



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

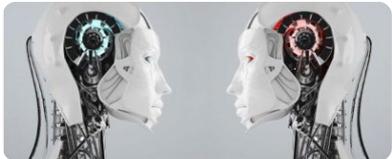
# 网络安全攻防的新形势

# 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)



**创意启蒙课程**

课程旨在为2-6岁儿童定制了创意启蒙课程, 该课程根据孩子的三个年龄段划分了三个阶段



**人工智能编程**

面向6-18岁青少年, 涵盖少儿启蒙编程和少儿趣味编程如Python, HTML, CSS, Java



**智能机器人编程**

采用体验式学习方式, 让小朋友在玩中学实现机器人设计与搭建, 并为机器人编写程序, 不断磨练与进行创新。



**信息学奥赛编程**

信息学奥赛的竞赛辅导课程, 是面向小学四年级及以上的小学生, 主要使用C++语言培训, 通过完整、高效的解題训练课程, 学员可参加NOIP比赛, 助力出国留学和开学考试。



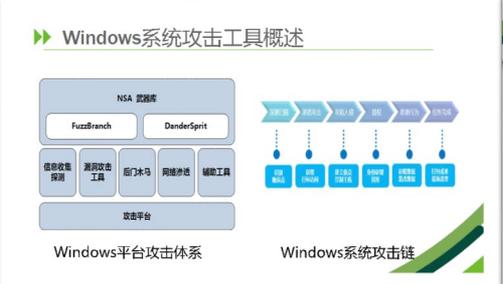
Linux系统攻击工具概述

Linux系统攻击体系

项目监控平台

文档管理 | 漏洞库 | 远控后门 | 辅助工具

漏洞情报收集 | 漏洞情报分析 | 漏洞情报研判 | 漏洞情报分发 | 漏洞情报利用 | 漏洞情报溯源 | 漏洞情报溯源



Windows系统攻击工具概述

NSA 数据库

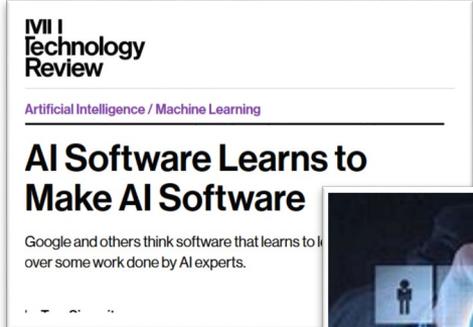
FuzzBranch | DanderSpirit

信息收集 | 漏洞情报工具 | 后门木马 | 网络渗透 | 辅助工具

攻击平台

Windows平台攻击体系

Windows系统攻击链



IVI I Technology Review

Artificial Intelligence / Machine Learning

### AI Software Learns to Make AI Software

Google and others think software that learns to do over some work done by AI experts.

