网络安全创新大会
Cyber Security Innovation Summit

AISecOps智能安全运营技术体系与实践

张润滋　绿盟科技天枢实验室 高级安全研究员

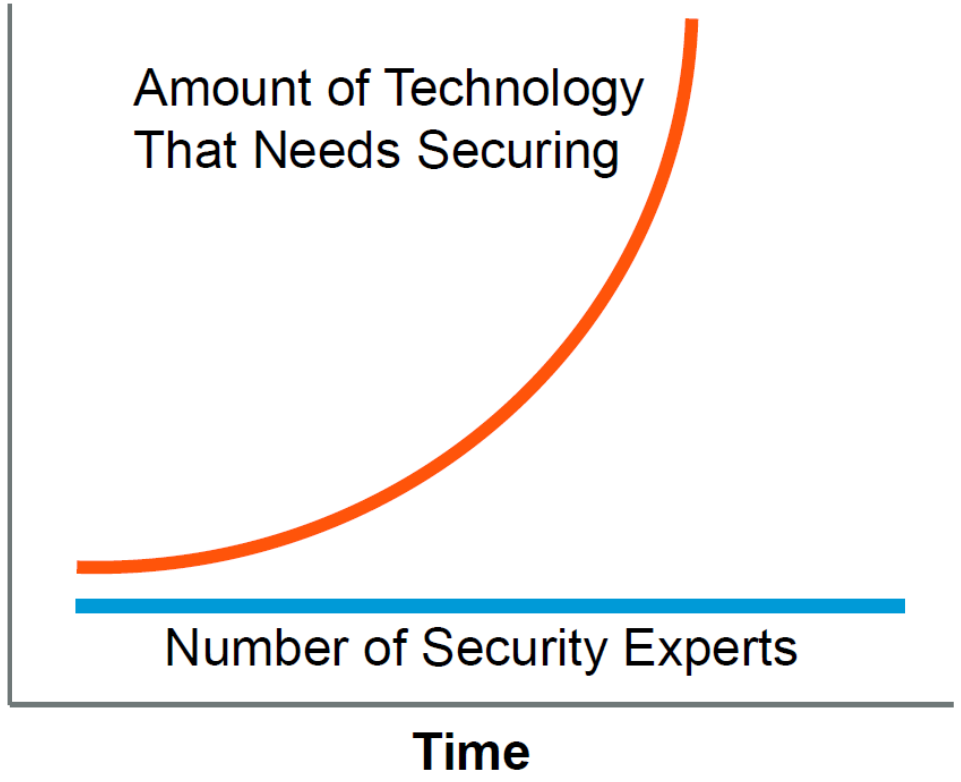
目 录
CONTENTS

01

智能安全运营的机遇与挑战

数据黄金还是数据梦魇?

安全运营(SecOps)迎来挑战



29%，93%

29%的告警得以妥善的调查
93%的企业无法处理当天告警

141 Days

攻击者驻留时间仍不容乐观

335,336,887
15,242,775
80,967

日志，告警，事件

86%

安全运营团队的身心健康
被广泛关注

难拓展：人的经验与知识难复制
难持续：人的精力有限

部分数据摘自：《2020 State of SecOps and Automation》 by dimensional research &《M-TRENDS 2020》 by FIREEYE

安全运营的发展趋势

单点攻防

安全专家即服务，主要应对恶意软件与单点网络事件，点对点技术对抗是核心能力。

边界防御

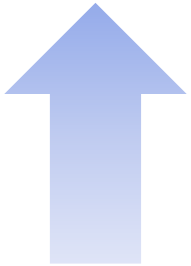
设备和维护即服务，主要应对规模化网络攻击，边界加固拒敌于外是核心能力。

安全运营中心

运营即服务，应对组织化攻击团伙和内部威胁，数据集成、威胁狩猎是核心能力。

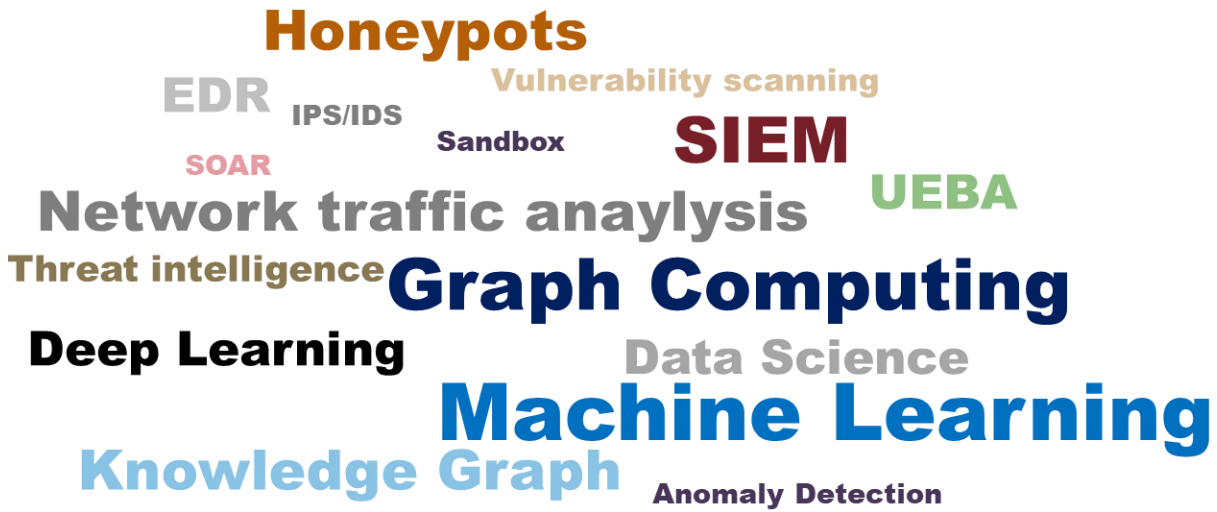
运营智能化

智能运营即服务，应对智能化、武器化高级持续威胁，高自动化、高智能化运营是核心能力。



理想：安全大数据/技术的集成

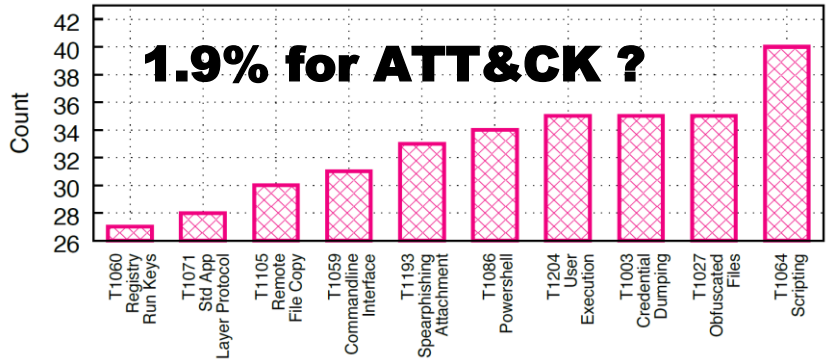
缺乏内在安全机制、隐私防护需求造成系统黑盒



打开网络、终端、模型黑盒看一看高级威胁?

