安全加社区

公益译文项目

2017

运用 MAEC 和 STIX 描述恶意软件特征

V1.0

文档信息			
原文名称			
原文作者		原文发布日期	2014 年 4 月 21 日
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

“安全加”社区　　小蜜蜂公益翻译组

目录

摘要

对组织来说，获得网络威胁情报能力越来越必要，而成功获取该等能力的关键要素是与合作伙伴、友商及所信任的其他人进行信息共享。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。STIX 指“结构化威胁信息表达”，是由多人群策群力共同定义、开发的描述结构化威胁信息的标准化语言，目前处于快速演进中。STIX 语言用以描述各种网络威胁信息，表达准确、灵活，具有可扩展性，可自动化，并易于理解。虽然是个较新的标准，且处于发展阶段，全球许多网络威胁相关组织及群体正积极采用或考虑采用 STIX。欢迎各方人士通过 STIX 网站、Email 讨论清单及其他合作论坛踊跃加入这个开放、合作的群体，一起推动 STIX 的发展。

反馈

STIX 的成功离不了各群体的输入。如对本文件或其他 STIX 文档有任何意见、问题、建议，可通过邮件发送至 stix@mitre.org。

引言

本文介绍了恶意软件属性枚举和特征描述（MAEC）及结构化威胁信息表达（STIX）与语言在恶意软件特征及恶意软件元数据交换环境中的运用。通过描述语言之间的关系并详细介绍每种语言获取恶意软件相关信息的能力，本文回答了“何时使用 MAEC，何时使用 STIX，以及何时使用两者”的问题。

文档架构

首先，执行摘要中介绍了如何使用 STIX、MAEC 和嵌入 STIX 的 MAEC 去获取恶意软件的相关信息。接下来，概要介绍了在这种情况下每种语言（或混合使用两种语言）的一般能力、上下文和目标受众。本节还包括一个简单的流程图，帮助读者确定最符合自己需求的语言。下一节详细介绍了每种语言，包括具体的使用方法。最后，我们讨论了每种语言之间的关系，包括它们对 CybOX 的相互使用。

执行摘要

MAEC 和 STIX 在设计时使用了截然不同的用例，因此在获取恶意软件信息时扮演的角色也不相同。MAEC 旨在提供全面的、结构化的获取恶意软件样本详细信息的方法，因此使用对象主要是恶意软件分析师。STIX 是为了获取各种网络威胁相关的信息，包括恶意软件的基本信息。因此它的受众更多样化。

MAEC 内容也可以嵌入到 STIX 中，使两种语言相互补充。若同时使用，它们可以获取详细的恶意软件信息和网络威胁相关的信息，可在恶意软件和更大的网络威胁环境之间建立有用的、更细粒度的关系。

另一方面，CybOX 为 MAEC 和 STIX 获取与每种语言相关的可观察物提供共同的基础。虽然 CybOX 不能作为一种独立的语言来获取有意义的恶意软件上下文，但它在 MAEC 和 STIX 中的使用使这两种语言在获取恶意软件相关的可观察物方面可以互通。

获取恶意软件信息的选项

STIX 和 MAEC 均可独立用以获取恶意软件信息。然而，在某些情况下，最好是将 MAEC 内容嵌入到 STIX 文档中。表 1 中分别列出了这三种方式（MAEC、STIX、嵌入 STIX 的 MAEC）获取的恶意软件信息的类型。表中还列出了每种情况的上下文及目标受众。