## 网络攻击的变化 – 攻击意图多样化



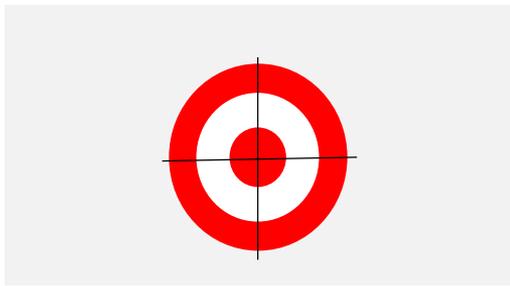
粗暴简单攻击



金钱导向



有组织网络犯罪



定向APT

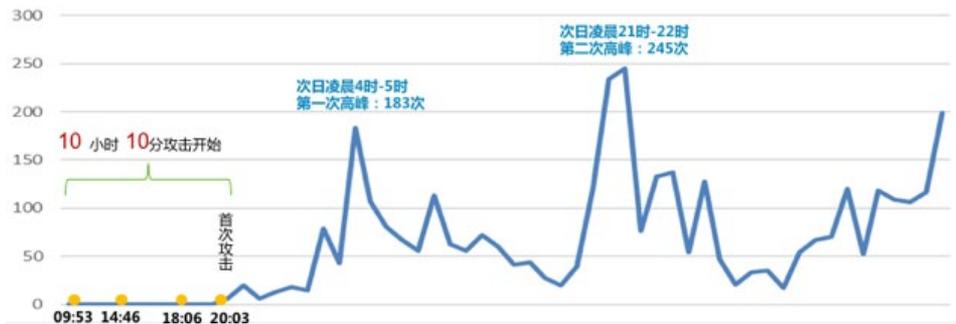


敏感数据泄露



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

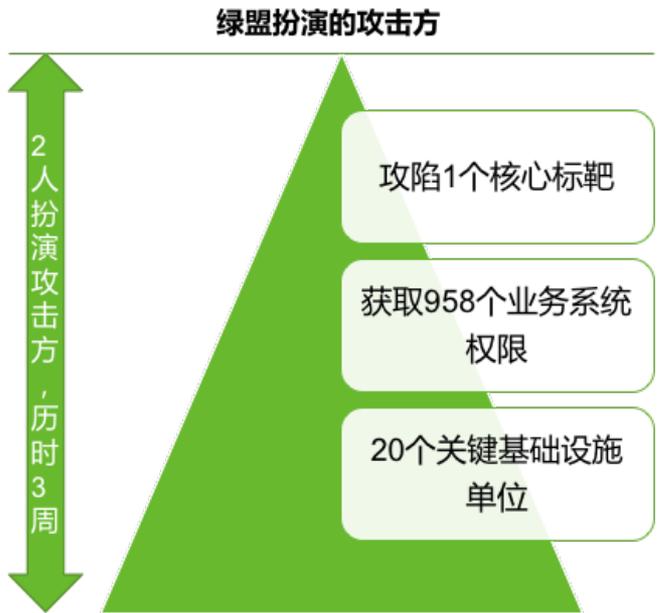
利用紧急漏洞的攻击行为  
10小时被监测到

从扫描到非法获取主机权限  
只用了8分钟

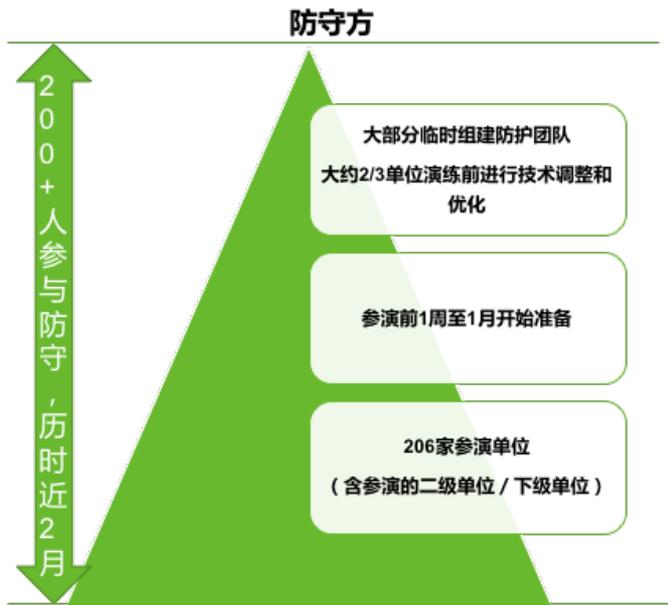


## 从安全演练观察防护现状

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

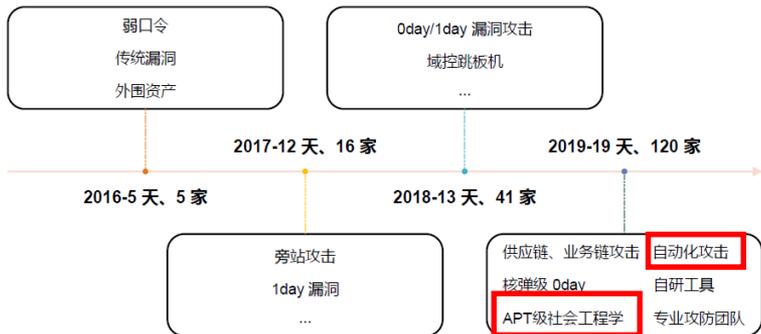


从安全演练看关键信息基础设施单位防护现状：  
人员、安全能力、技术方案规划和计划欠缺、



# 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)

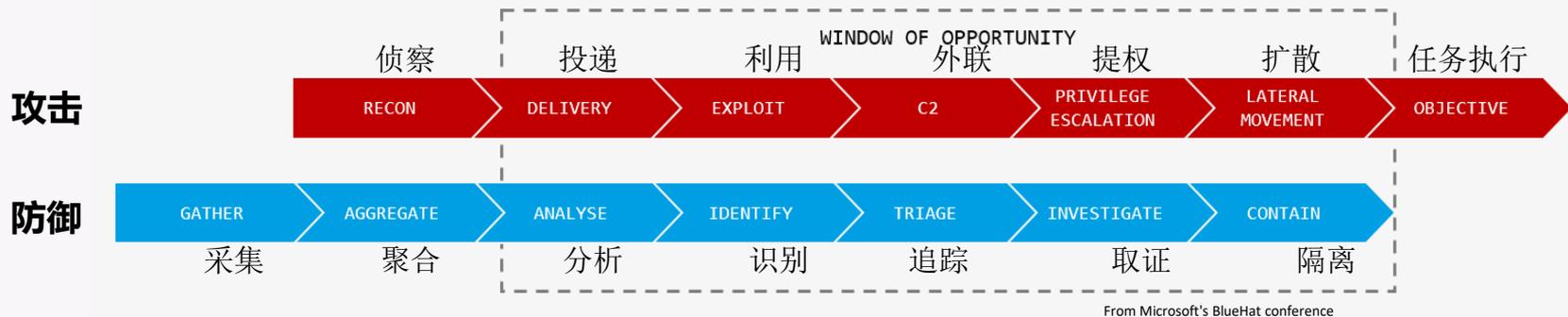
What is Red Team Service?  
~ Latest Penetration Test Trends in U.S.

- IBM X-Force Red
- McAfee Red Team Services
- MANDIANT RED TEAMING
- RAPID7 PENETRATION TESTING SERVICES
- Red Team Attack Simulation
- CROWDSTRIKE RED TEAM SERVICES
- Microsoft Enterprise Cloud Red Teaming

## 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



## 威胁新范式理念的普遍接受

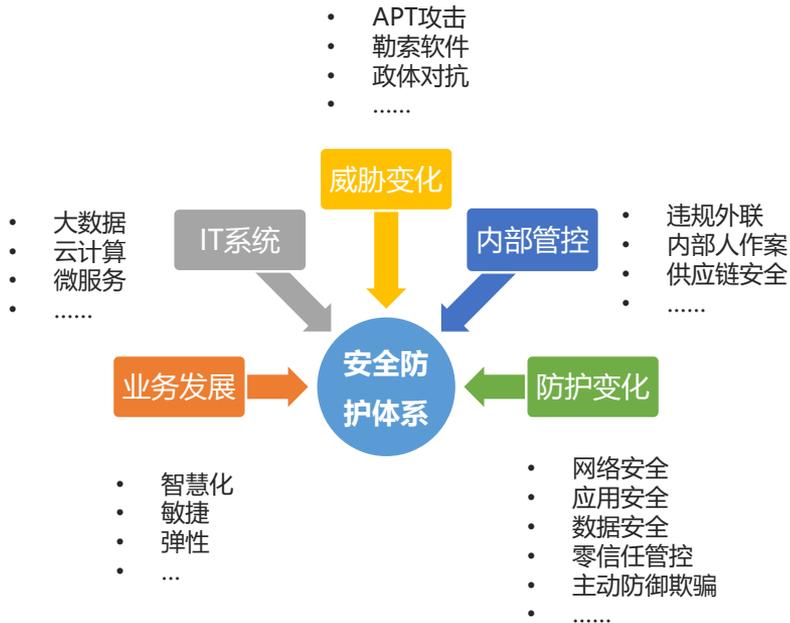
- 无法阻断所有攻击/You can't prevent all attacks.
- 网络将会被攻陷/Your network will be compromised.
- 百分百的安全不存在/One hundred percent security doesn't exist.