现实：智能安全运营的关键挑战

图片来源：https://blog.paloaltonetworks.com/2019/07/help-soc-analysts-fight-alert-fatigue/



细节与态势并重

- 运营日常是持续降低风险，规模化战役少

数据膨胀与大海捞针

- 低频攻击与高级持续威胁（Stealthy & Slow）
- 系统开销上升

召回模型高误报

- 告警疲劳，事件失焦

依赖爆炸，语义模糊

- 统计相关不同于因果依赖
- 多源异构数据视图难统一

技术/平台低交互、无交互

- 专家经验转化为规则周期长
- 黑盒模型难解释

缺乏鲁邦安全性

- 攻击失效与数据风险

难测量难评估

- 缺乏运营导向的技术指标体系

下图数据来源：《Tactical Provenance Analysis for Endpoint Detection and Response Systems》

02

AISecOps 技术体系

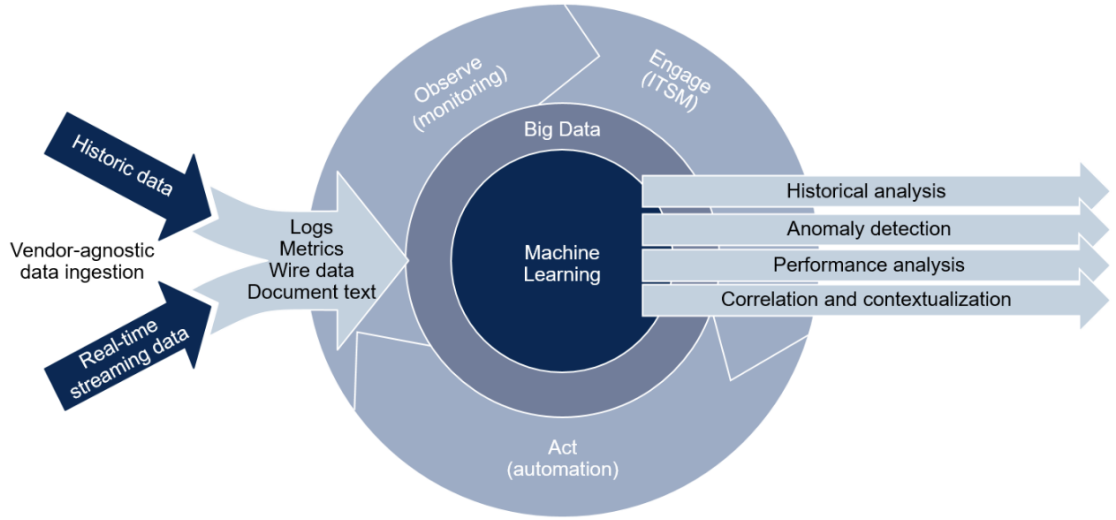
敢问路在何方？

安全运营三要素

SecOps

https://www.securityondemand.com/security-operations/

AIOps Platform Enabling Continuous ITOM



ID: 340492

AIOps

安全与智能

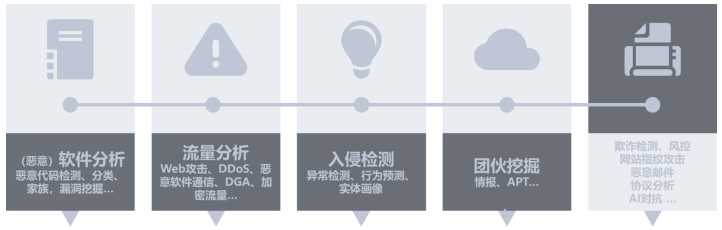

(恶意)软件分析
恶意代码检测、分类、家族，漏洞挖掘...
流量分析
Web攻击、DDoS、恶意软件通信、DGA、加密流量...
入侵检测
异常检测、行为预测、实体画像
团伙挖掘
情报、APT...
欺诈检测、风控
网站指纹攻击
恶意邮件
协议分析
AI对抗 ...

AISec

AISecOps内涵

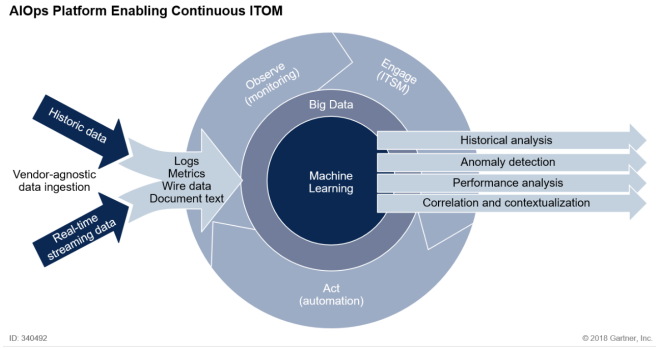
AISecOps

AISec



SecOps

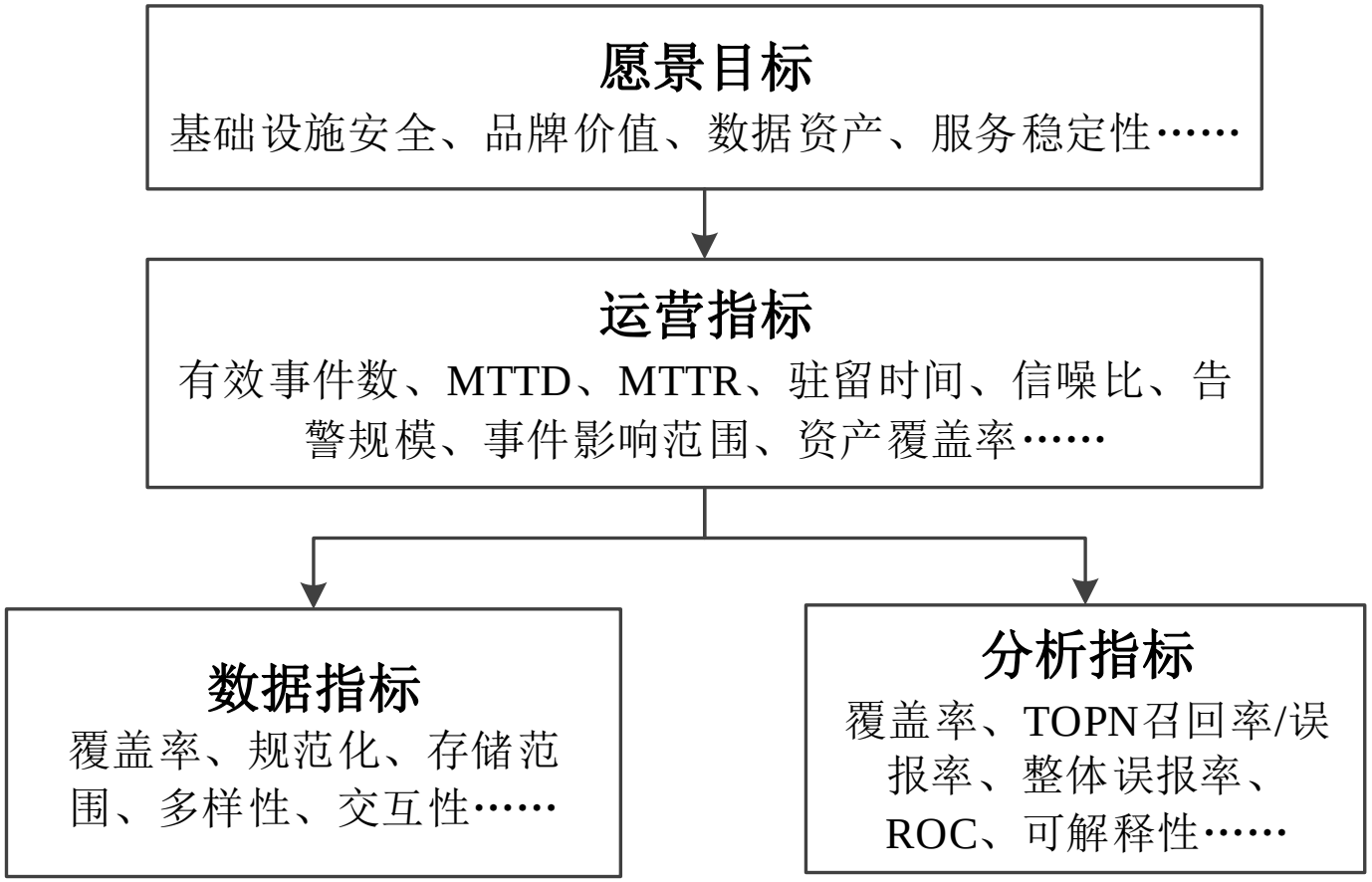
AIOps



AISecOps的四要素

“智能驱动安全运营，以安全运营目标为导向，以人、流程、技术与数据的融合为基础，面向预防、检测、响应、预测、恢复等网络安全风险控制、攻防对抗的关键环节，构建具有高自动化水平的可信任安全智能，以辅助甚至代替人提供各类安全运营服务的能力。”

