安全运营中
ATT&CK框架的实用性挑战与应对

—— 威胁检测溯源维度

绿盟科技 天枢实验室 张润滋

NSFOCUS

目 录
CONTENTS

NSFOCUS

01

ATT&CK 框架带来新机遇

词典化与语义抽象的力量

NSFOCUS

ATT&CK关键词

MITRE

APT

实战

Behavior

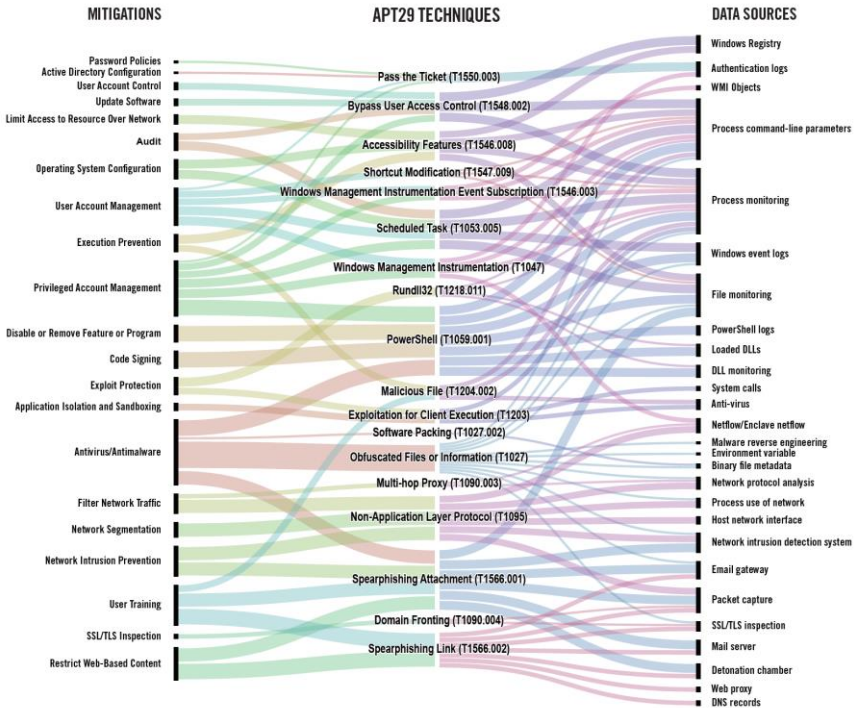
XDR

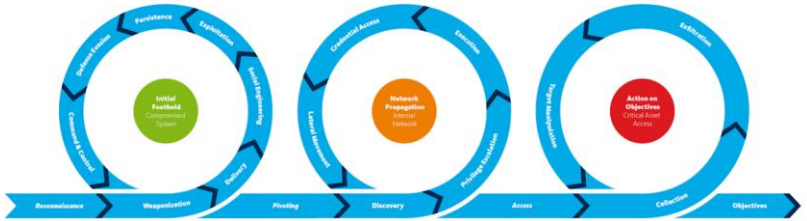
威胁情报

NSFOCUS

机遇

- MITRE通过开源众筹的ATT&CK知识库，以**适中的抽象方法**，较成功的实现了系统化的攻击者技战术行为建模，有效的降低了威胁情报、威胁建模等领域的沟通成本。
- 传统威胁分析能力的建设是大家在各自的语境方言里自说自话，那么**ATT&CK就给出了一个词典基线**，识不识字、能力强弱的问题大家对齐语义就可以拿出来比一比了





机遇

数据归一化、本体化及关联性提升

•ATT&CK矩阵为企业或组织内数据湖的数据融合提供了**技战术抽象层次的对齐方案。**基本的，类似告警或事件有了明确的归类层次。进阶的，数据中隐含的数据实体及其关联关系，能够在统一的框架下实现本体化建模，**为知识图谱等基于网络和图的数据结构的构建提供基础。**

促进分析能力与业务的解耦

•**通用算法能力能够从传统的数据分析孤岛中抽象出来，并与上一层的安全业务需求解耦。**例如，经典的序列分析模型可用于事件预测、异常检测等不同层次的场景。在统一的数据湖之上，分析算法能够充分模块化，形成可编排的调用接口以供灵活的调用与集成。