02

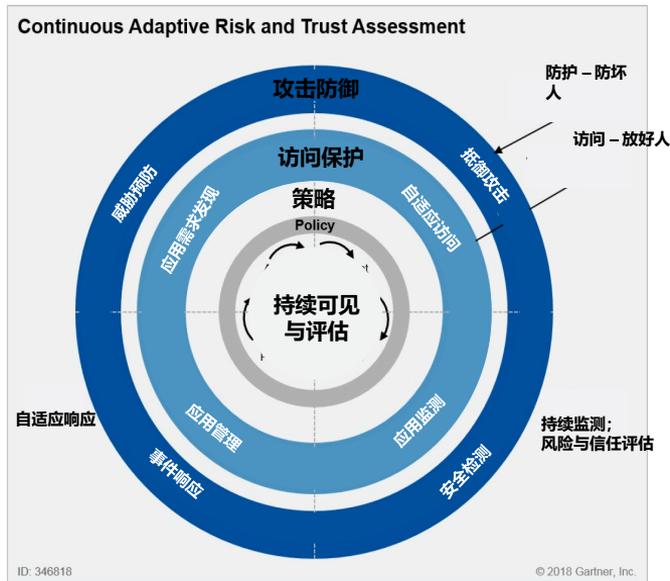
# 体系化防御运营中 威胁hunting的价值

# 体系化的防御实践

## 设计驱动要素



## 理念参考模型



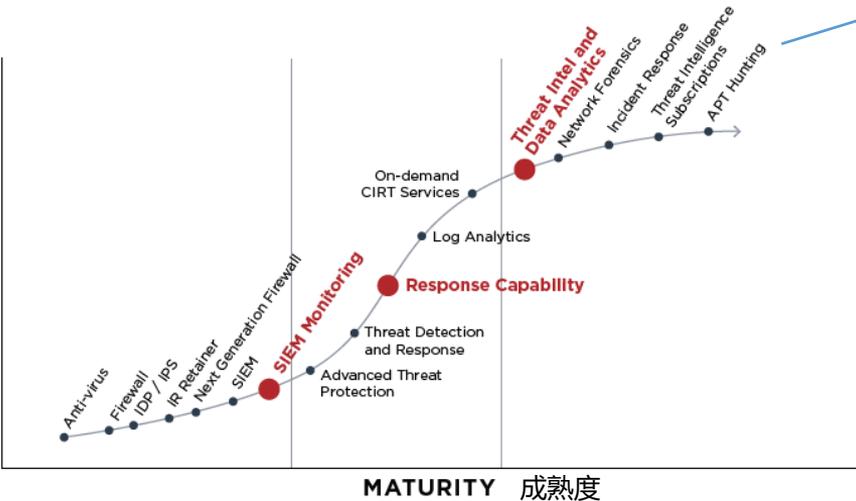
Source: Gartner (March 2018)