AISecOps指标体系



技术支持运营，技术自身可运营

AISecOps成熟度矩阵

网络安全创新大会
Cyber Security Innovation Summit

自动化水平	名称	定义	任务阶段									数据交互(DIKW模型)
			感知阶段		认知阶段			决策阶段		行动阶段		
			识别	检测	关联	溯源	预测	评估	制定	响应	反馈	
L0	无自动化	由运营人员全权完成安全运营操作										数据采集
L1	运营辅助	自动化运营系统完成感知、认知、决策中的多个子任务，其他运营操作由人完成										数据集成 信息加工
L2	部分自动化	自动化运营系统针对指定初级任务完成感知、认知、决策、行动全流程子任务，与运营人员进行持续数据交互										信息融合 知识获取
L3	有条件自动化	自动化运营系统完成包含行动层子任务在内的全流程子任务，运营人员须在关键阶段提供适当应答										
L4	高度自动化	在限定场景下，自动化运营系统完成包含行动层子任务在内的全流程子任务，运营人员不一定提供应答										知识理解 知识沉淀
L5	完全自动化	在所有场景下，自动化运营系统完成包含行动层子任务在内的全流程子任务，运营人员不一定提供应答										

完全运营人员完成 → 无运营人员参与

横向覆盖，纵向分级

AISecOps数据体系

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[illegible]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