促进分析算法的语义化

•ATT&CK通过矩阵的战术阶段划分，在目标层、分析层以及数据层上自然的提供了有明确语义的关联关系。这一语义增强，**给数据驱动威胁分析结果提供了讲故事的范本**，为运营人员提供了可解释、可理解的线索入口。

安全运营中ATT&CK实用性挑战

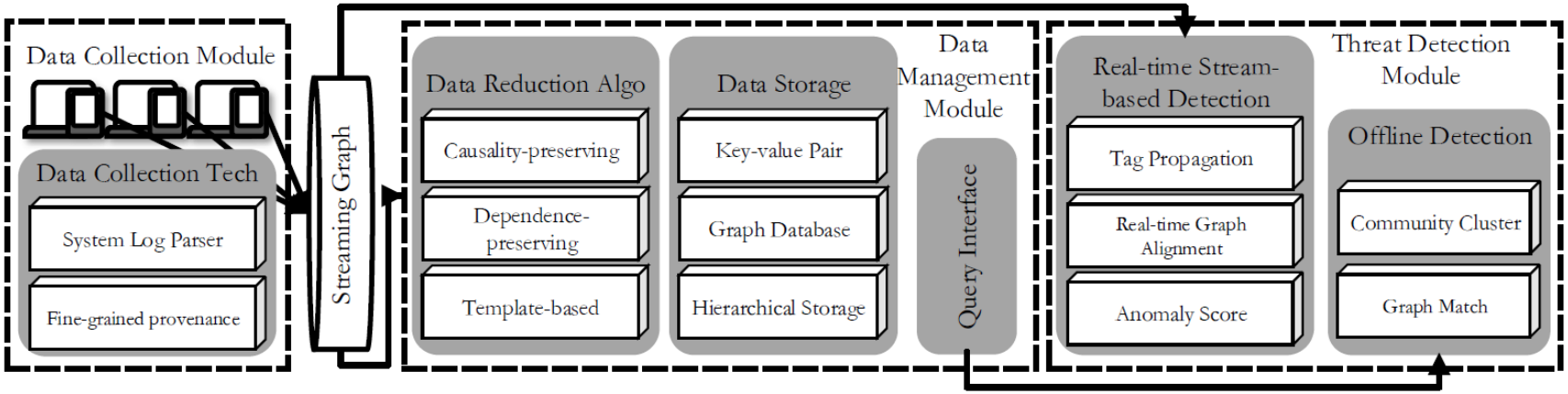
02

实战中的困境

NSFOCUS

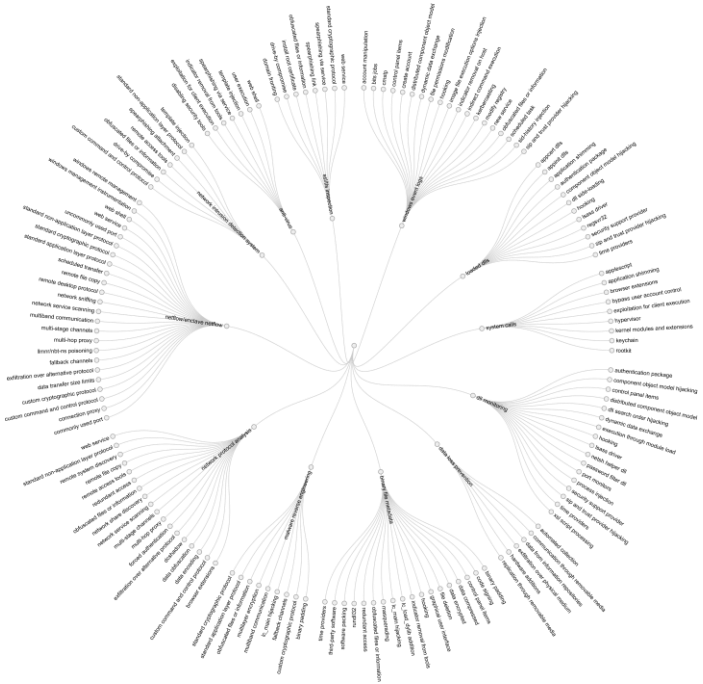
挑战1：采集与分析系统瓶颈

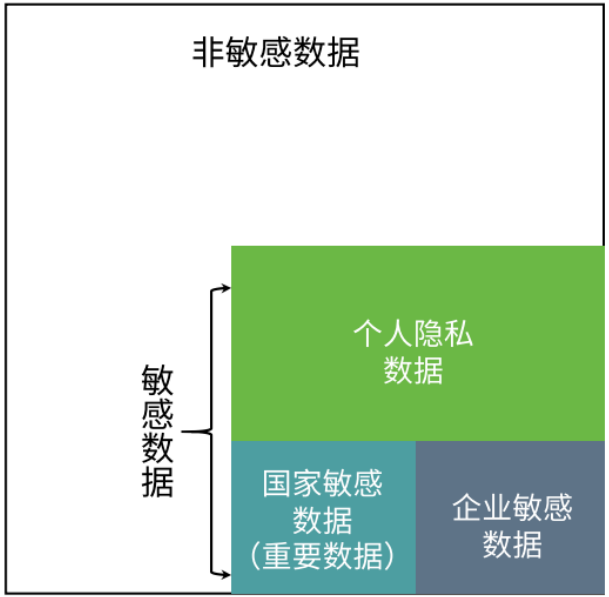
- 理想：全面收集丰富的指标数据，支撑威胁研判与溯源