MAEC	STIX	MAEC+STIX
获取结构化的、详细的恶意软件信息 • 能力 • 行为 • 动作 • 杀毒软件类型 • 提取的对象 • 关系 • 相关元数据	**获取结构化的、基本的恶意软件信息** • 类型 • 名称 • 描述	**获取更广泛的恶意软件信息** • 通过 STIX 获取基本的描述性信息 • 提供身份识别 • 通过 MAEC 获取详细的、结构化的信息 • 扩大认识 • 例如，简单介绍某一恶意软件族并详细介绍其中的几个成员
提供分析上下文 • 恶意软件是用来“干什么”的? • 恶意软件是“如何”运行的?	**提供周边上下文** • “谁”在使用恶意软件? • 恶意软件用在“什么地方”？	**提供周边及分析上下文** • 将详细的恶意软件信息与更广泛的威胁上下文联系起来 • 例如，恶意软件实例中的“哪些”具体特征与某个威胁源起方相关?
目标受众: • 恶意软件分析师 / 反向工程师	**目标受众:** • 网络威胁 / 情报分析师 • SOC/CERT 操作员 • 事件响应员	**目标受众:** • 恶意软件分析师 / 反向工程师 • 网络威胁 / 情报分析师 • SOC/CERT 操作员 • 事件响应员

表 1 用于获取恶意软件信息的选项

图 2 中的流程图是为了进一步帮助读者了解在哪些情况下应使用 MAEC、STIX 或嵌入 STIX 的 MAEC。下一节将分别详细介绍它们。

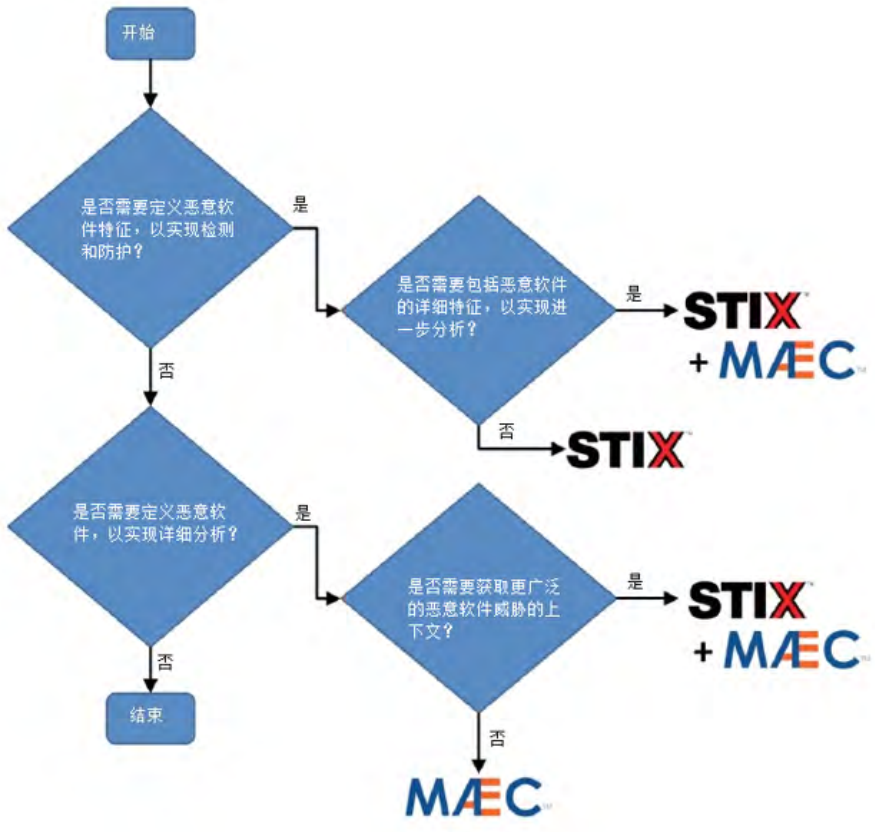

图 2 STIX、MAEC 和嵌入 STIX 的 MAEC 的使用流程图

单独使用 MAEC

MAEC 可获取结构化的恶意软件特征，包括恶意软件具体是如何运行的。通常情况下，MAEC 被用于获取各种形式的恶意软件分析结果，例如恶意软件二进制在沙箱中的执行结果或分析师的手动静态分析结果。此外，MAEC 还可用于获取辅助信息，例如恶意软件的流行程度及恶意软件分析工具的详细信息。因此，MAEC 旨在传达恶意软件的详细分析信息，用以促进器或人类分析师的分析和理解。

