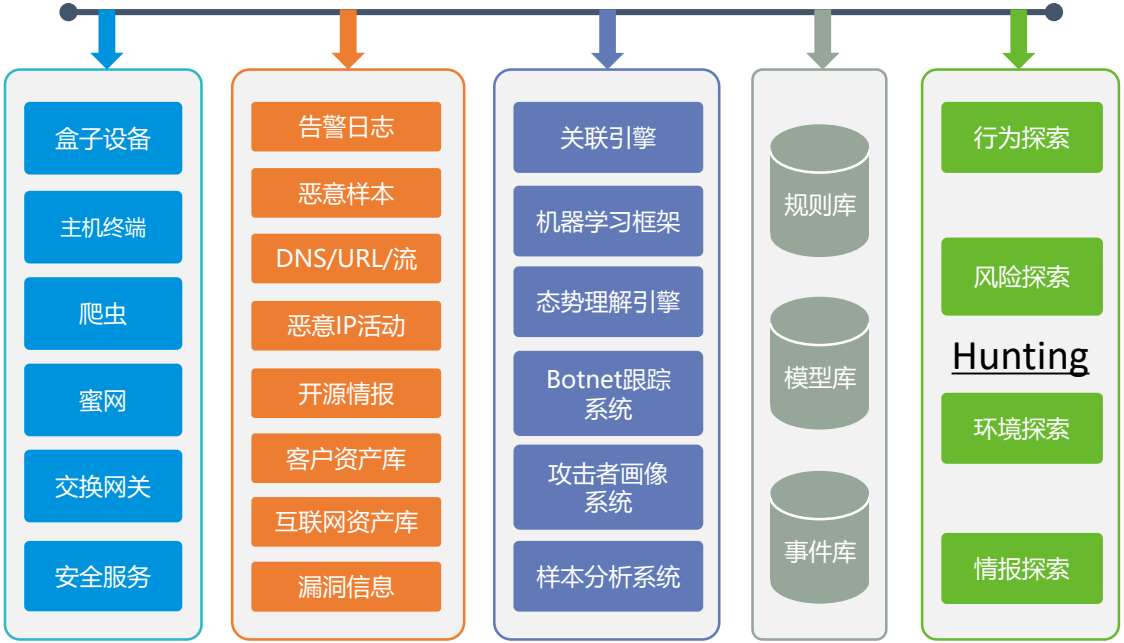
From Sqrrl

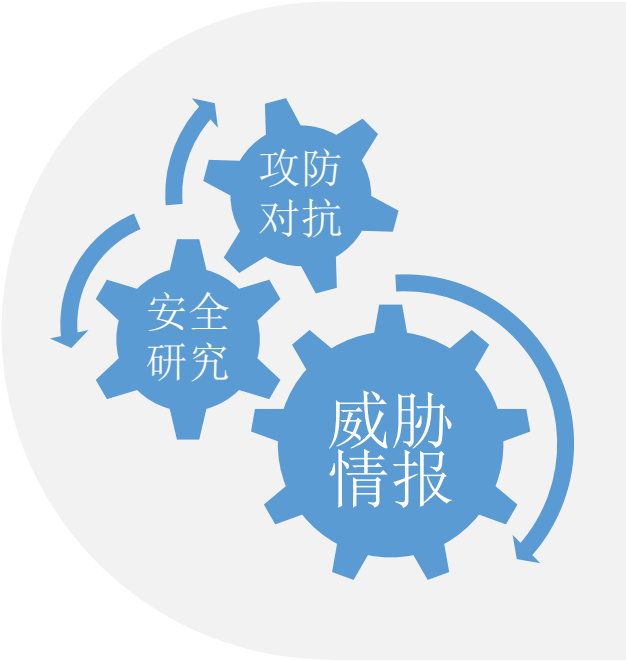
Sqrrl model

03

威胁Hunting系统建设思路及关键技术

威胁Hunting能力的建设思路参考





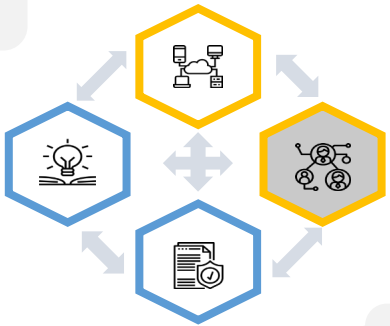
图关联-威胁hunting关键技术一

战场包含的实体信息，包括网络拓扑、用户资产、资产脆弱性等