Gartner CARTA  
持续自适应风险与信任评估

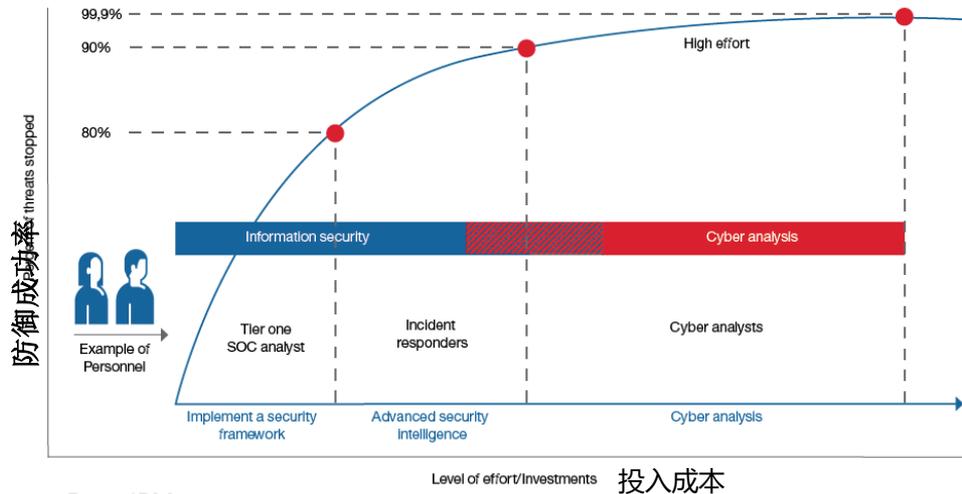
# 防御能力和运营成熟度

## 网络安全防御项目发展模型

要求提升主动对抗防御能力  
威胁捕获&追踪 Threat Hunting

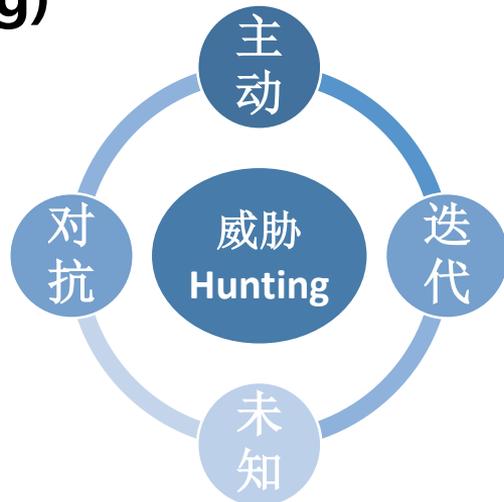
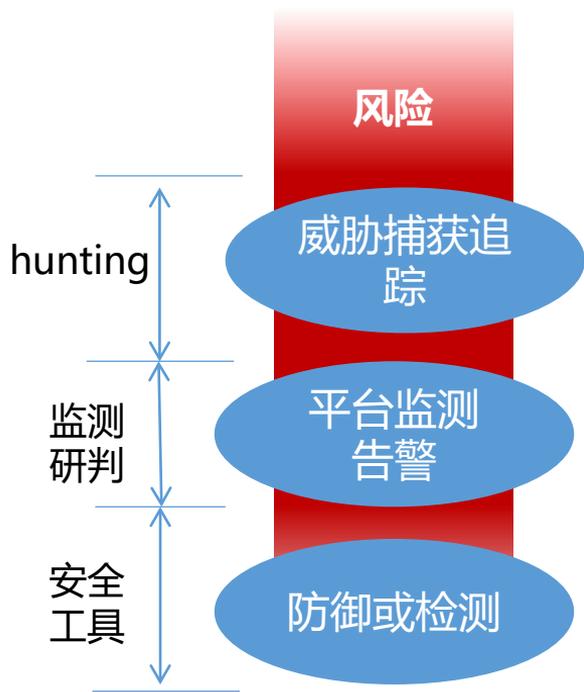


From FireEye



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."

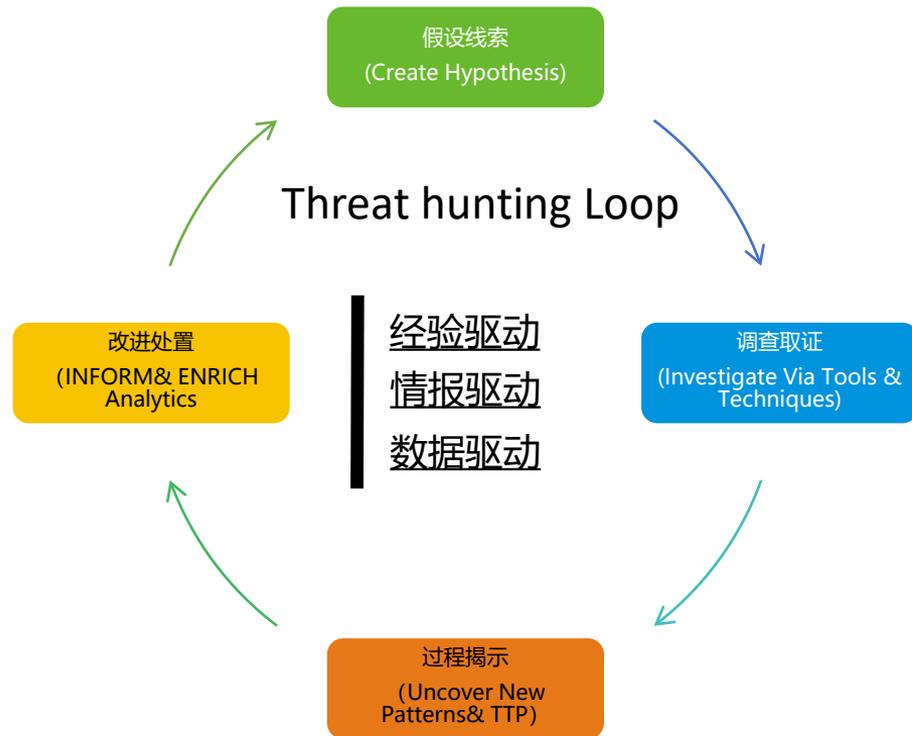
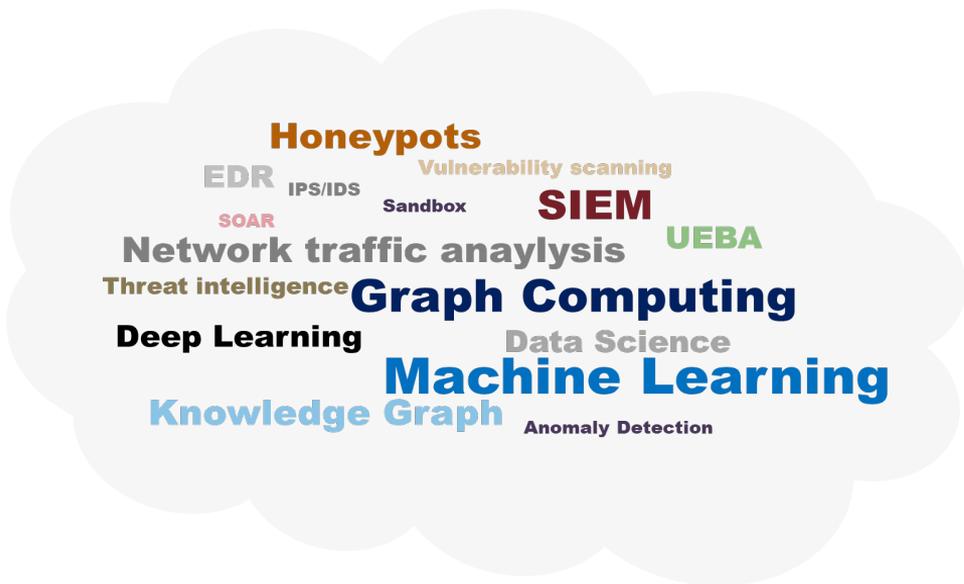
[Cyber threat hunting - Wikipedia](#)