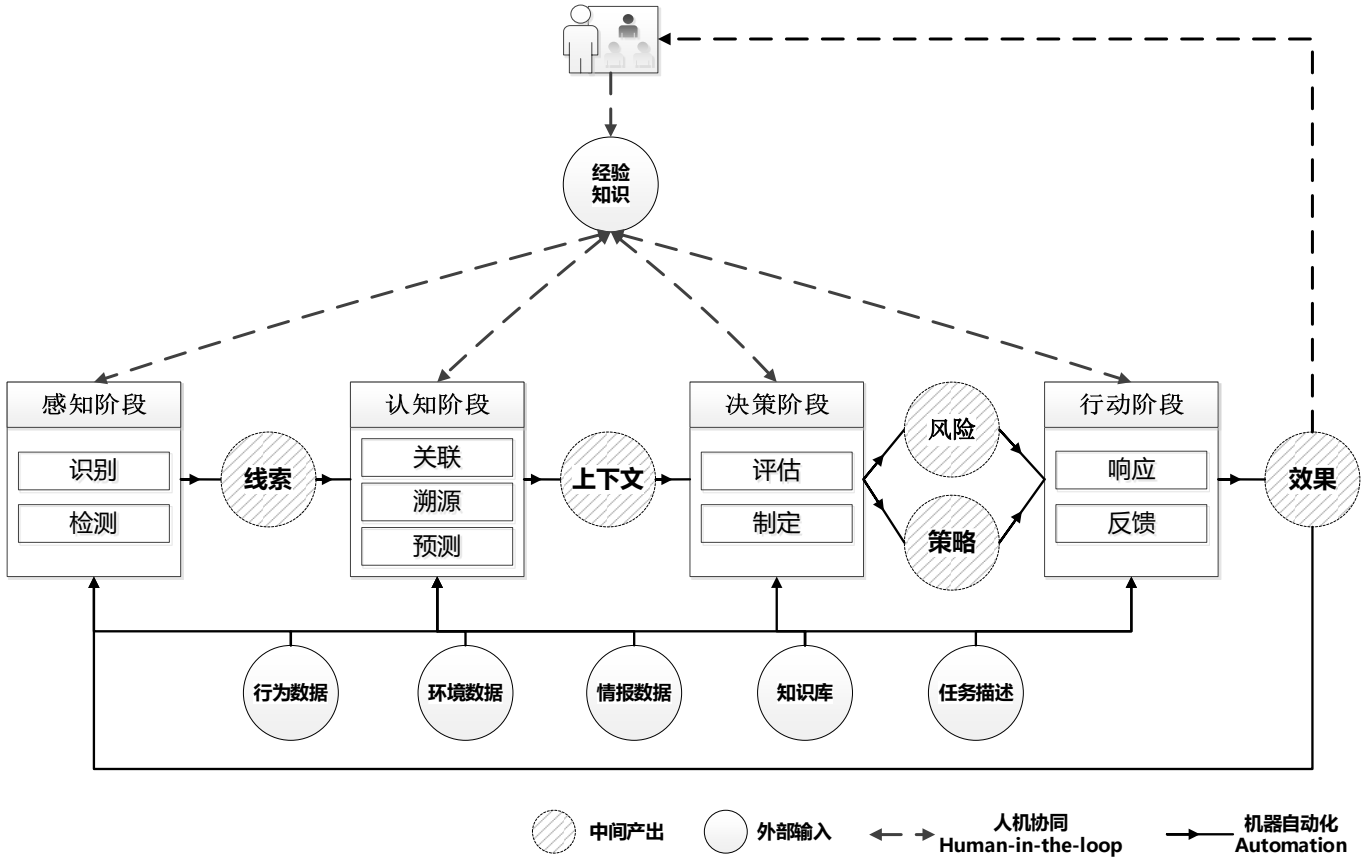
情报数据图

威胁情报及关联

时效性较强的、特定领域威胁情报数据

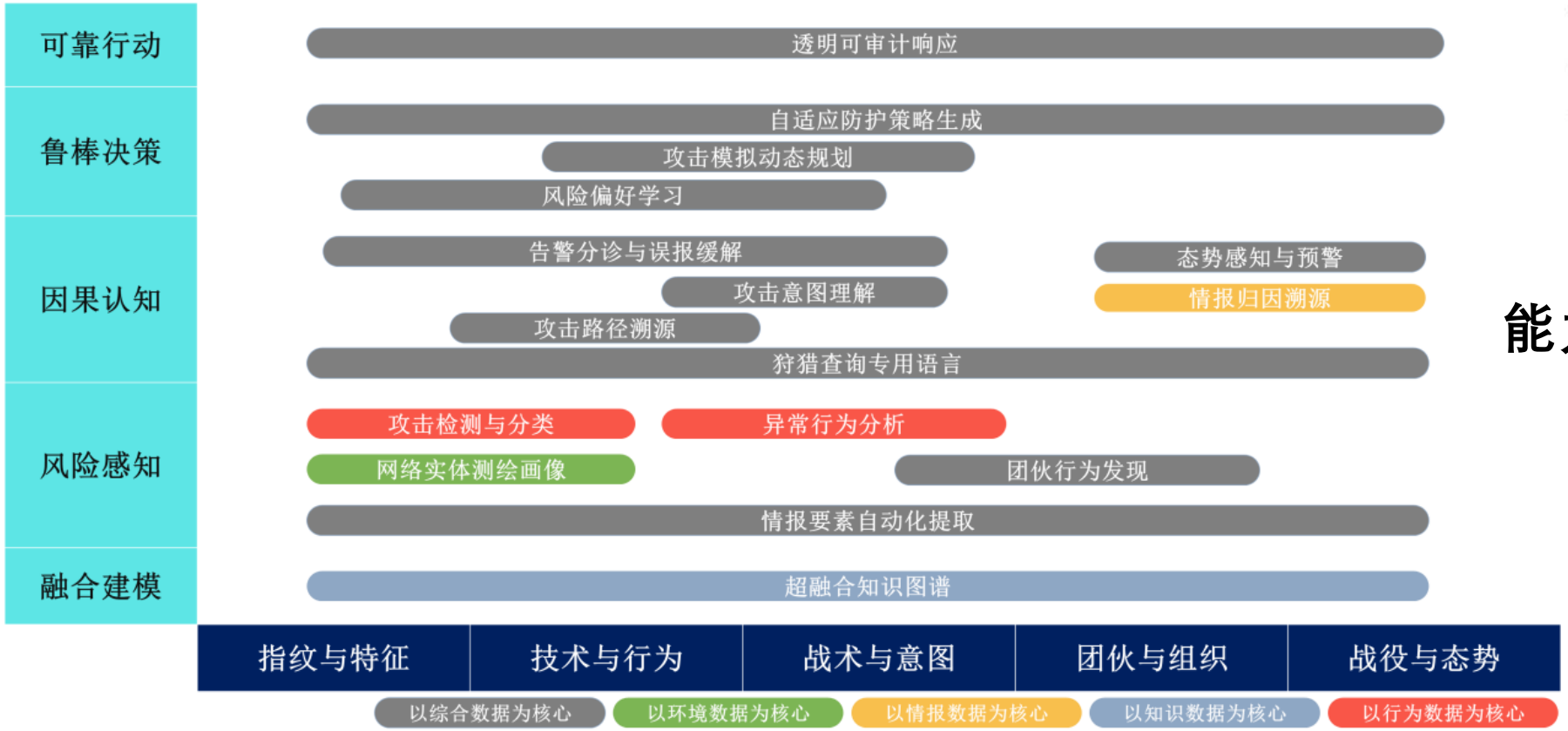
规范化/标准化/全局化
支持数据联动

AISecOps技术框架



人机协同闭环
支持机器自动化闭环

AISecOps前沿技术图谱



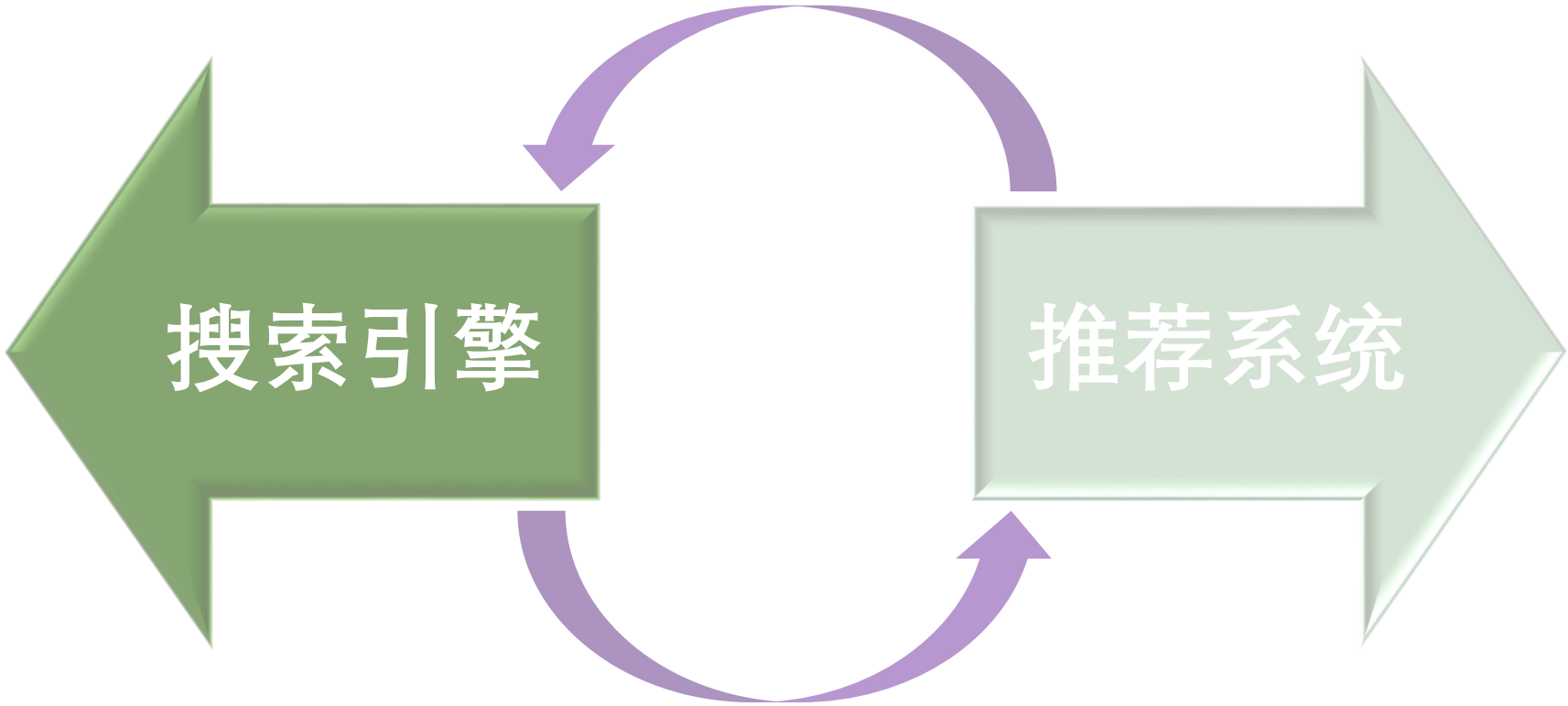
能力抽象而非算法绑定

03

AISecOps 技术实践

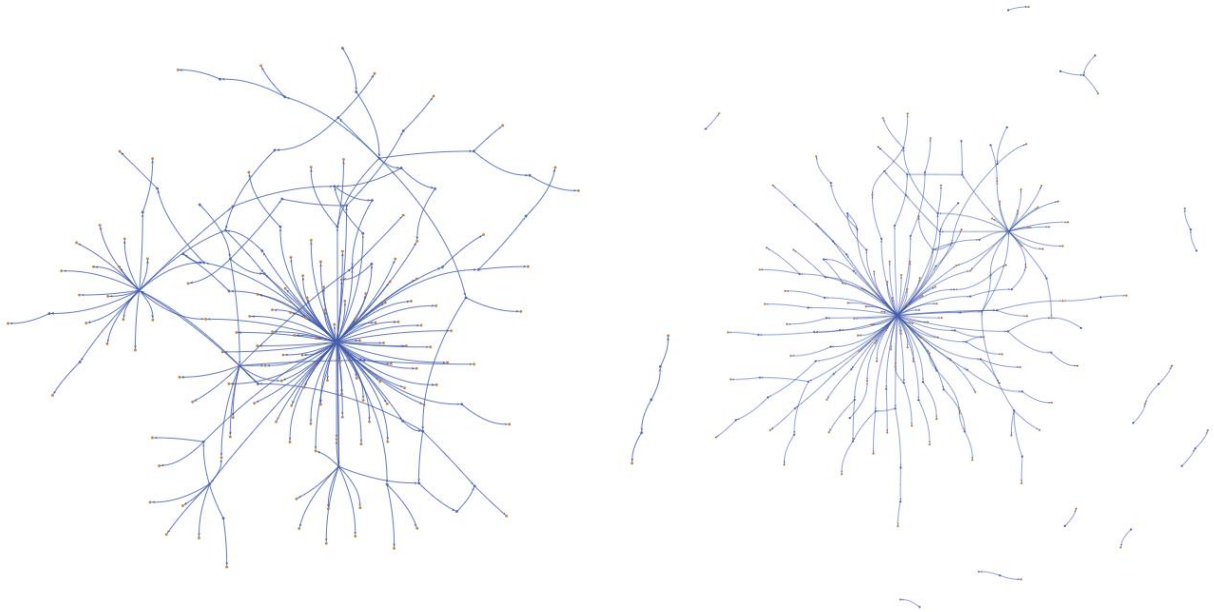
路在脚下

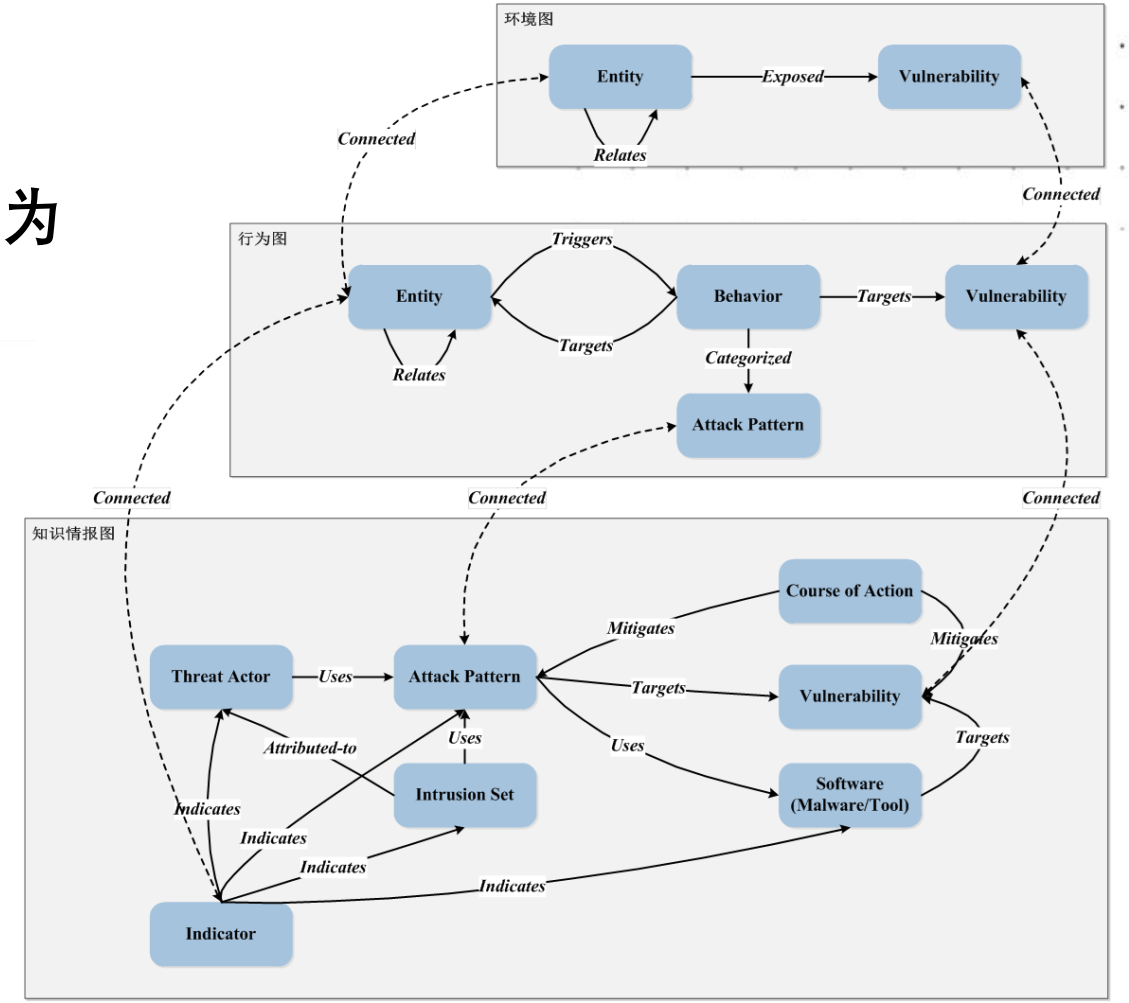
运营数据挖掘挑战本质
攻防不对称导致的信息爆炸



ContexGraph：超融合知识图谱

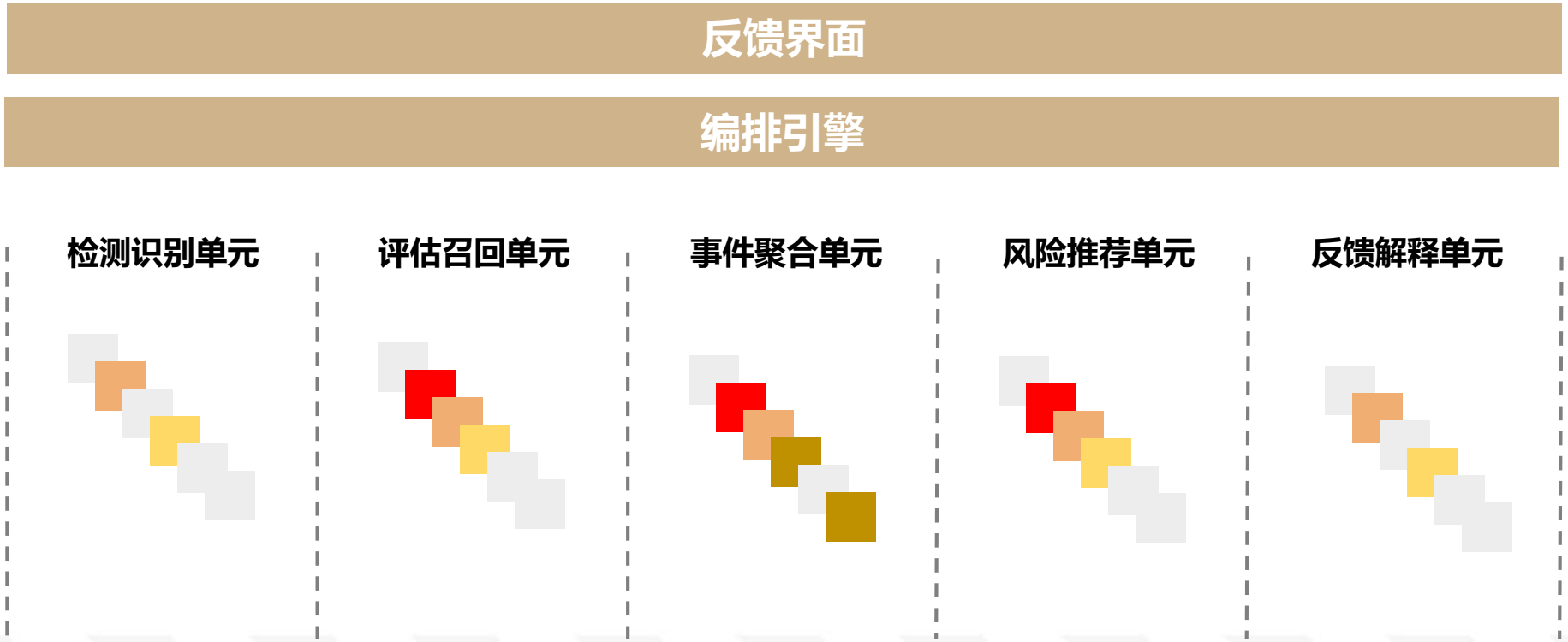
统一本体设计，任何子图节点/边都可以成为已知线索搜索入口





FocusRS：可编排推荐引擎

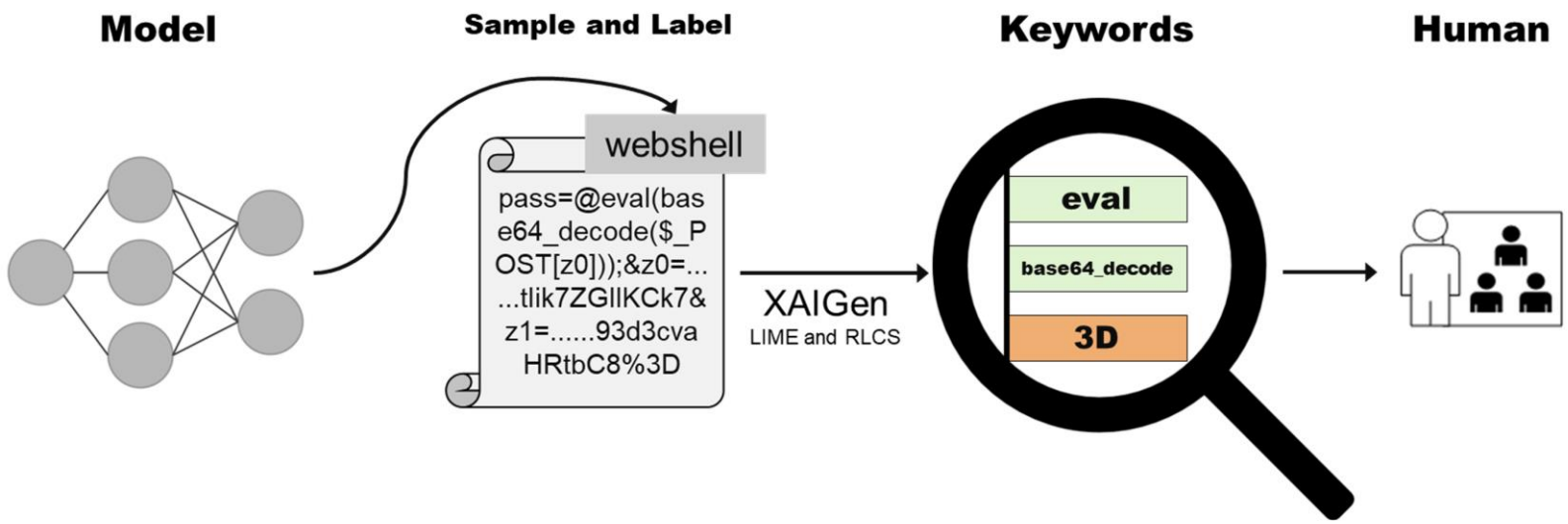