- 现实：高级威胁低频且具有隐匿性与企业和组织需要持续进行风险管控的矛盾，导致大规模数据采集开销、传输开销、存储开销、分析开销大幅提升



挑战2：数据隐私风险

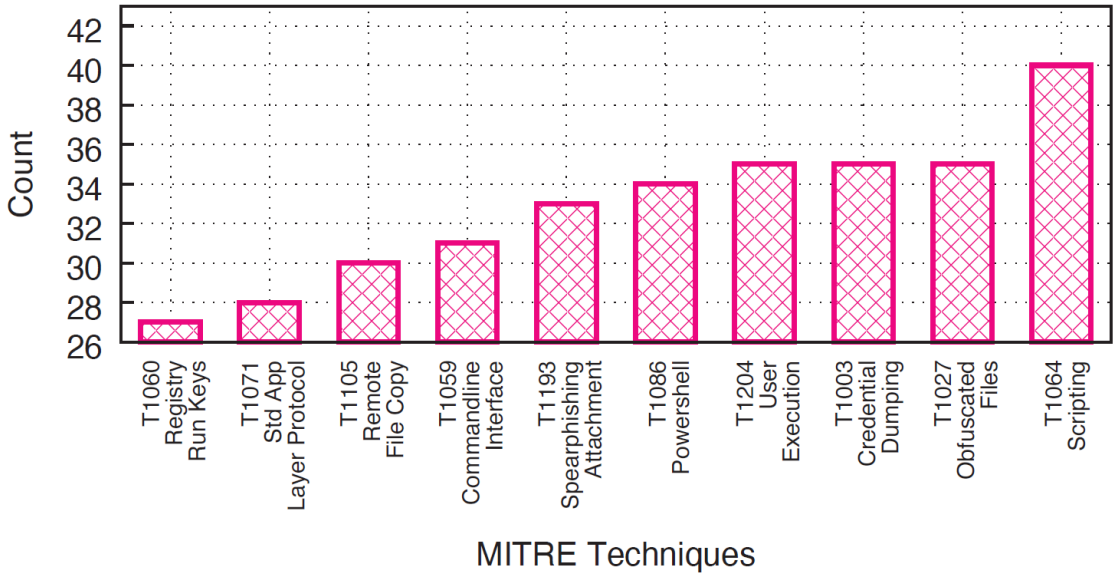
- 理想：主机全覆盖，用户全覆盖，行为全覆盖，数据全覆盖的ATT&CK数据资源池
- 现实：关键数据资产与个人隐私保护需求上升与数据分析可用性之间的矛盾





挑战3：召回模型与高误报率

- 理想：根据ATT&CK的技战术覆盖，逐步提升检测能力的覆盖率、准确性
- 现实：ATT&CK的目标是行为覆盖，然而安全运营需要高精度、低误报的事件（下图只有Spearphishing Attachment，Credential Dumping和Obfuscated Files这三类，其他七类技术划分单独来看，都是正常网络行为与操作）

