SySCAN+360
I HACK THEREFORE I AM

国际前瞻信息安全会议
INFORMATION SECURITY CONFERENCE
2016.11 · SHANGHAI

机器学习在威胁情报挖掘中的应用

360追日团队
HELIOS TEAM

360追日团队（Helios Team）

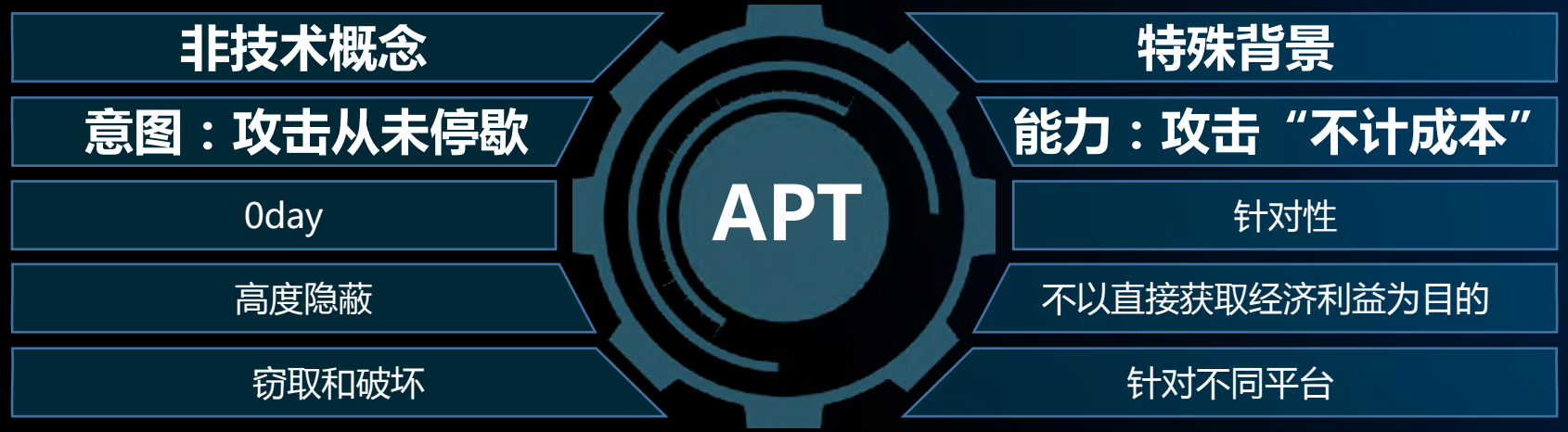
- 专注APT等高级威胁的研究
- 致力于发现和披露更多的APT组织或行动
- 截至目前已发现三十多个APT组织