环境数据图

实体的最新状态及实体关联

一切网络实体行为，如网络侧检测告警、终端侧检测告警、文件分析日志、应用日志、蜜罐日志、沙箱日志等



知识数据图

知识库及知识关联

行为数据图

实体的行为（原始的或聚合的）及关联

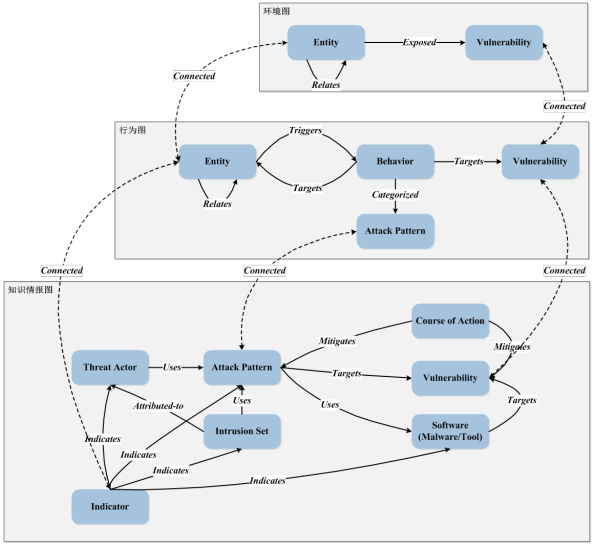
时间弱相关的、可推理的知识，如企业积累的攻防知识，或公开的知识库，如CAPEC、ATT&CK、CWE、NVD、CNNVD等