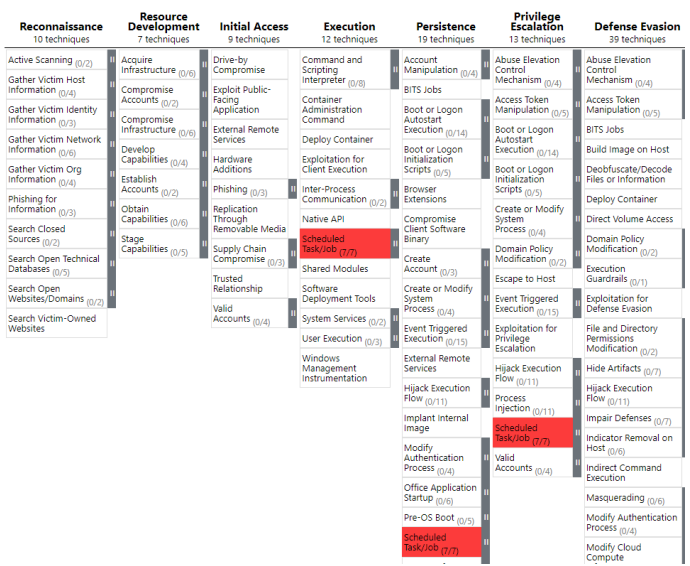


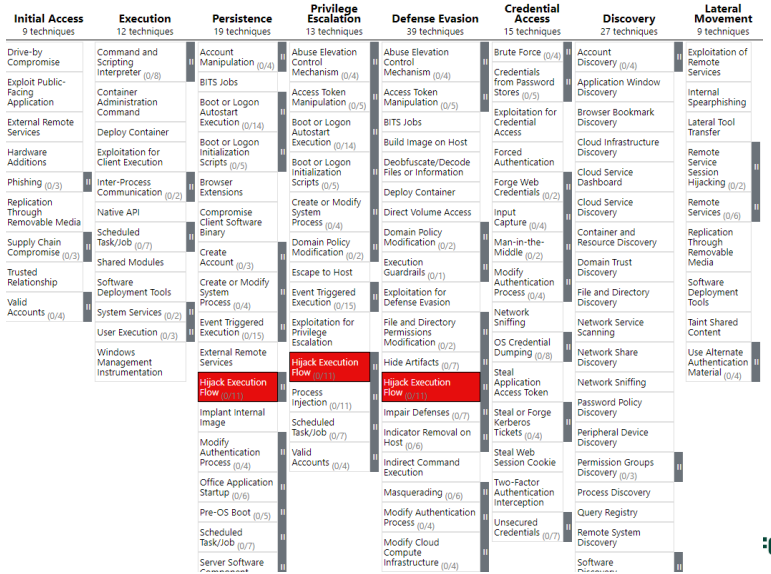
一项针对某著名国外安全企业终端告警的分析表明，由34台机器触发的58096条告警中，与检测目标APT29行为相关真实告警只有1104条，告警的精度只有1.9%。

NSFOCUS

挑战4：一词多义现象

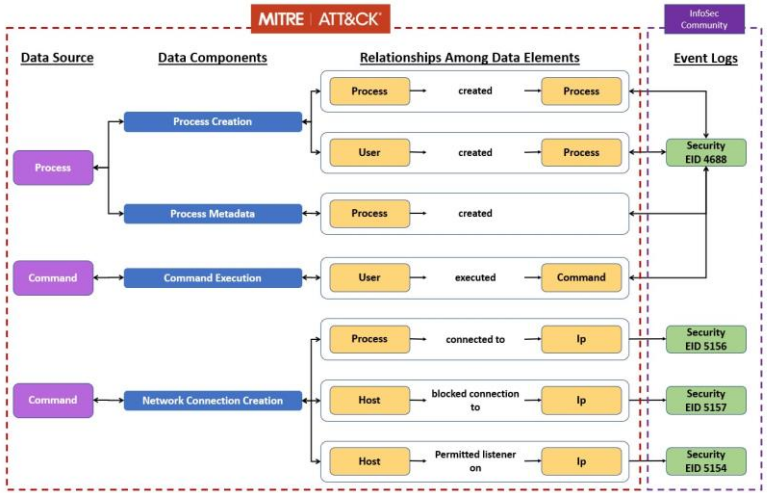
- 理想：ATT&CK通过阶段划分，给具体技术的归类赋予了一定的语义关联，提供了模板化攻击分析策略。
- 现实：一个技术可能横跨多个战术实现，并以不同的粒度出现在一定的威胁上下文中。