特别是，应独立运用 MAEC 获取和交换以下信息：

- 一个或多个恶意软件样本的详细信息（源于一个或多个分析）

a) 静态分析结果

b) 动态分析结果

c) 手动（例如，人为的）分析结果，可提供关于恶意软件行为或能力方面更高级别的信息

- 与恶意软件分析相关的元数据

a) 分析所用工具的信息

b) 分析师 / 组织的信息

c) 恶意软件分析过程中记录的建议和其他观察结果

- 多个恶意软件样本之间的关系

a) 分析相关恶意软件样本集群的群组关系

另一方面，MAEC 不是用于获取与恶意软件相关的网络威胁情报数据的。指标、威胁源起方和其他可能与恶意软件相关的实体都属于 STIX 领域。特别是，MAEC 文档（通常获取原始的静态和动态恶意软件分析数据）不可直接用作恶意软件指标。了解这一点很重要。虽然 MAEC 确实可以获取构成恶意软件指标基础的数据，但这些信息需要分析师进行删减和审核后才能被有效利用。

MAEC 能够获取的数据类型比此处列出的更多，详细信息请参见《MAEC 语言规范》和《详细示例》文档。

单独使用 STIX

STIX 能够以标准化和结构化的方式获取更广泛的网络威胁信息，包括详细的指标、活动、威胁源起方和 TTP（战术、技术和程序）。STIX 还可以提供关于恶意软件样本、族或类别的基本识别信息。因此，概况的网络威胁信息可与明确的恶意软件样本进行直接关联（例如，STIX 指标可与具体的待检测恶意软件样本进行关联）。然而，独立的 STIX 内容设计并不包括恶意软件本身的详细特征；只适合 STIX 以这种方式来获取更广泛的适用数据，如被人们所熟知的利用恶意软件的威胁源起方。

在恶意软件相关信息方面，STIX 能够独立获取和交换以下信息：

- 提供一个或多个恶意软件样本的轻量级描述的 TTP
- 与一个或多个恶意软件样本相关的指标，如对某个被恶意软件样本丢弃的文件的描述
- 利用了一个或多个恶意软件样本的安全事件
- 与一个或多个恶意样本相关的活动
- 利用一个或多个恶意软件样本的威胁源起方

STIX 能够获取所描述的恶意软件的类型（如实例或族）、名称，以及通过 TTP 组件架构提供的恶意软件简介。一般来说，创建 STIX 包应包括多个 TTP，每个被识别的恶意软件实例、族或类别都有一个 TTP。其他的高级 STIX 实体（如指标）可参考这些恶意软件相关的 TTP 来提供相关恶意软件实体的基本上下文。关于示例和更详细信息，请参考《STIX 习惯表达》。

在 STIX 中嵌入 MAEC

通过在 STIX 文件中嵌入本地 MAEC 数据，可获取一个或多个恶意软件样本的结构化详细信息以及各广泛的网络威胁信息。如表 2 所示，在这种情况下通常有 2 种用例。

	用例 1	用例 2
主要内容	对一个或多个恶意软件样本的详细了解	一个或多个威胁实体的上下文环境
次要内容	关于恶意软件的网络威胁上下文环境	对恶意软件样本的详细了解
目标受众	• 恶意软件分析师 • 情报分析师	• 恶意软件分析师 • 情报分析师 • SOC/CERT 操作员
示例	恶意软件样本的详细信息及相关的威胁源起方	完整描述多个网络活动，包括所用的恶意软件