数据驱动的方式学习专家的潜在风险偏好
支持未知风险事件评级



详见XCON 2020：《打造风险驱动的智能威胁推荐引擎》张润滋

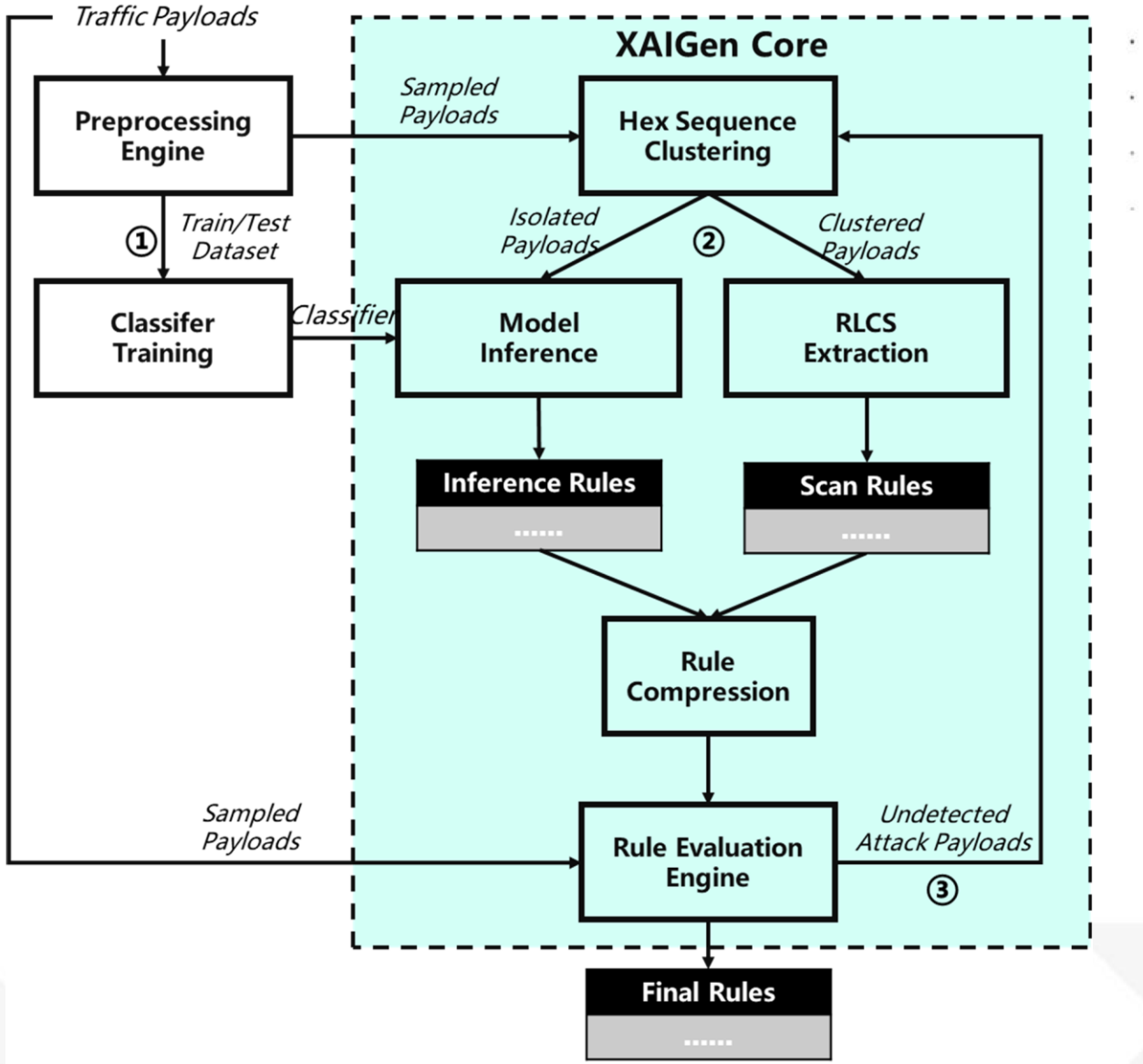
XAIGen：规则提取引擎

授之以鱼，不如授之以渔。
数据驱动的提取模型知识，支持已知威胁分析



XAIGen：规则提取引擎

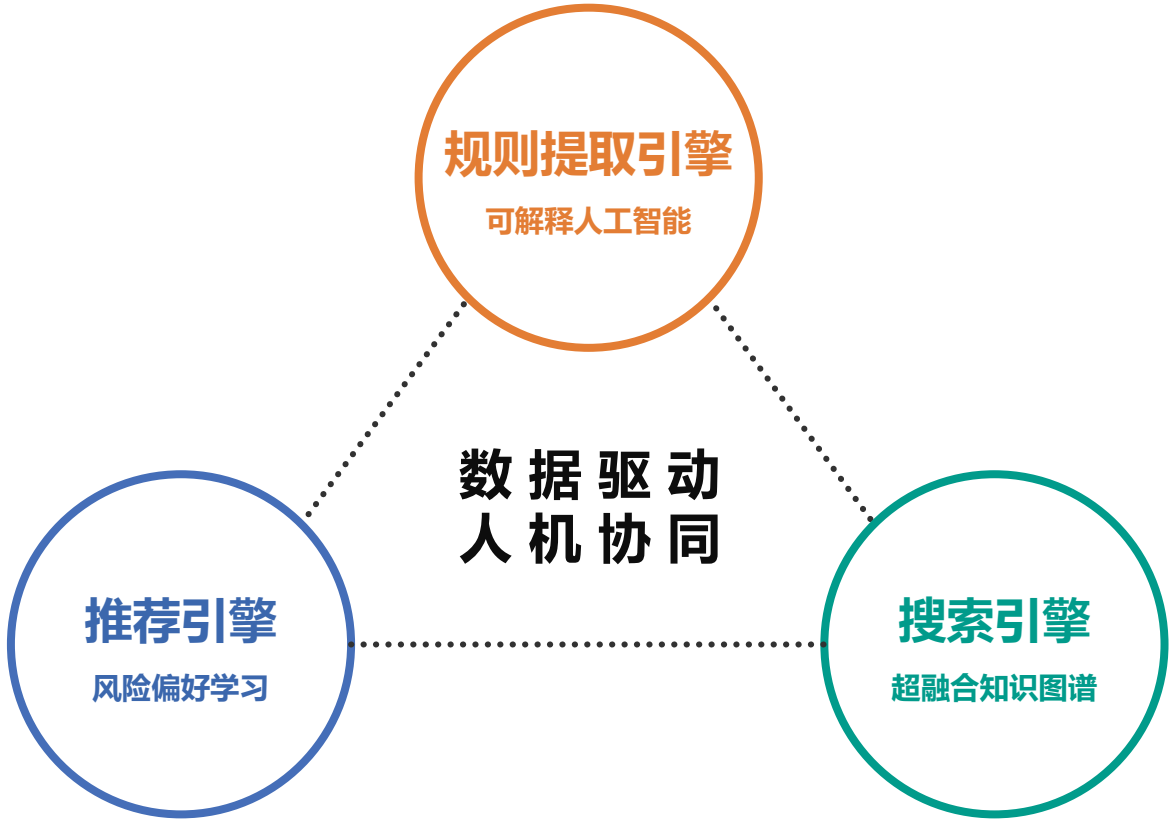
同时针对同质载荷与异质载荷
提取关键词特征



应对信息过载，降低已知与未知风险

决策解释与知识抽取

搭建数据规律与安全语义转化的桥梁



风险排序与运营反馈

提升专家经验与模型算法融合的效率

威胁狩猎与知识固化

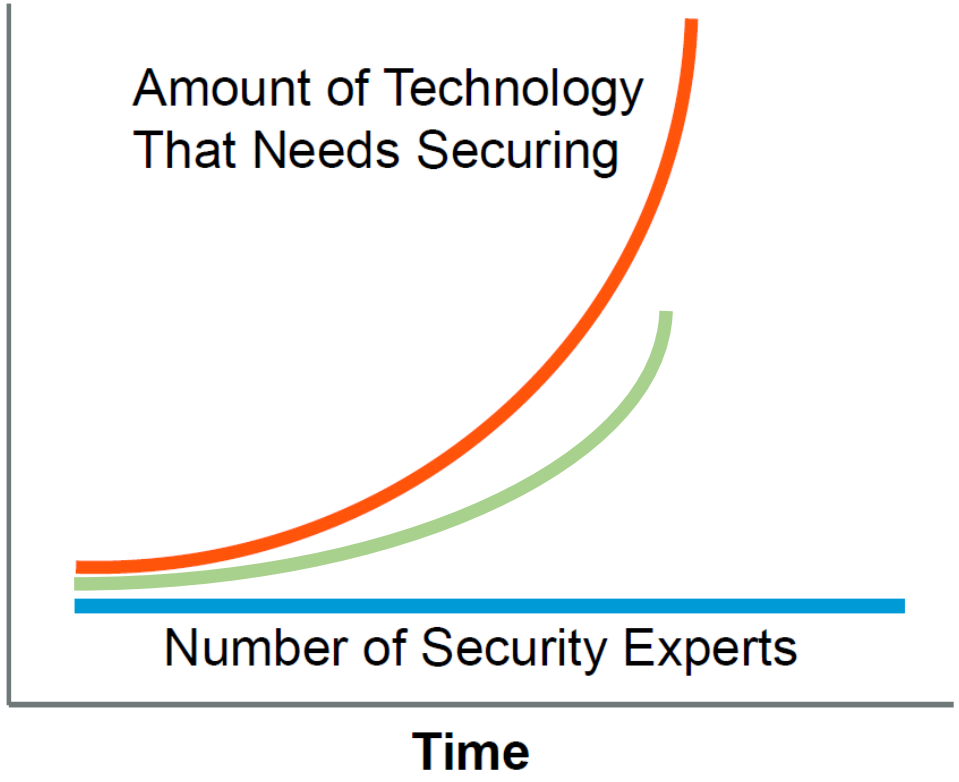
降低动、静态多层次数据统一分析的成本

02

总结与展望

打造可信任安全智能

AISecOps: 智能化是手段，自动化是目标

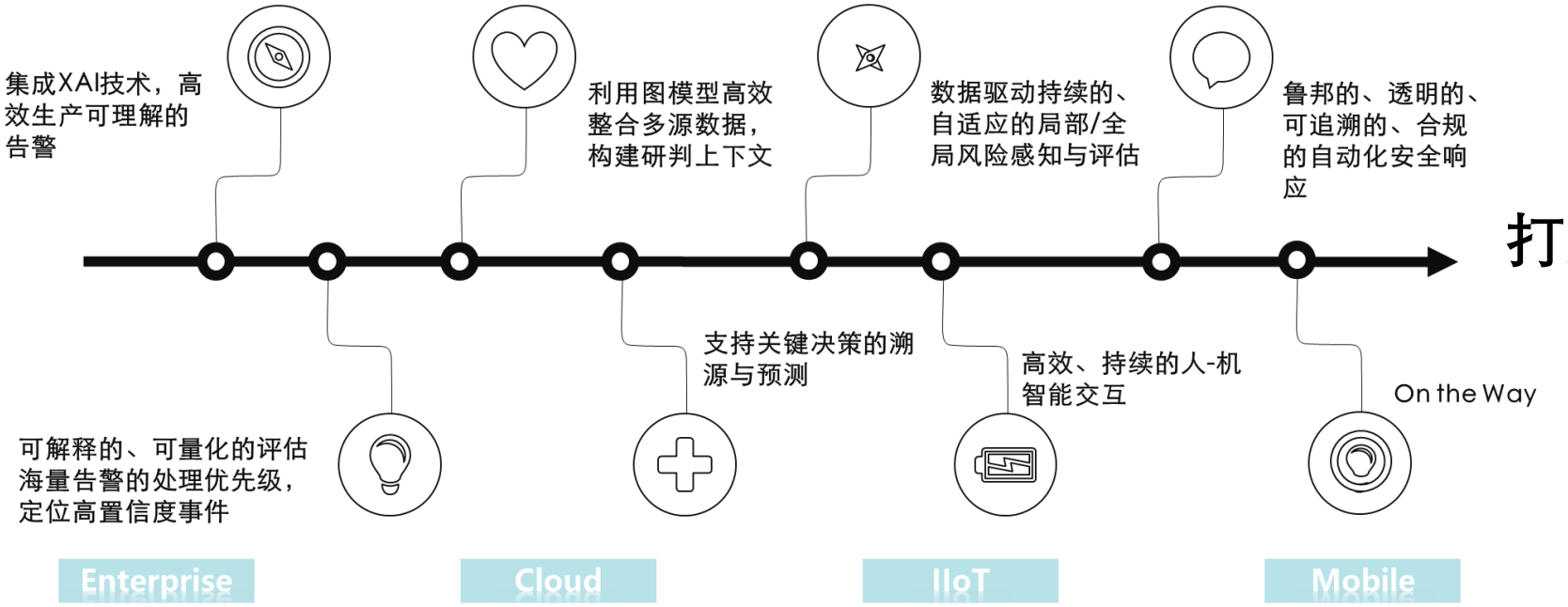


可拓展：人的经验与知识难复制，机器智能可量产
可持续：人的精力有限，机器智能7×24值守