## ▶▶ 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

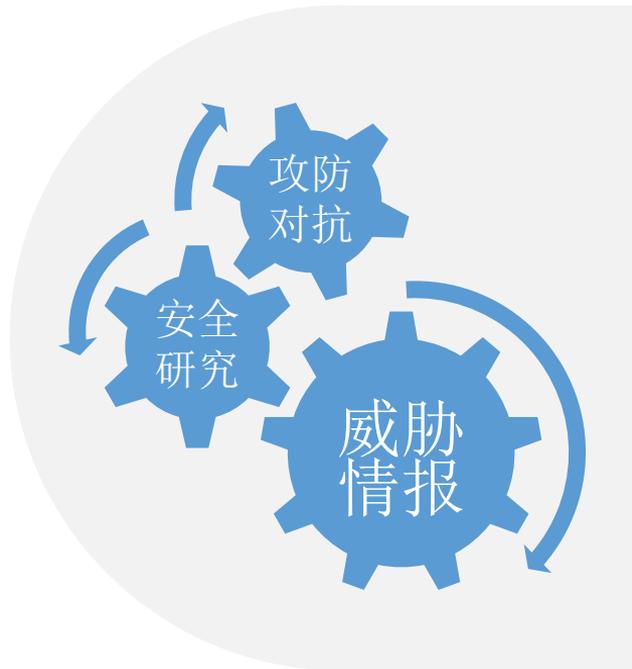
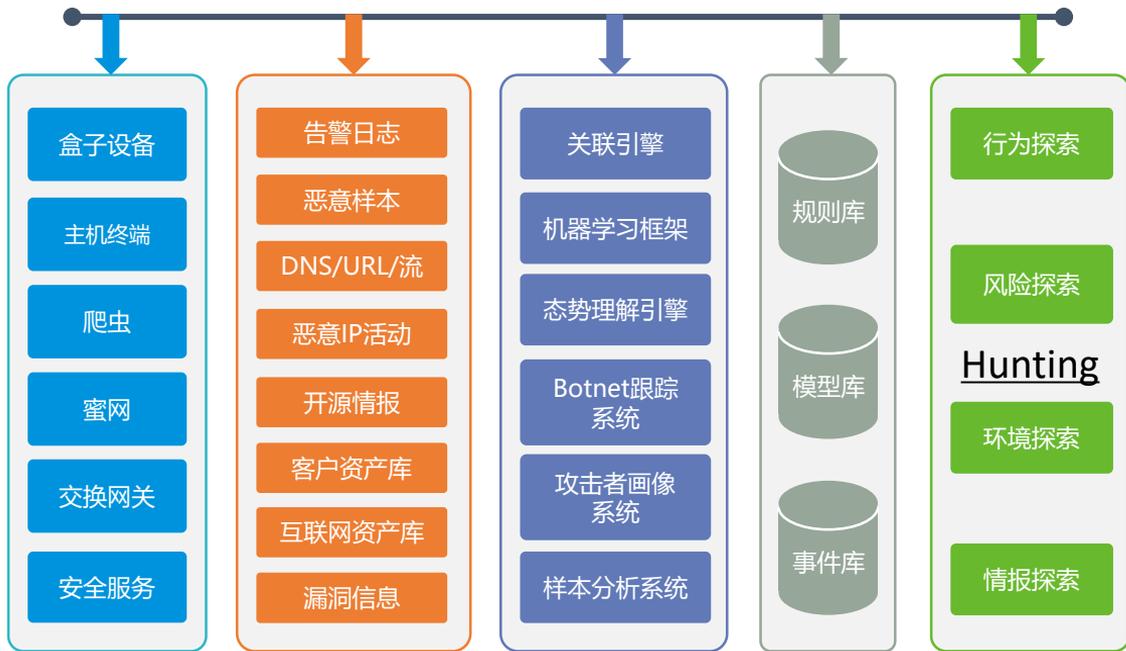