360追日团队（Helios Team）

360追日团队（Helios Team）

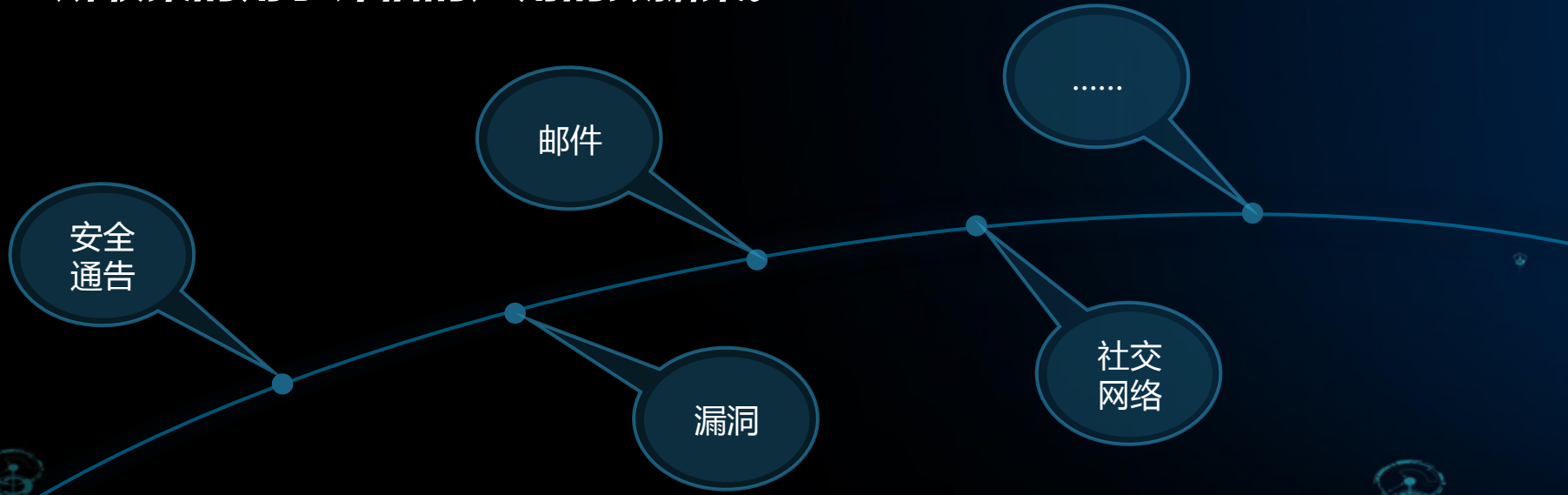
发布时间	报告名称	APT编号
2015.05.29	海莲花：数字海洋的游猎者	APT-C-00
2015.12.10	007黑客组织及地下黑产活动分析报告	
2016.01.18	2015年中国高级持续性威胁（APT）研究报告	
2016.05.30	美人鱼行动——长达6年的境外定向攻击活动揭露	APT-C-07
2016.06.03	SWIFT之殇：针对越南先锋银行的黑客攻击技术初探	APT-C-26
2016.07.01	人面狮行动——中东地区的定向攻击活动	APT-C-15
2016.07.21	台湾第一银行ATM机“自动吐钱”事件分析	
2016.08.04	摩诃草组织——来自南亚的定向攻击威胁	APT-C-09
2016.08.09	关于近期曝光的针对银行SWIFT系统攻击事件综合分析	APT-C-26
2016.08.11	索伦之眼	APT-C-16
2016.11.04	蔓灵花攻击行动简报	

关于定性APT


非技术概念
意图：攻击从未停歇
0day
高度隐蔽
窃取和破坏
APT
特殊背景
能力：攻击“不计成本”
针对性
不以直接获取经济利益为目的
针对不同平台

威胁情报

“针对安全威胁、威胁者、利用、恶意软件、漏洞和危害指标、所收集的用于评估的应用的数据集。”



威胁情报

APT攻击链

威胁情报

- 网络数据异常
- 系统遭到破坏

可观察到的行为

- 威胁处理的条件
- 可能的影响
- 有效时间
- 检测或测试方法

威胁特征指标

- 时间
- 位置
- 日志

事件描述

技术手法

- 恶意攻击的行为
- 采用的工具
- 攻击链

受害者信息

- 受害系统的基本信息
- 被利用的漏洞信息

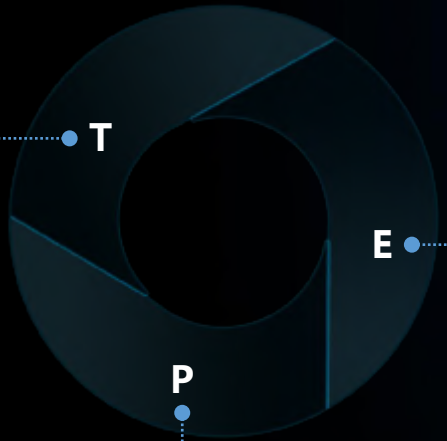
攻击者信息

- 动机
- 幕后背景

威胁情报


Proof
➢ 一种基于证据的描述威胁的一组关联的信息
Threat
➢ 威胁相关的环境信息、采用的手法机制、指标、影响
IOC
➢ 攻击组织
➢ 恶意域名
➢ 恶意文件HASH
➢ URL
➢ 威胁指标之间的关联性
➢ 时间维度上攻击手法的变化
Extend
➢ 其他传统威胁种类
➢ 包括：木马远控、僵尸网络、间谍软件、Web后门等