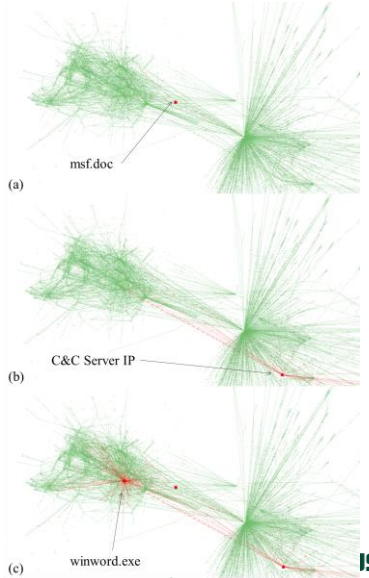




挑战5：信息流依赖爆炸现象

- 理想：结合ATT&CK技战术对应原始日志，快速还原攻击路径，进行检测、溯源、取证
- 现实：
  - 在细粒度的溯源数据层面（Provenance），现阶段的数据采集在一定的资源限制下，难以精细刻画信息传递流。
  - ATT&CK的战术模型不是因果模型，也不具有统计意义





ATT&CK相关技术实战化展望

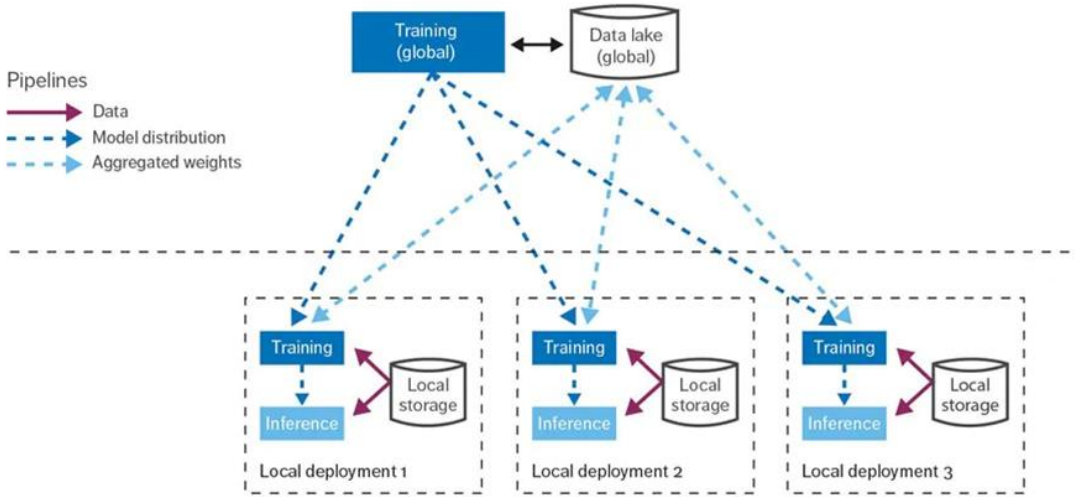
03

如何应对困境

NSFOCUS

应对1：去中心化架构

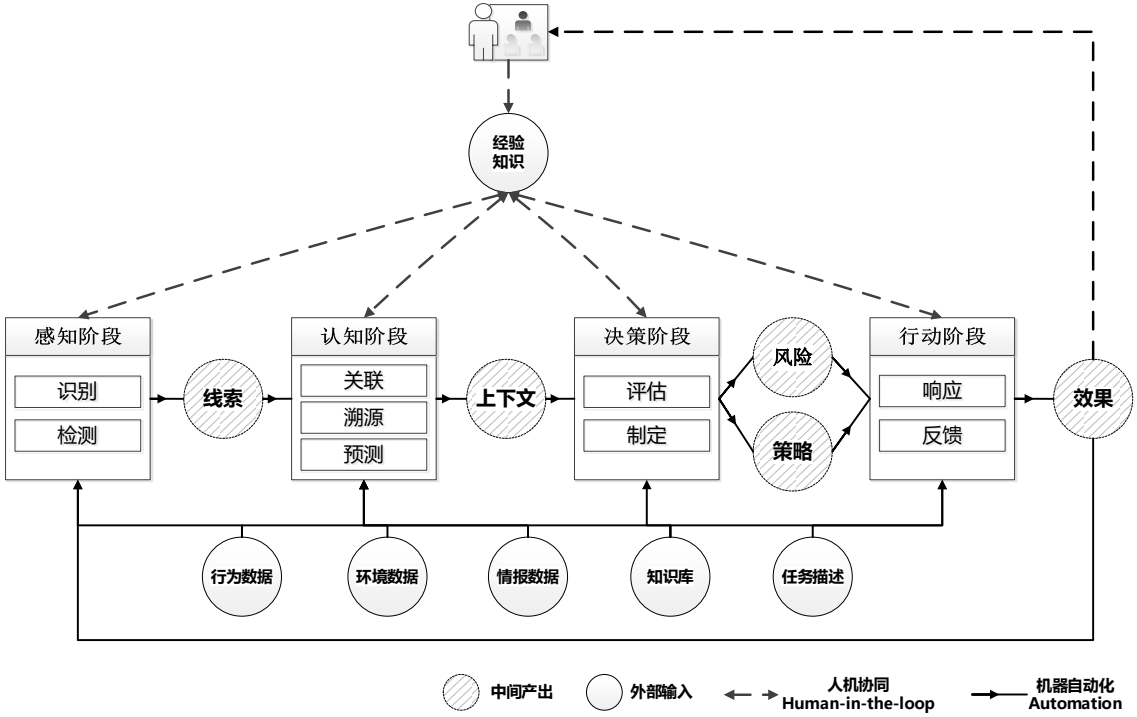
- 去中心化的边缘分析方案，融合分布式模式学习，缓解存储、传输、分析性能瓶颈，降低关键数据资产安全风险