AISecOps技术路线

网络安全创新大会
Cyber Security Innovation Summit

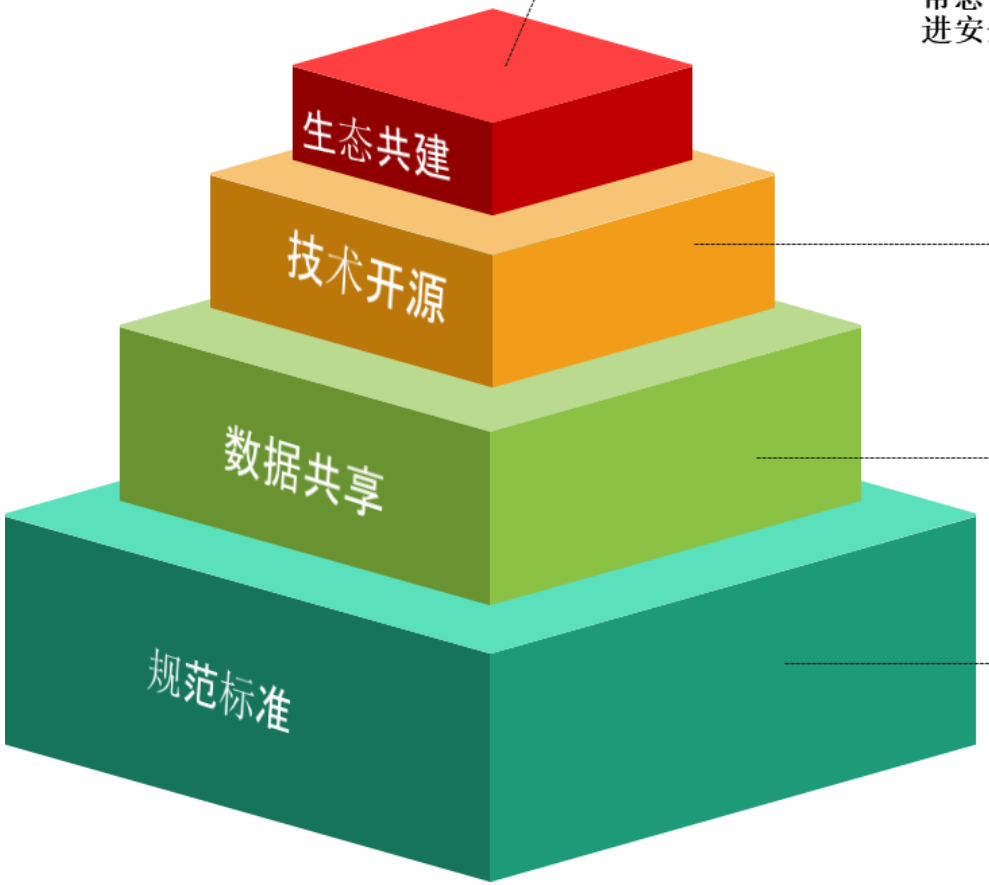
预测性能 | 可解释性 | 安全性 | 合法合规 | 可审计 | 道德约束



打造可信任的安全智能战友

(平台、技术、模型、算法...)

AISecOps技术生态构建



生态促持续

常态化的技术沟通、竞赛、集成机制，促进安全运营多方、多角度持续互动

开源助燃剂

体系共享，技术开源，提升安全运营技术透明度、可信度、鲁棒性

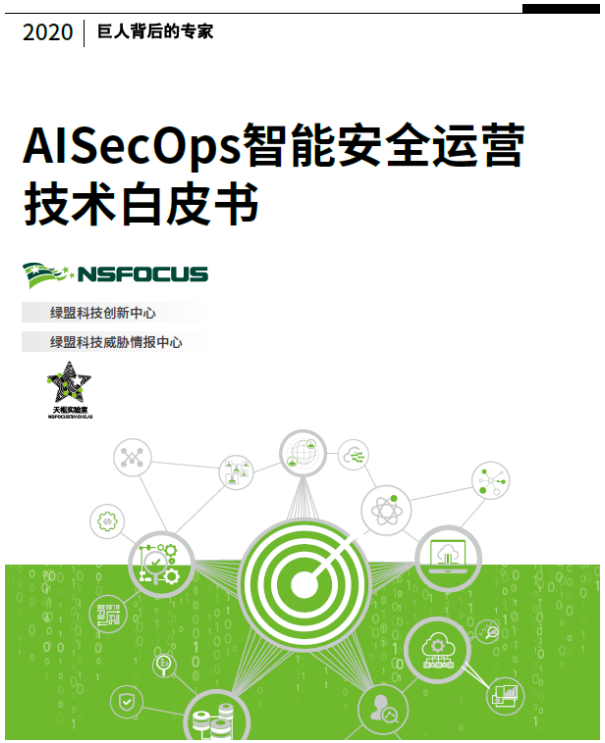
数据筑基石

巧妇难为无米之炊，运营数据共享促进技术迸发

标准打基础

技术元语共建，运营体系接口对齐，促进技术、流程、人的持续融合

分享与开源



《AISecOps智能安全运营技术白皮书》

README.md

XAIGen

Introduction

This project is about extracting signature rules from malicious payloads and texts to help understand and strenthen predictions of machine learning black box models. XAIGen leverages both optimized sequence similarity based and black-box model inference based methods (such as LIME) to extract patterns from homogeneous and heterogeneous text payloads respectively. Such rules can be applied to the detection on malicious intrusion, DDoS attack, sensitive data, spam email etc. XAIGen is able to improve the efficiency of rule extraction and free hands of security experts, improve the interpretable interaction ability of security operation products and platforms, and then enhance the level of automation.

Installation

XAIGen now support Python 3.6 and we suggest run it in your own virtual environments. The following commands are to prepare the execution environment.

git clone https://github.com/oasiszrz/XAIGen.git

pip install -r requirements.txt

Test with Notebooks

XAIGen项目已经开源，项目地址：
https://github.com/oasiszrz/XAIGen

网络安全创新大会
Cyber Security Innovation Summit

THANKS

绿盟科技研究通讯公众号：nsfocus_research

个人微信号：oasiszrz