安全加社区

公益
译文
项目

2017

结构化威胁信息表达 (STIX™)

网络威胁情报信息的结构化语言

文档信息			
原文名称			
原文作者		原文发布日期	
作者简介			
原文发布单位			
原文出处	https://stixproject.github.io/		
译者	小蜜蜂公益翻译组	校对者	小蜜蜂公益翻译组

免责声明

- 本文原文来自于互联网的公共方式，由“安全加”社区出于学习交流的目的进行翻译，而无任何商业利益的考虑和利用，“安全加”社区已经尽可能地对作者和来源进行了通告，但不保证能够穷尽，如您主张相关权利，请及时与“安全加”社区联系。
- “安全加”社区不对翻译版本的准确性、可靠性作任何保证，也不为由翻译不准确所导致的直接或间接损失承担责任。在使用翻译版本中所包含的技术信息时，用户同意“安全加”社区对可能出现的翻译不完整、或不准确导致的全部或部分损失不承担任何责任。用户亦保证不用做商业用途，也不以任何方式修改本译文，基于上述问题产生侵权行为的，法律责任由用户自负。

“安全加”社区　　小蜜蜂公益翻译组

STIX 由多人群策群力共同定义和开发的描述网络威胁信息的结构化语言。STIX 语言用于描述各种潜在网络威胁信息，表达准确、灵活，具有可扩展性，可自动化，并易于理解。欢迎各方人士踊跃加入这个开放、合作的社区，一起推动 STIX 的发展。

STIX 与 TAXII

指标信息的可信自动交换 (TAXII™) 是用于交换通过 STIX 语言描述的信息的首选方法，可使组织以安全和自动化的方式分享结构化的网络安全信息。

STIX 有以下用途：

- 分析网络威胁
- 指定网络威胁的指标模式
- 管理网络威胁防护和响应活动
- 分享网络威胁信息

挑战

现今，组织须具备“网络威胁情报”能力，作为抵御已识别的网络攻击者的一个关键环节。网络情报包括理解信息并描述其特性，例如已发生和可能发生哪些攻击行动、如何检测、识别和缓解这些攻击、相关威胁源起方是谁，试图达到什么目的、从其已利用和将来可能利用的策略、技术与过程 (TTP) 来看，他们具备哪些能力、他们可能要利用哪些漏洞、错误配置或缺陷、他们之前采取了哪些行动等等。

成功实现威胁情报能力的一个关键因素是与合作伙伴、同行及所信任的其他组织共享威胁情报。网络威胁情报和信息共享可帮助组织聚焦庞杂的网络安全信息，并对数据的使用进行优先级排序。组织要处理此类信息，就必然需要标准化的、结构化的信息表达。

解决方案

STIX 是通过群策群力完成的解决方案，可解决上述挑战。它提供网络威胁信息的结构化表达，其表达准确、灵活，具有可扩展性，可自动化，并易于理解。STIX 可实现在不同组织或社区之间分享各类产品 / 服务的全面、丰富和可靠的网络威胁信息。STIX 可扩展简单的指标分享，并对更为准确的各类指标描述和其他各种网络威胁信息进行管理和交换。

STIX 语言

STIX 语言是社区携手所有感兴趣的各方共同开发的，描述了标准网络威胁信息的规范、捕获、特性以及交流。STIX 通过结构化的方式进行威胁信息描述，为更有效的网络威胁管理流程和应用自动化提供支撑。

STIX 提供在一系列用例之间传递结构化的网络威胁信息的通用机制，从而增强了一致性和互操作性，并提升了效率和总体态势感知。此外，STIX 也提供了统一架构，用于绑定一系列广泛多样的网络威胁信息，包括：

- 网络可观察物：例如创建注册表项、特定 IP 地址上出现网络流量、发现特定 IP 地址发送了电子邮件等。
- 指标：指附带含义和情境的潜在可观察物。
- 事件：指特定攻击者行动。
- 攻击者的 TTP，包括攻击模式、恶意软件、利用程序、攻击链、工具、基础设施和锁定受害者等。
- 利用目标：例如，漏洞、缺陷或配置。
- 措施：例如，事件响应或漏洞 / 缺陷修复。
- 网络攻击行动：为实现同一目的而发起的一系列攻击事件和 / 或使用的 TTP。
- 网络威胁源起方：攻击者的识别和 / 或鉴定。