From Sqrrl

03

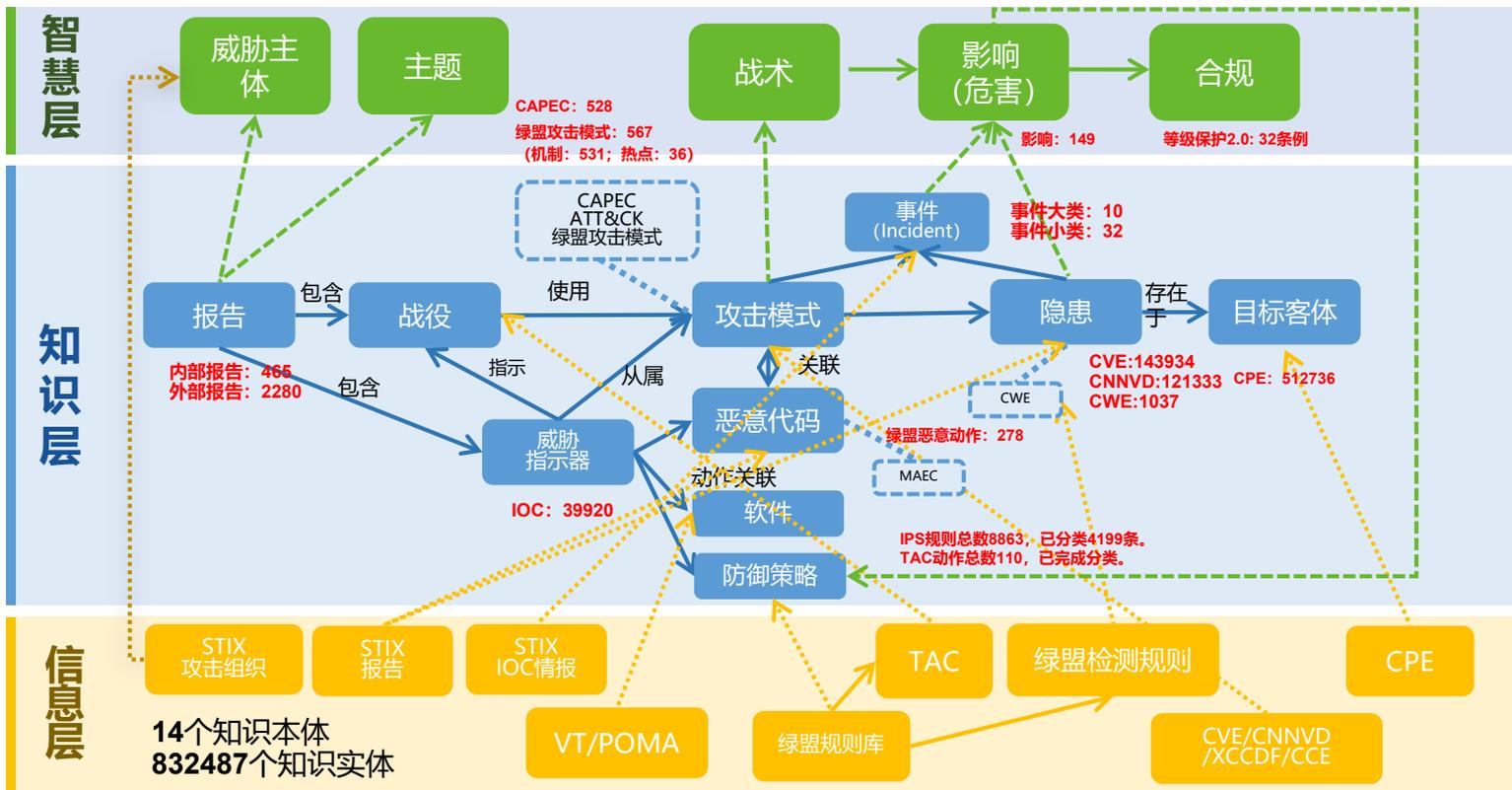
# 威胁Hunting系统 建设思路及关键技术

## 威胁Hunting能力的建设思路参考

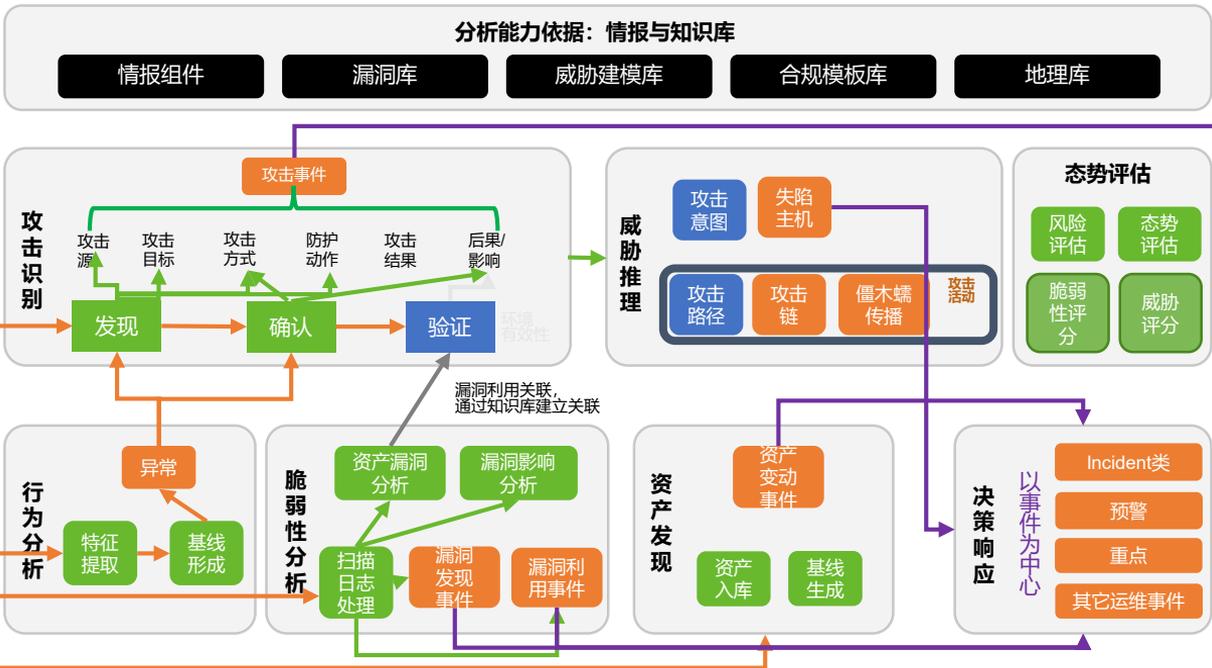
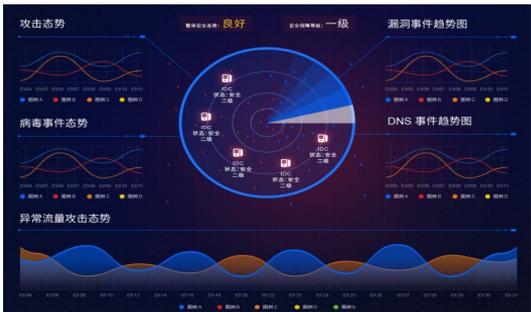