机器学习



任务

威胁情报

经验

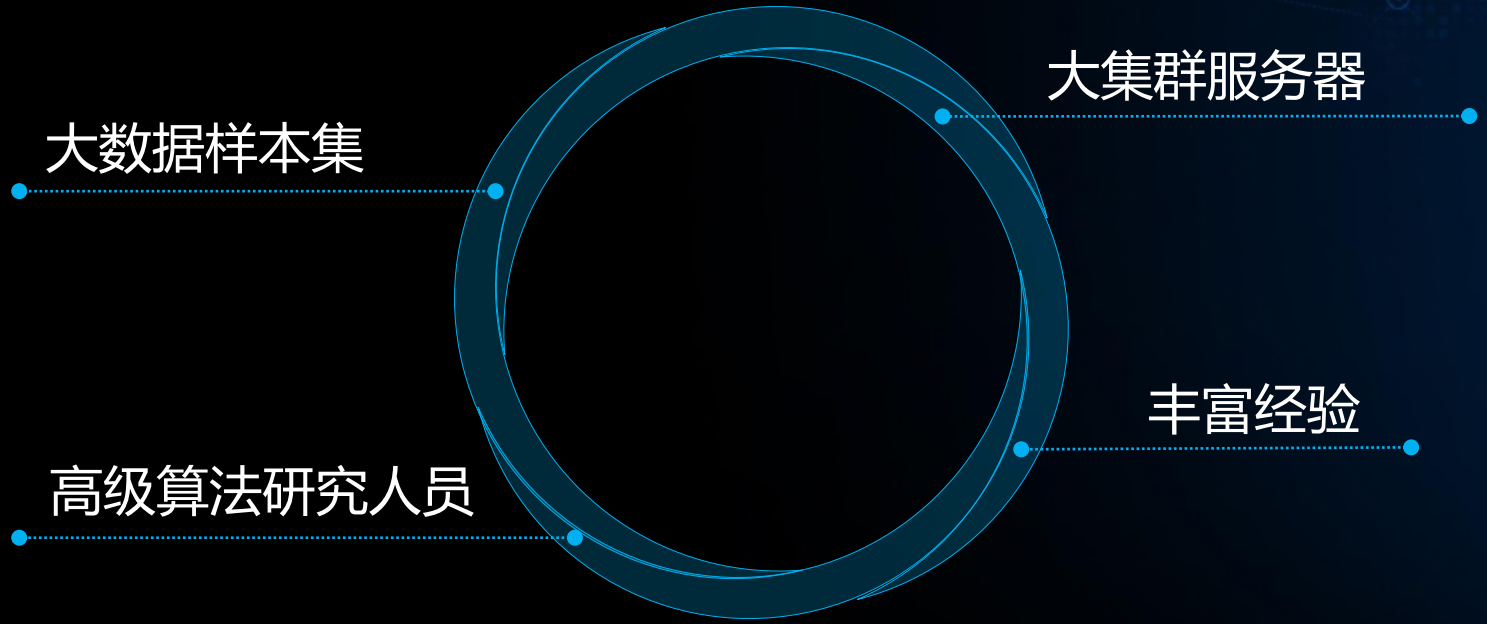
高效、自主、真实

性能

机器学习与威胁情报

- 高效地检测并识别出APT攻击中的恶意载荷
- 提高APT攻击威胁感知系统的效率与精确性
- 实现APT攻击的快速发现和回溯
- 发现和追踪APT攻击的过程中起到了关键性的作用