情报数据图

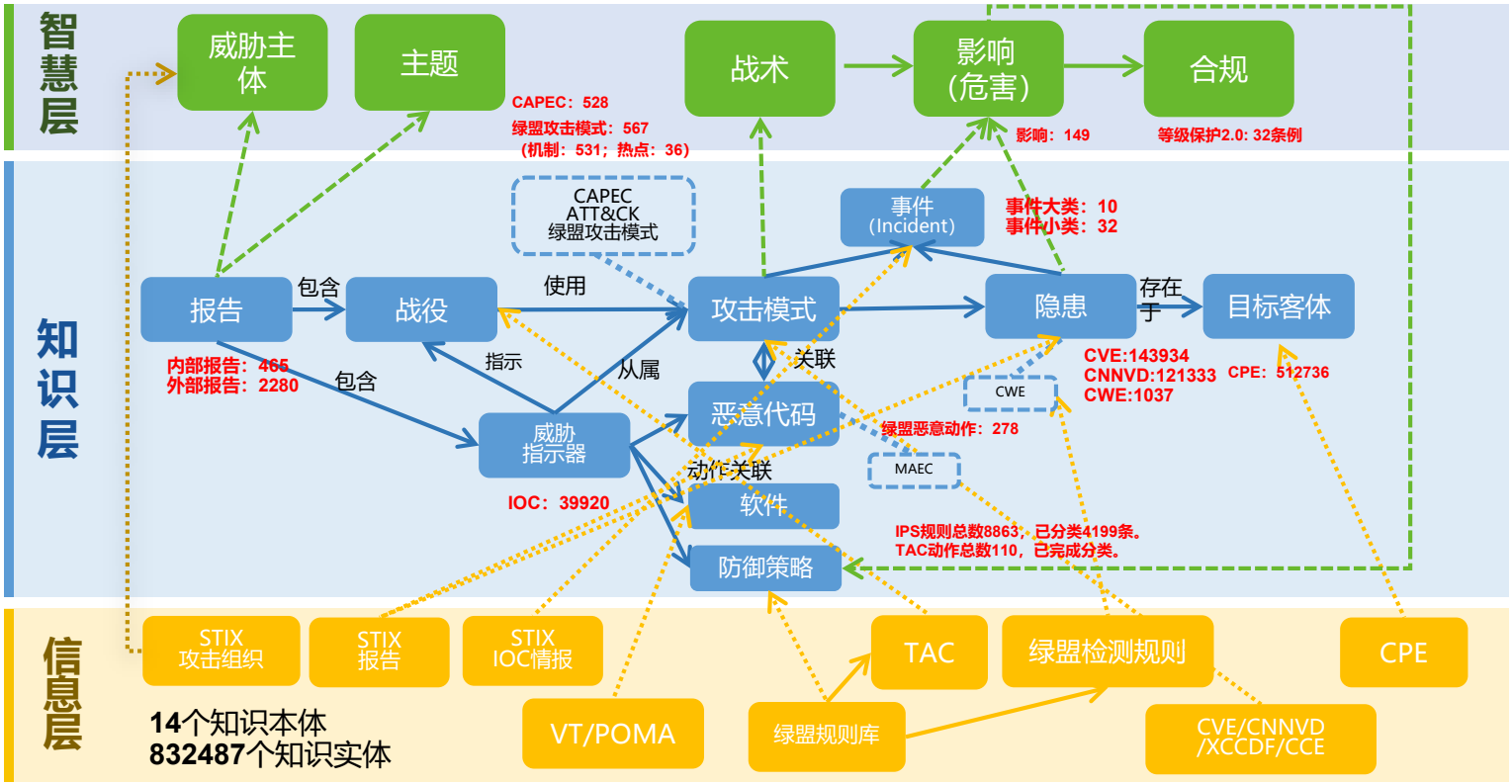
威胁情报及关联

时效性较强的、特定领域威胁情报数据

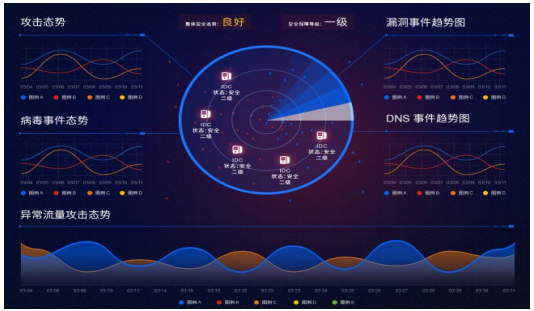
线索驱动的图分析

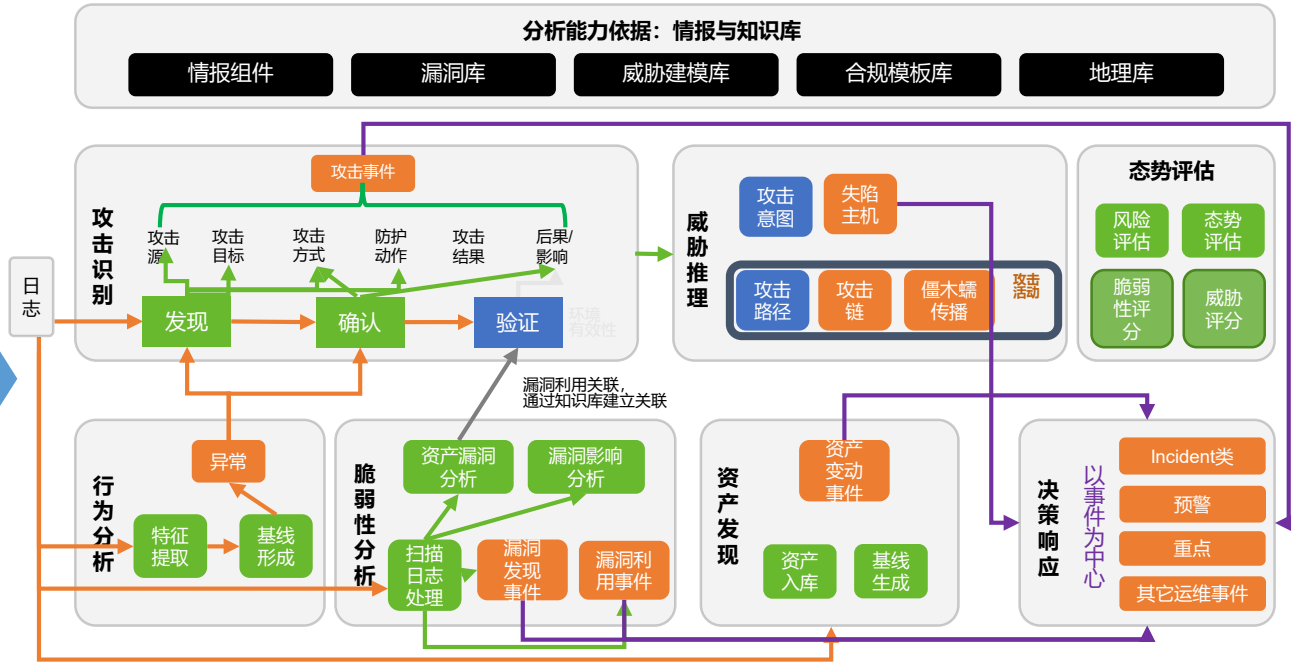


知识库 - 威胁hunting的重要基础



智能分析整合：威胁hunting关键技术二

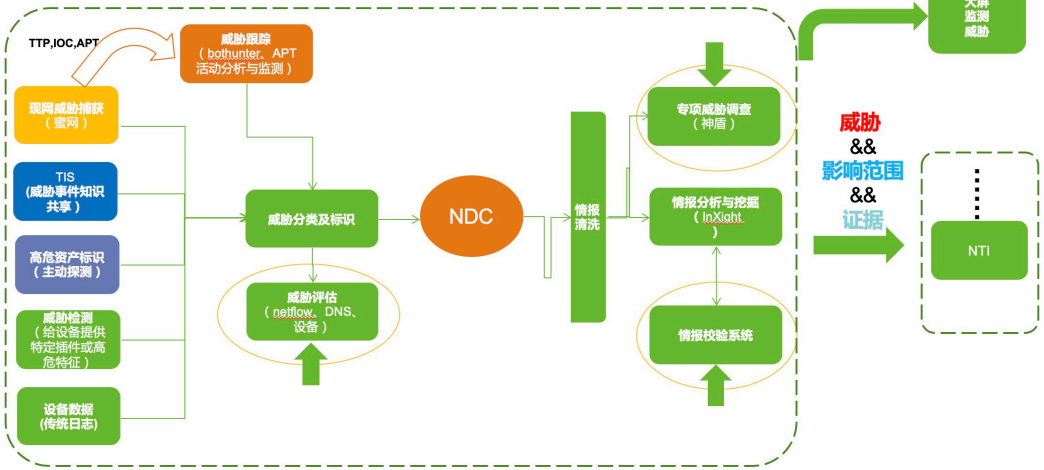