# 知识库 - 威胁hunting的重要基础



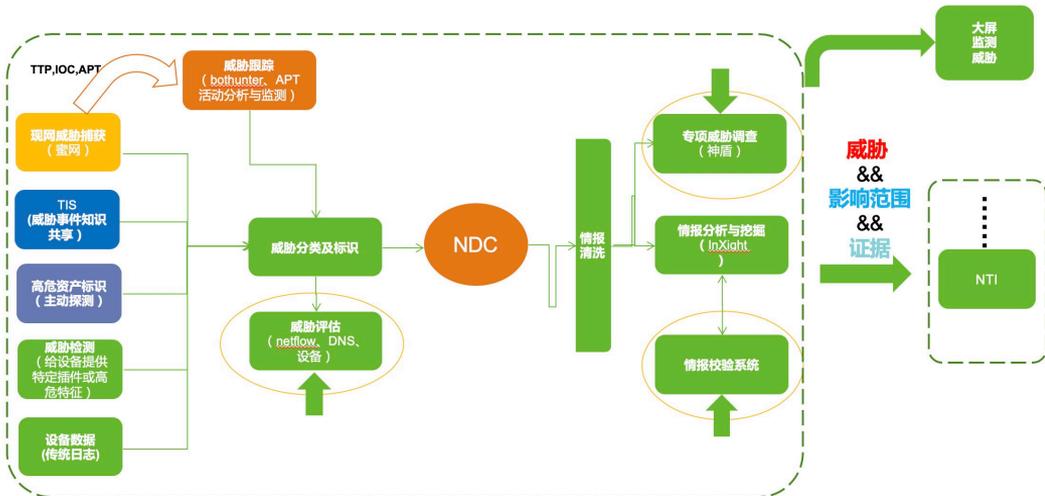
# 智能分析整合：威胁hunting关键技术二



## 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

The screenshot shows a security dashboard with a world map highlighting a specific geographic area. To the right, there is a tweet from @MalwareMustDie mentioning a report on the XorDox malware family. Below the tweet is a thumbnail for an 'ANALYSIS REPORT OF THE XORDDOX MALWARE FAMILY'.

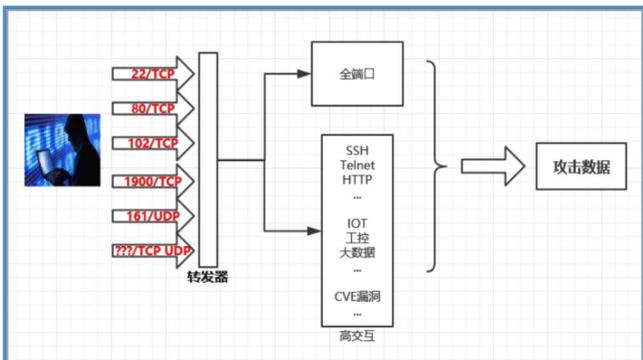
## 攻击团伙分析研究

The screenshot displays a report titled 'Cybersecurity Insights - IP Gang Report'. It features several visualizations: a network graph on the left, a radar chart in the center, and a relationship diagram on the right. Below the radar chart is a table with the following data:

语言平台	攻击时频	Word2Vec
攻击工具	攻击特性	自然语言处理
攻击方法	目标/源特性	密度聚类

Text on the right side of the report includes: '活跃攻击团伙总览(C&C和攻击目标)' and '团伙 G1 年度 C&C 和攻击目标的关系拓扑'.