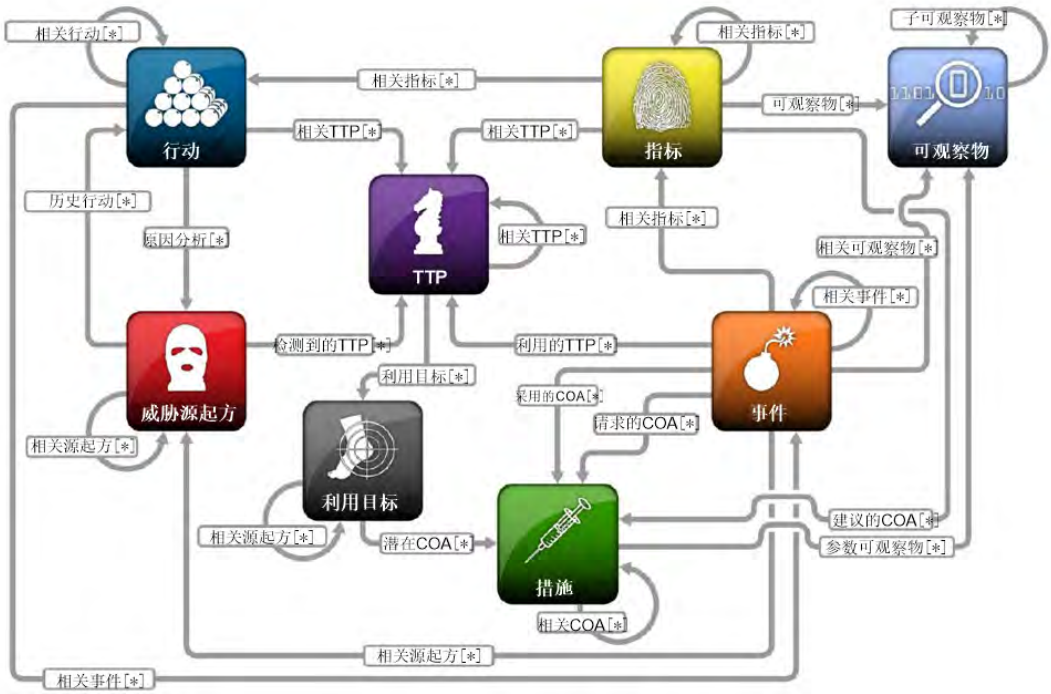
为使这一整体方案适用于任一用例，在适当时，可利用现有的结构化语言，如网络可观察物表达规范（CybOX™）、恶意软件属性列举和特性化（MAEC™）、通用攻击模式列表和分类（CAPEC™）等，并在语言中集成众多灵活性机制。

需特别指出的是，这一完全结构化的语言中，几乎任何一部分都是可选的。这样，单个用例仅需利用 STIX 语言中与其相关的部分，包括小至单个字段，大到整个语言以及介于二者之间的部分。也就是说，各部分之间互相独立。

反馈请求

STIX 社区成员为 STIX 的开发作出了贡献，他们对 STIX 模式、工具、规范和支撑信息的进行了问题追踪管理。网络安全社区成员也受邀加入到持续扩展的社区工作中来。

STIX 由美国国土安全部牵头，由网络安全和通讯办公室实现。MITRE，作为国土安全部的联邦政府资助的研究和开发中心（FFRDC）运营，负责管理 STIX 网站、社区互动、讨论列表，从而实现各利益主体之间公开和开放的协作。



STIX V1.1 架构

结构化威胁信息表达 (STIX™)

网络威胁情报信息的结构化语言

安全加社区

公益译文项目

2017

网络安全公益译文项目旨在分享国外先进网络安全理念，将网络安全战略性文档翻译为中文，促进国内安全组织在相关方面的思考和交流。该项目由安全加社区发起，安全加社区是国内的网络安全社区，社区欢迎网络安全人士的加入，并致力于交付网络安全问题的解决能力。