图片来源：https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/privacy-aware-machine-learning

应对2：人机协同的分析机制

- 打造灵活的威胁语义描述语言体系与标准
- 利用ATT&CK构建人-机语言的转换机制，打通经验、知识、情报、数据的语义鸿沟。
- 融合数据规律与专家经验，增强ATT&CK或其他关联的语义强度，主动进行语义消歧。



《AISecOps智能安全运营技术白皮书》

应对3：实战化攻防模拟

- ATT&CK衔接和凝聚了攻防两端，通过实战化、原子化、模板化攻防模拟习得数据与攻防行为之间的映射关系。
- 大型的、标准的、取得共识的统一评测，促进数据的标准化与兼容性提升。

SANS Webcast on MITRE ATT&CK® and Sigma

The SANS webcast on Sigma contains a very good 20 min introduction to the project by John Hubbart from minute 39 onward. (SANS account required; registration is free)

MITRE ATT&CK® and Sigma Alerting Webcast Recording

Atomic Red Team

CALDERA™

Full documentation, training and use-cases can be found here.

CALDERA™ is a cyber security framework designed to easily automate adversary emulation, assist manual red-teams, and automate incident response.

It is built on the MITRE ATT&CK™ framework and is an active research project at MITRE.

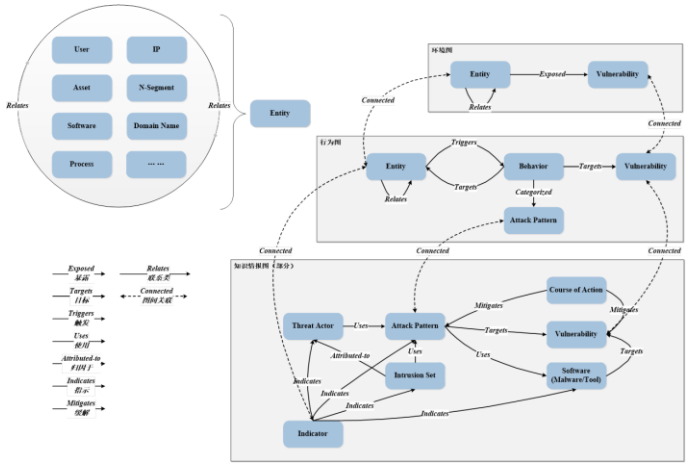
The framework consists of two components:

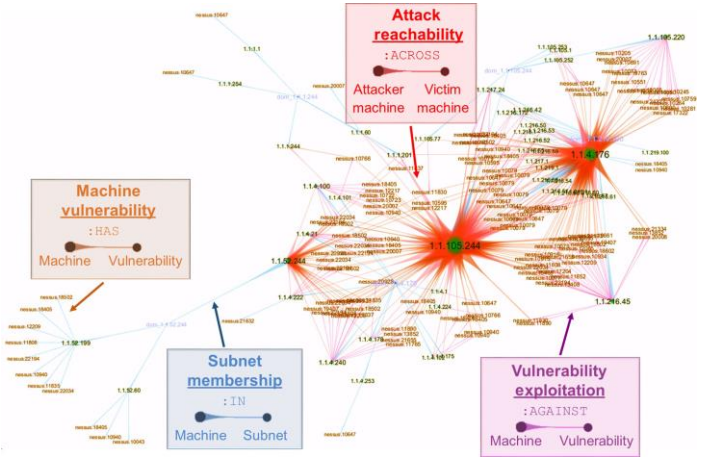
1. **The core system**. This is the framework code, consisting of what is available in this repository. Included is an asynchronous command-and-control (C2) server with a REST API and a web interface.
2. **Plugins**. These repositories expand the core framework capabilities and providing additional functionality. Examples include agents, reporting, collections of TTPs and more.