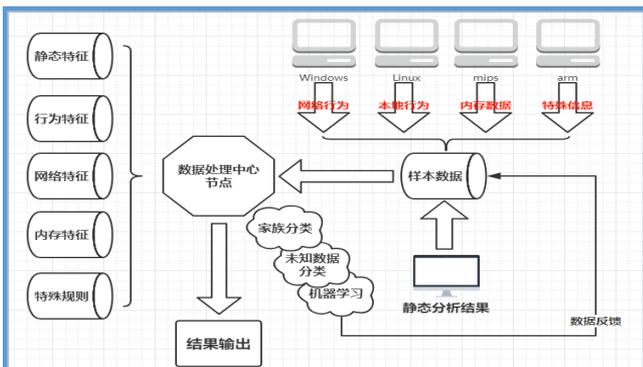
# 类蜜罐的威胁捕获系统



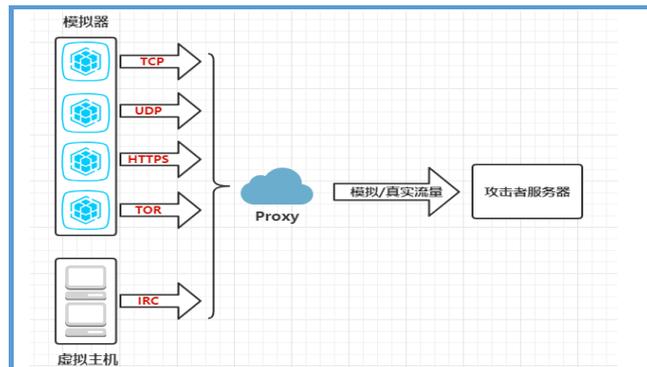
混合型捕获节点



遍布全球的捕获节点

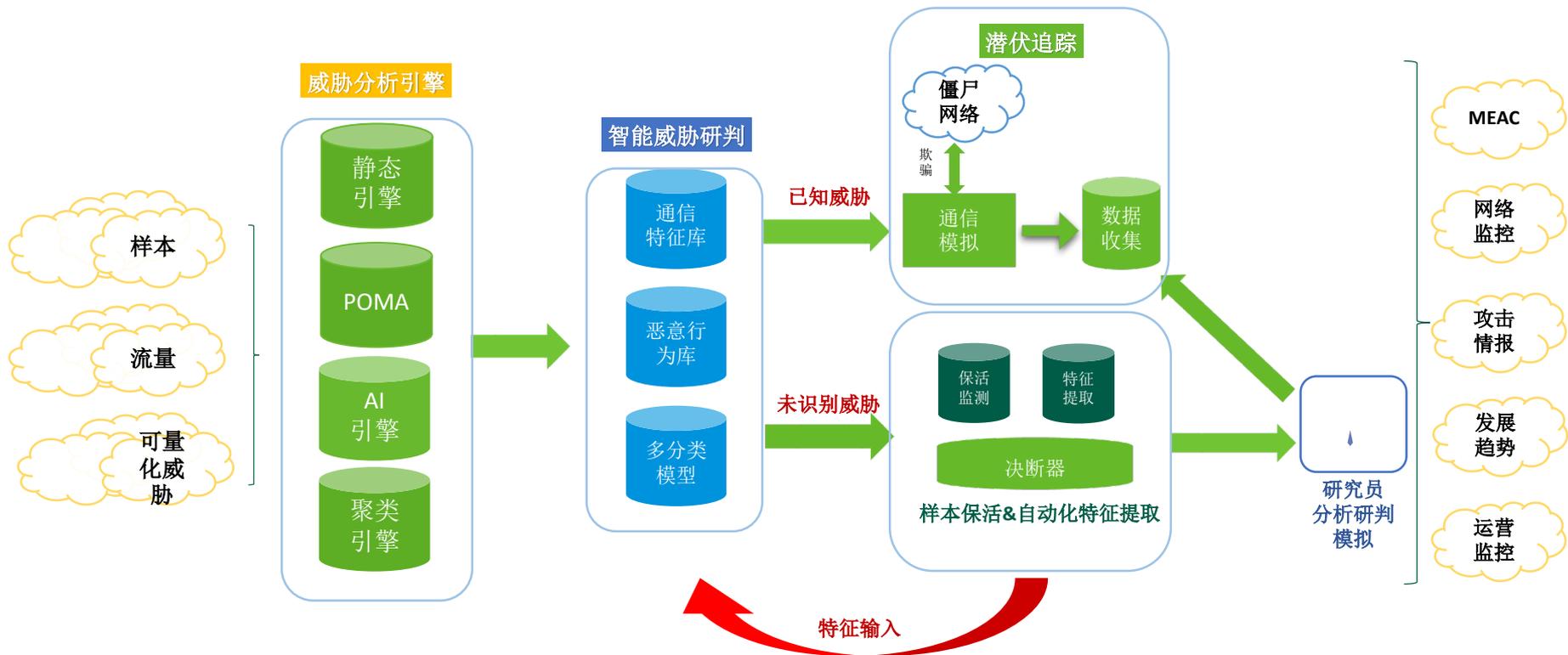


动静结合的精准识别



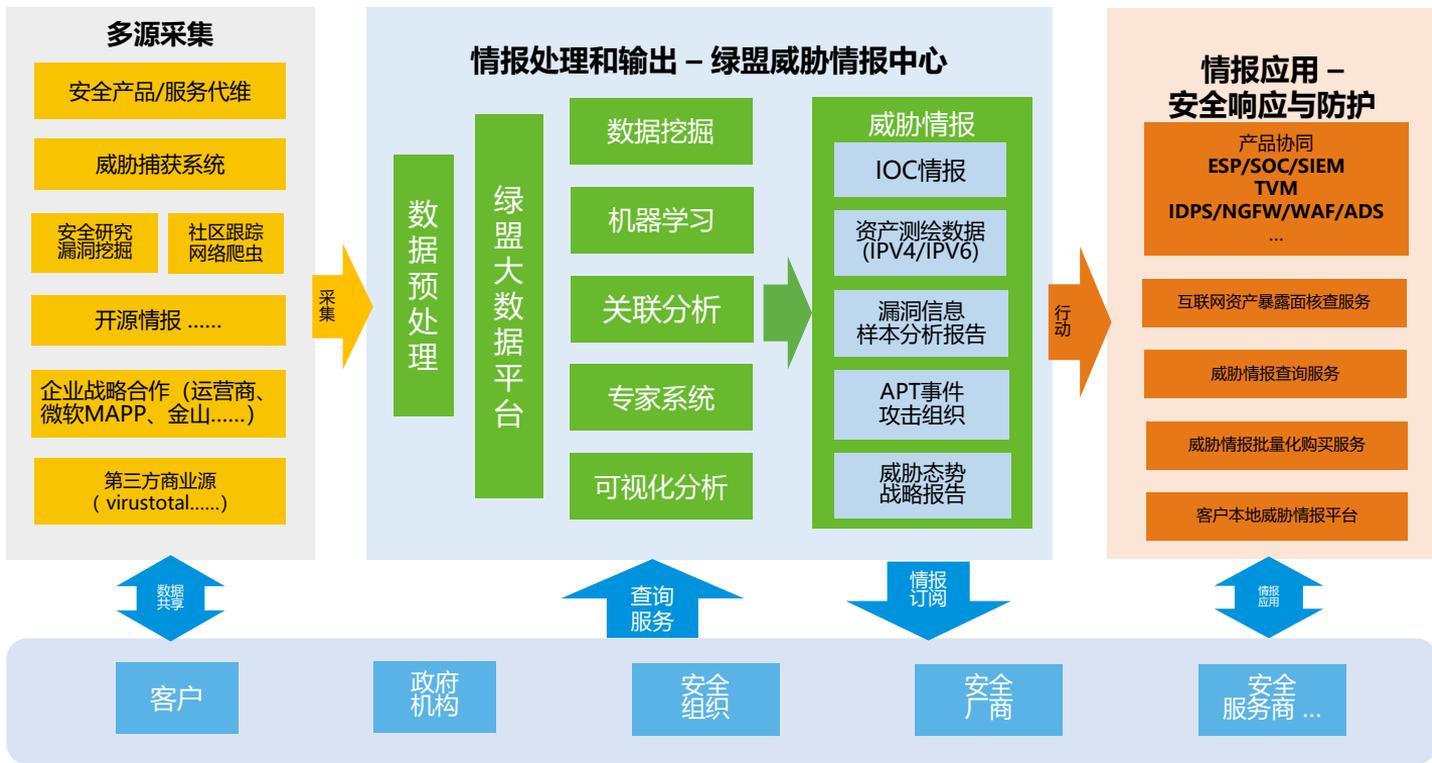
多系统、多协议的仿真僵尸网络节点

# 威胁捕获系统的生产过程





# 威胁情报的生态体系





## 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



对话·交流·合作 前沿·实用·人才

# Thanks

谢谢关注!