我们的优势



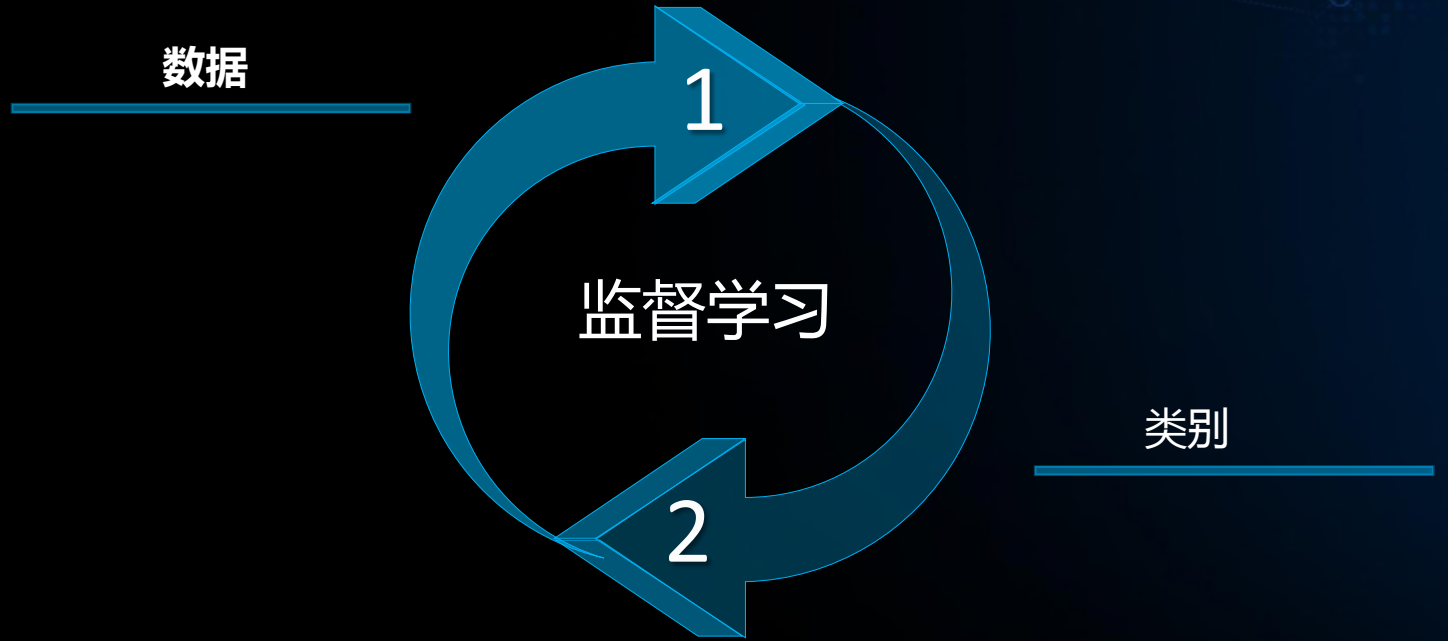
大集群服务器

大数据样本集

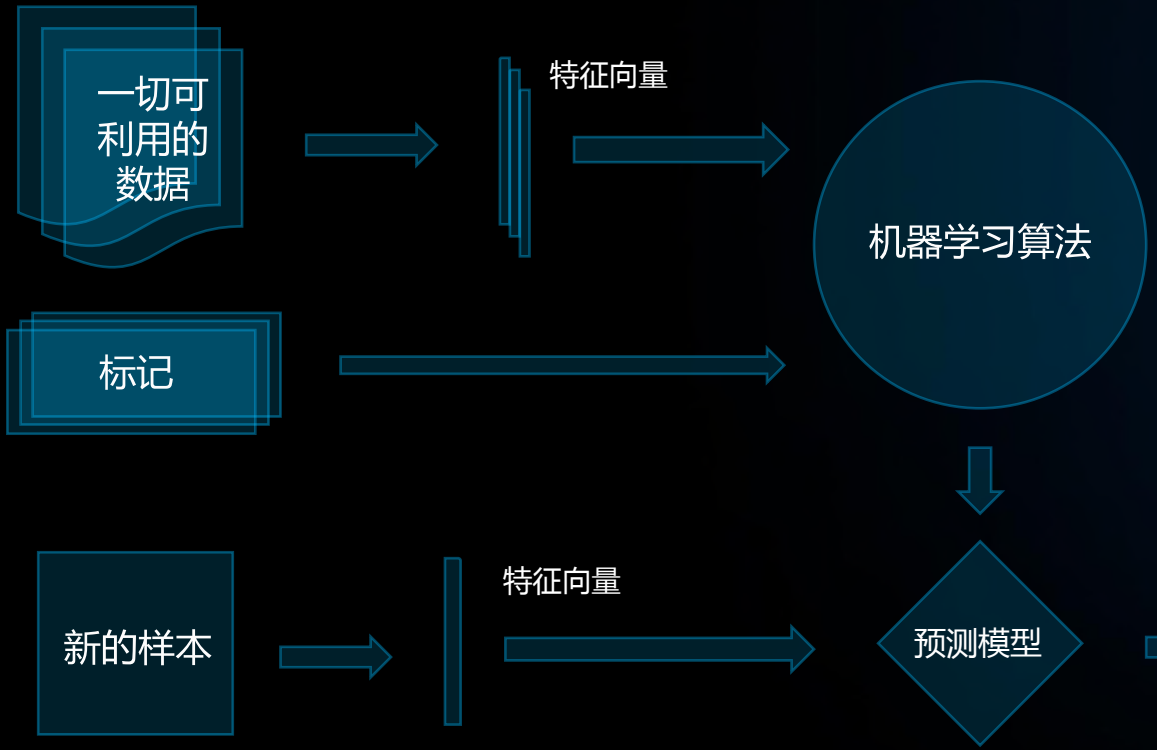
丰富经验

高级算法研究人员

机器学习



一般过程



一般过程

特征抽取与筛选

初始特征集

高效特征

高效特征

高效特征

训练周期—静态特征

PE

特征选取

- 文件描述
- 可执行代码