Rules within this folder are organized by solution or platform. The structure is flattened out, because nested file hierarchies are hard to navigate and find what you're looking for. Each directory contains several .toml files, and the primary ATT&CK tactic is included in the file name when it's relevant (i.e. `windows/execution_via_compiled_html_file.toml`)

应对4：可运营的智能分析手段

- 通过因果建模、上下文建模与可解释性提升，构建可运营的分析策略闭环，缓解信息流的爆炸。
- 构建超融合的知识图谱，提升上下文富化的自动化水平。





MITRE Cygraph

总结——技术实用性方面

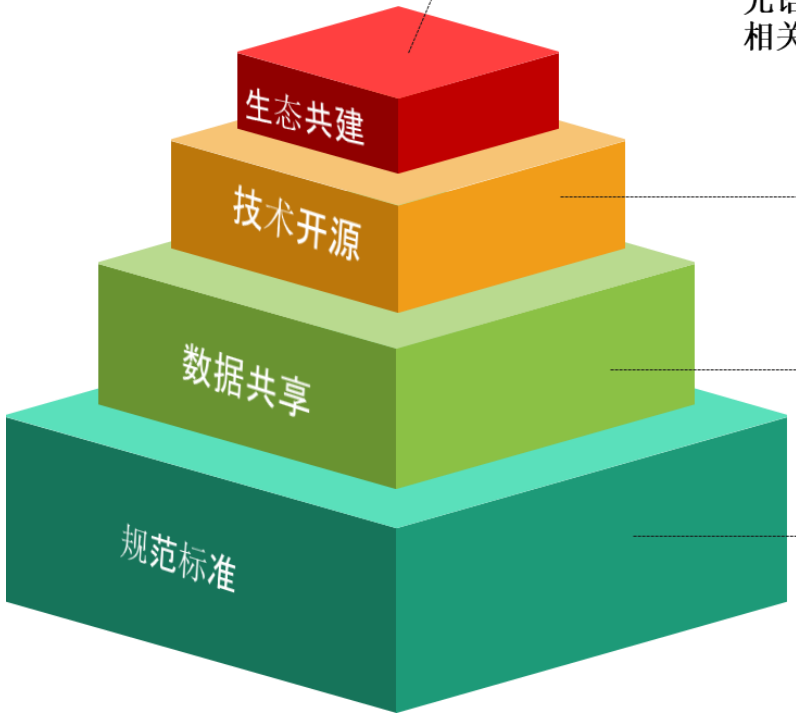
ATT&CK源于实战，回归实战。APT行为与威胁情报数据的深入分析构建可用的、**浓缩的ATT&CK数据资源池。**

探索更完备的攻防知识元语言。ATT&CK适度抽象，但是仍然缺乏对标准化、规范化检测的指导意义，**需从规范的攻防靶场模拟推动攻防知识的扩展与统一。**

人-机智能结合是安全运营、威胁狩猎的技术必由之路。**ATT&CK作为语言粘合剂，仍需要完备的、更形式化的表达形式。**

围绕ATT&CK，Engage等防御知识库兴起。然而，通用知识库的限制也在于通用，**面向场景化的攻防对抗，仍需要数据级、分析级知识构建。**

总结——生态共建方面



构建评估机制，构建一个以标准元语言为核心的技术生态，促进相关技术领域的关键问题突破

围绕标准化、规范化方案，打造高质量的开源技术栈，保持技术的开放性，促进技术的快速演进

基于实战化攻防战场模拟，提升围绕ATT&CK等标准语义的数据质与量，打造促进技术演进的数据基础设施

ATT&CK等技术元语共建，促进人-人、人-机器、机器-机器的低成本互通

THANK YOU FOR WATCHING!

非 常 感 谢 您 的 观 看

NSFOCUS