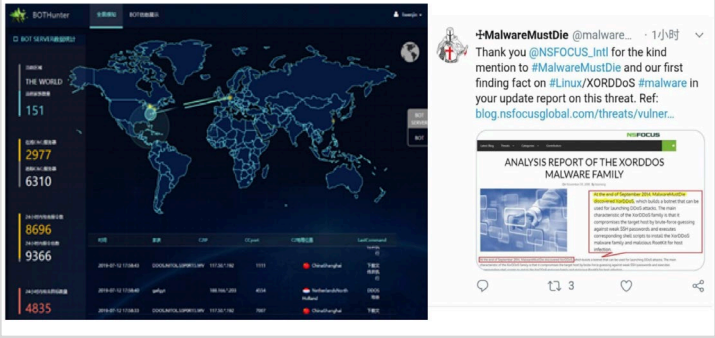
网络威胁态势感知系统的回归

网络威胁情报-威胁hunting关键技术三

绿盟互联网威胁狩猎系统

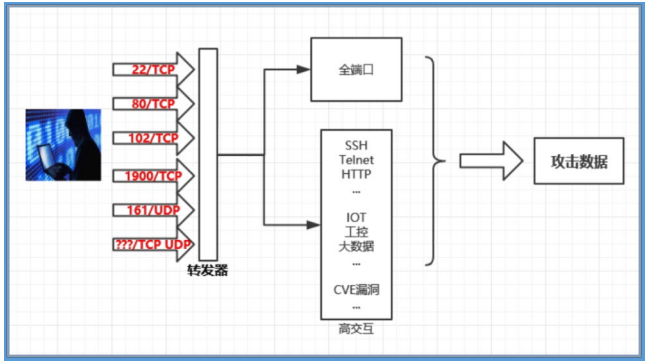


僵尸网络追踪



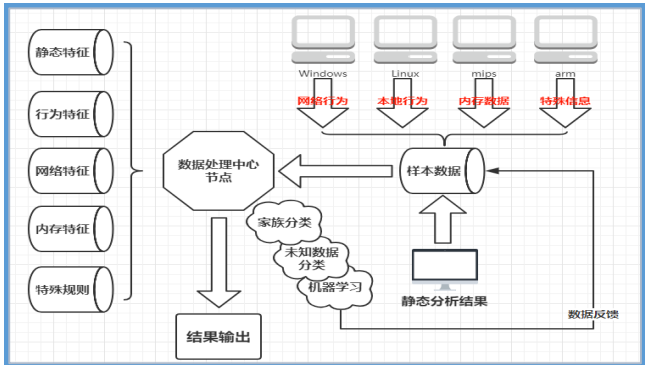
攻击团伙分析研究

类蜜罐的威胁捕获系统

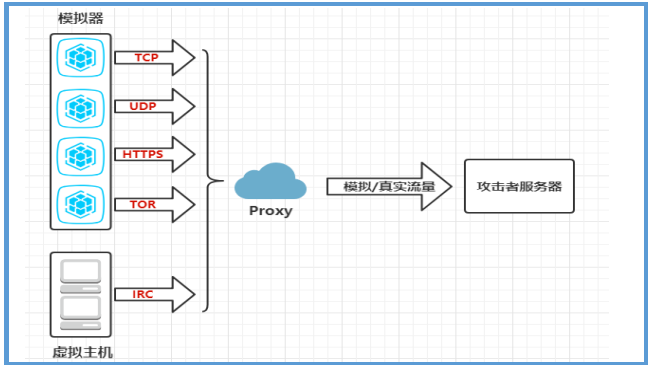