- 静态数据
- 签名版权
- 附件文件

降维

特征转换

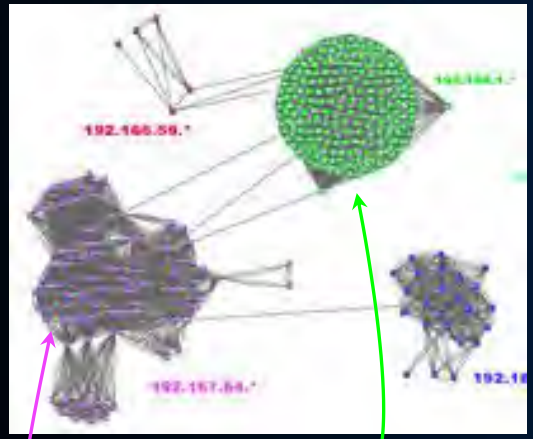
3000+特征维度

亿级海量文件

	维度1	…	维度N
文件a	A1	A…	An
文件b	B1	B…	Bn
文件c	C1	C…	Cn
…	…1	… …	…n
文件n	N1	N…	Nn

PCA算法　LDA算法　LLE算法

检测

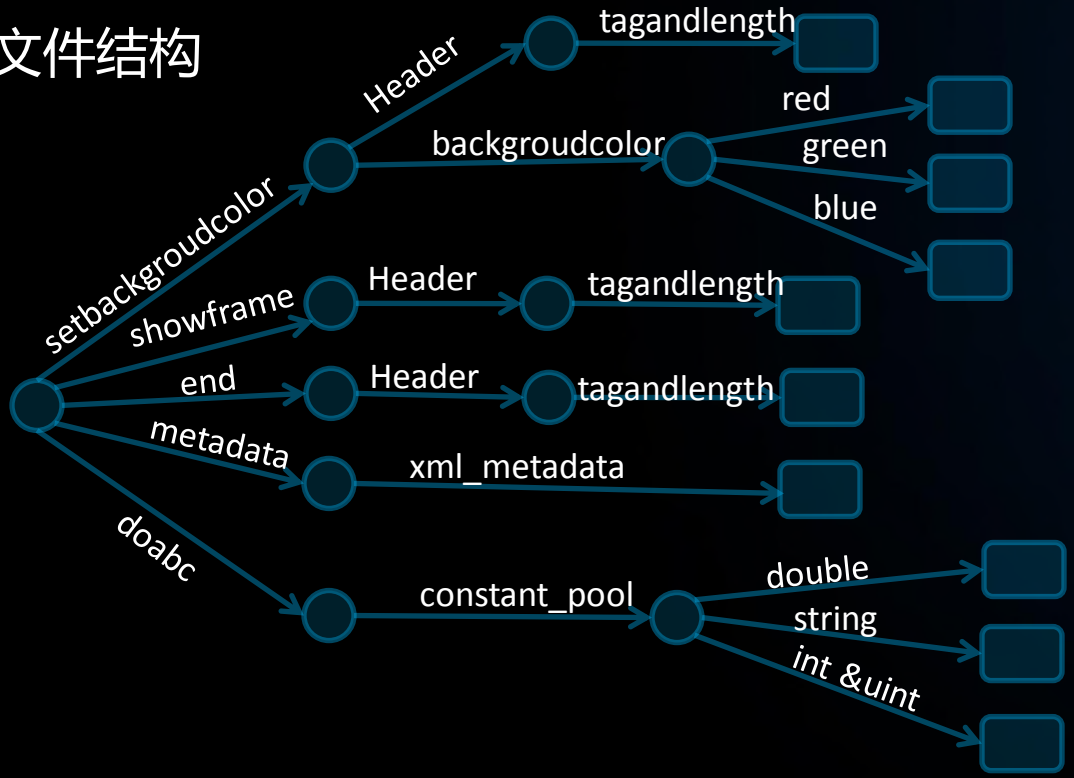