混合型捕获节点

遍布全球的捕获节点

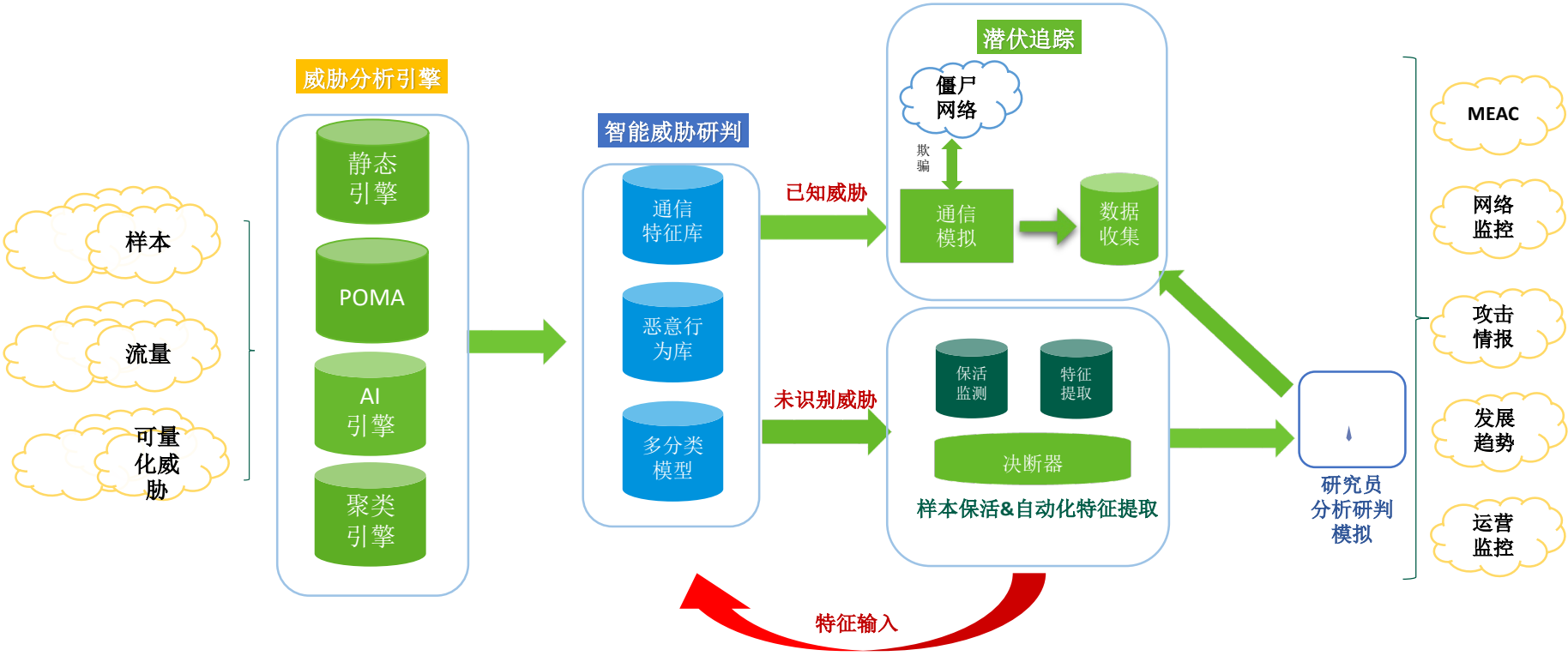


动静结合的精准识别

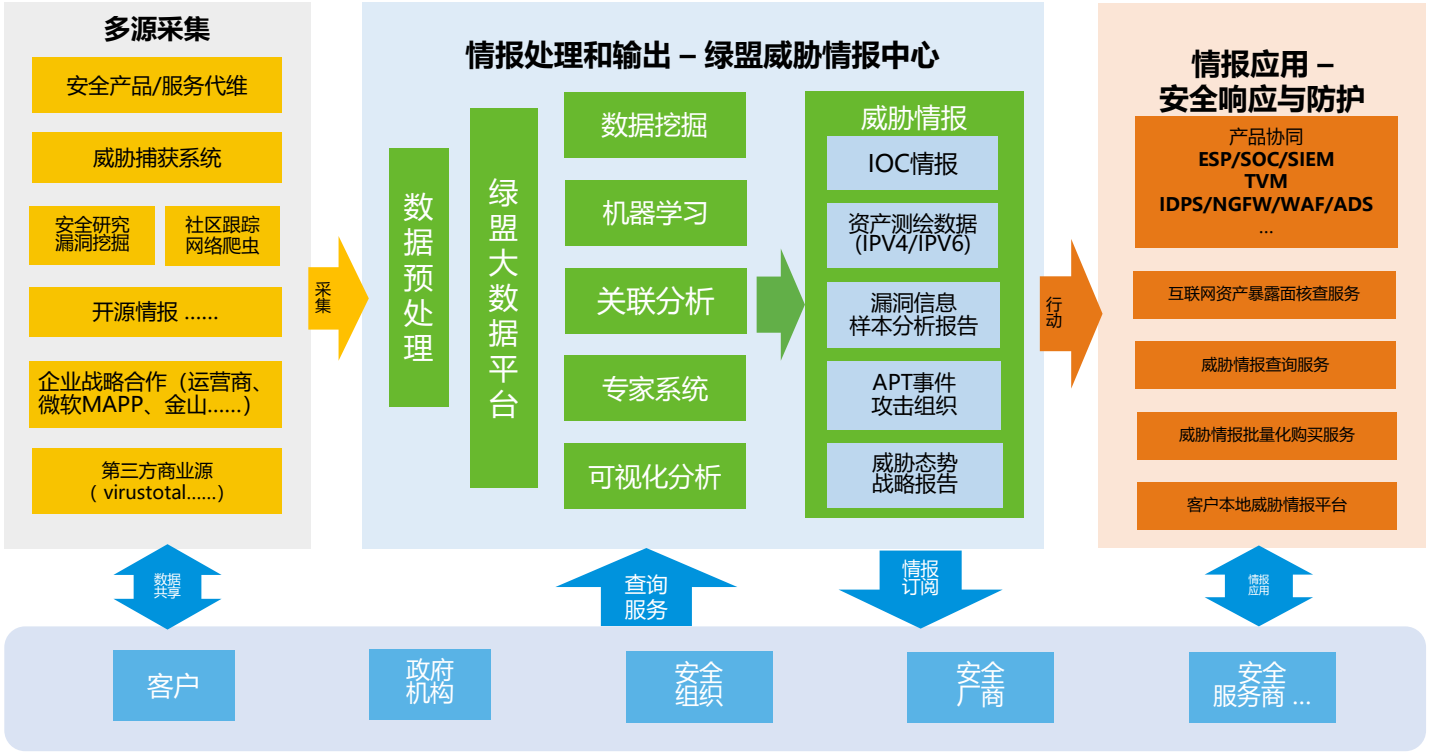


多系统、多协议的仿真僵尸网络节点

威胁捕获系统的生产过程



威胁情报的生态体系


多源采集
安全产品/服务代维
威胁捕获系统
安全研究
漏洞挖掘
社区跟踪
网络爬虫
开源情报 .....
企业战略合作（运营商、
微软MAPP、金山.....）
第三方商业源
(virustotal.....)
采集
情报处理和输出 – 绿盟威胁情报中心
数据预处理
绿盟大数据平台
数据挖掘
机器学习
关联分析
专家系统
可视化分析
威胁情报
IOC情报
资产测绘数据
(IPV4/IPV6)
漏洞信息
样本分析报告
APT事件
攻击组织
威胁态势
战略报告
行动
情报应用 –
安全响应与防护
产品协同
ESP/SOC/SIEM
TVM
IDPS/NGFW/WAF/ADS
...
互联网资产暴露面核查服务
威胁情报查询服务
威胁情报批量化购买服务
客户本地威胁情报平台
数据共享
查询服务
情报订阅
情报应用
客户
政府机构
安全组织
安全厂商
安全服务商 ...

威胁情报的生态体系

平台及工具

- 主机、终端、网络检测分析工具，行为分析、欺骗诱导工具
- 全场景感知的大数据平台
- 提供数据范式化接入、情报管理、大数据搜素、场景化关联分析，图谱关联、自动化

安全能力

- 威胁知识库
- 运营知识库
- 互联网威胁情报库
- 安全研究能力
- 专家

XDef 2019

对话·交流·合作　前沿·实用·人才

Thanks

谢谢关注!