向量机算法　逻辑回归算法　深度学习算法

训练算法

训练周期—静态特征

SWF文件结构

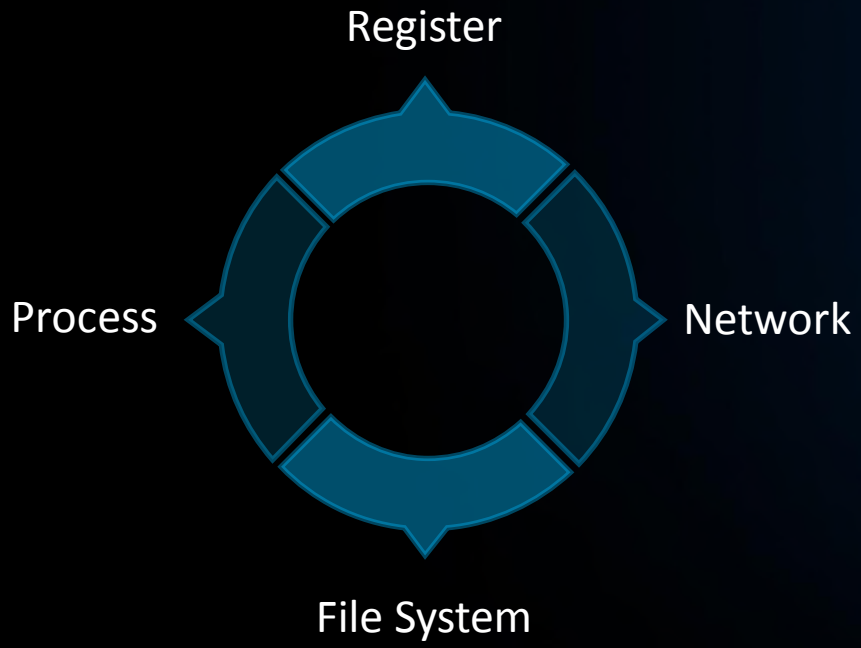


特征总数：428

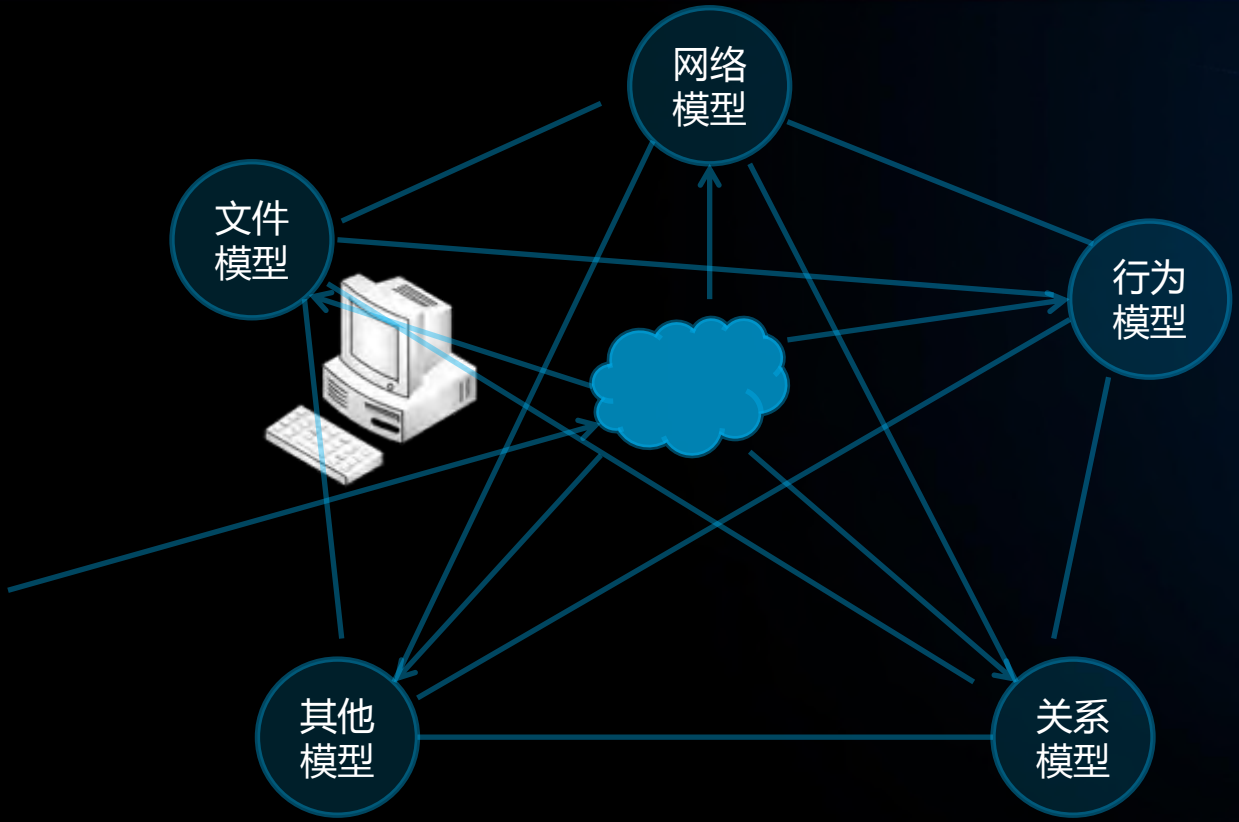
训练周期—静态特征

系统流程设计

训练周期—动态行为



训练周期—动态行为



模型检验

应用

应用


数量
低
高
黑龙江
吉林
辽宁
新疆
内蒙古
北京
天津
河北
宁夏
山西
山东
青海
甘肃
陕西
河南
江苏
安徽
上海
西藏
四川
湖北
重庆
浙江
江西
贵州
湖南
福建
云南
广西
广东
海南

应用


数量
低
高
黑龙江
吉林
辽宁
新疆
内蒙古
北京
天津
河北
宁夏
山西
山东
青海
甘肃
陕西
河南
江苏
西藏
四川
湖北
安徽
上海
重庆
浙江
江西
贵州
湖南
福建
云南
广西
广东
海南

一些思考

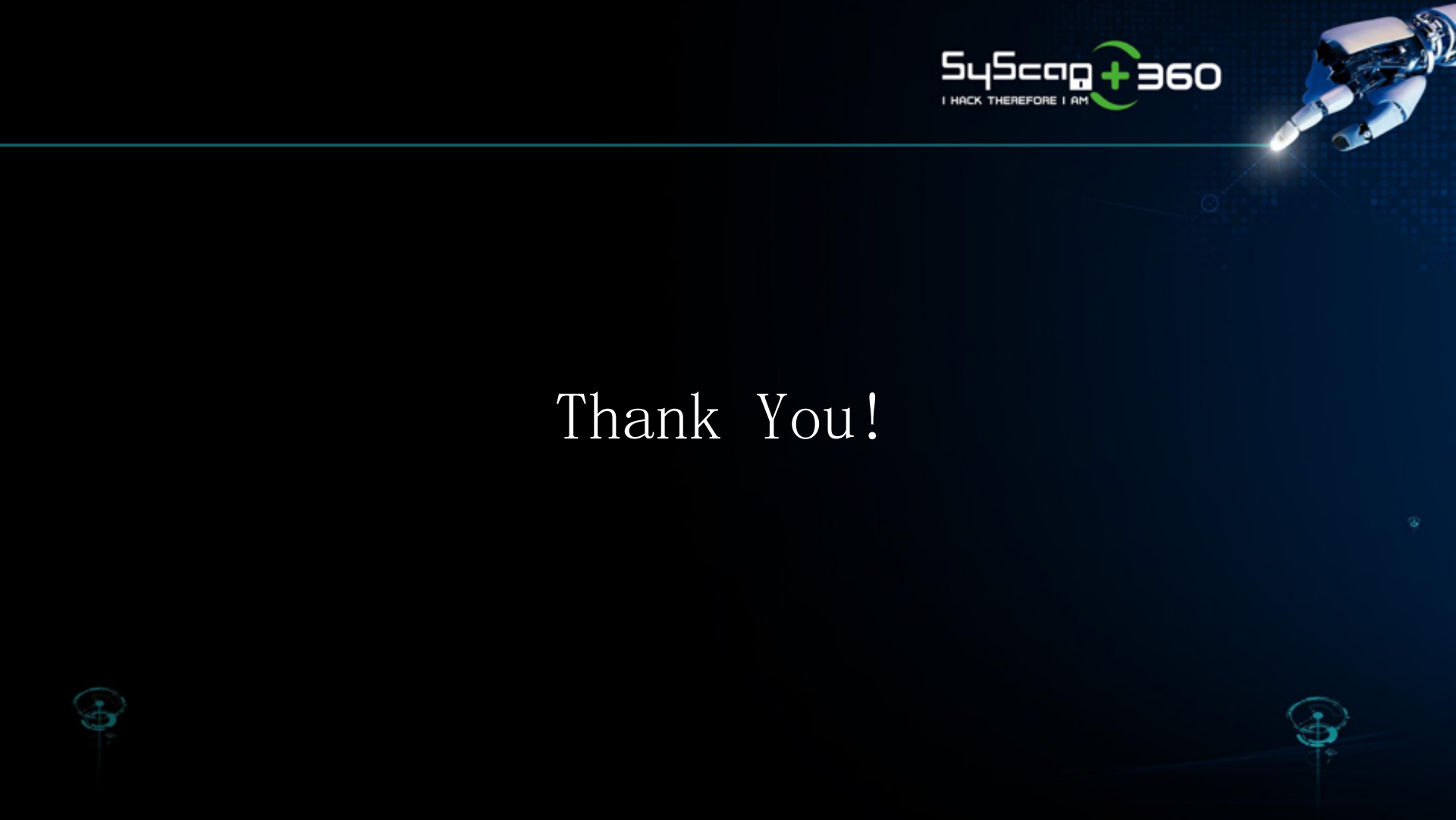
- 机器学习的未来：降噪、降误报
- 交叉验证：多维度、来源和时间
- 协同联动：政府机构、企业用户和安全厂商

联系我们

- 网站： zhuiri.360.cn
- Email： 360zhuiri@360.cn

360追日团队

HELIOS TEAM


Thank You!