表 2 在 STIX 文档中嵌入 MAEC 的使用案例

通常，STIX 和嵌入的 MAEC 数据可用于获取和交换以下信息：

- 获取一个或多个恶意软件样本的轻量级和详细描述的 TTP

a) 情报分析师和 SOC 操作员可使用轻量级描述

b) 恶意软件分析师和逆向工程师可使用详细描述

c) 两类描述可相互关联，以方便未来的访问和关联。

- 网络威胁的实体之间的关系和对任何相关恶意软件样本的详细描述

a) 例如，这可能包括涉及一个或多个恶意软件样本的网络安全事件，以及对恶意软件样本的结构化描述

- 基于恶意软件的属性中使用的线索以及攻击者本身的信息

a) MAEC（通过与 CybOX 合并）可获取很多详细信息。这些详细信息可提供属性线索（如代码是在哪个目录下编译的）

b) STIX（通过其威胁源起方实体）可以提供关于“谁”（攻击者）的上下文信息

如果 MAEC 内容嵌入到 STIX 文档中，还可以通过 TTP 组件架构获取详细的恶意软件信息。不过，应使用 MAEC 恶意软件扩展架构中的“MAEC4.1InstanceType”类型（“MalwareInstanceType”的扩展类型）而不是 TTP 架构中定义的“MalwareInstanceType”类型。如此以来，MAEC 包可嵌入到 STIX TTP 中，提供一个或多个恶意软件样本的结构性特征（建议 MAEC 包应由为每个恶意软件样本定义的恶意软件主体组成）。

如图 3 所示，除了创建包含嵌入 MAEC 数据的 TTP，可能还需要使用现有的“MalwareInstanceType”类型创建一个相应的包括恶意软件简述的 TTP。这两个 TTP（一个包含 MAEC 内容，另一个只是简单描述）可通过“Related_TTPs”字段相关互联。这样，便可以在使用或交换详细或简单的 TTP 时，仍然能够访问另一个 TTP，非常灵活。

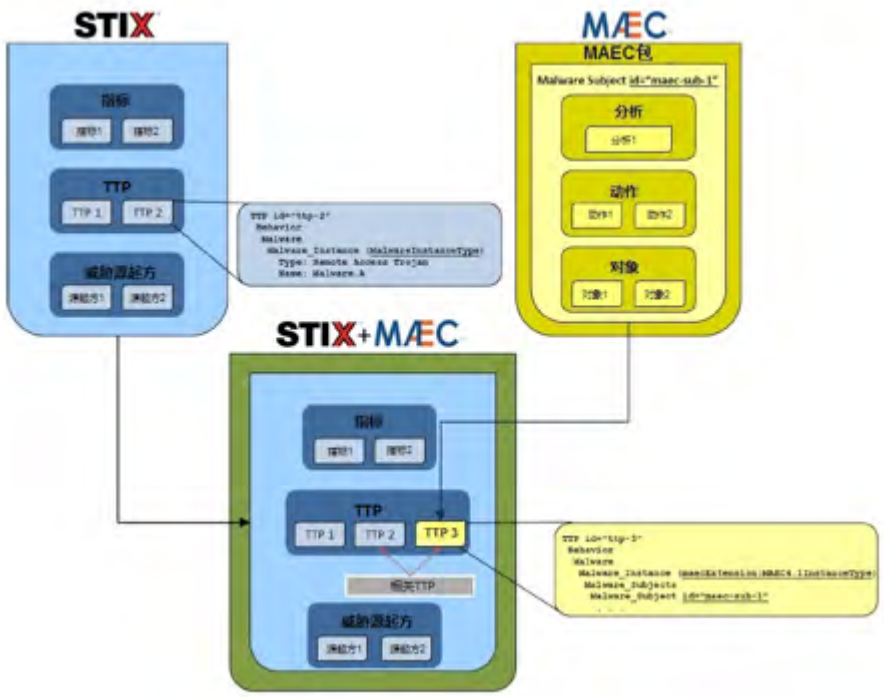

图 3 嵌入 STIX 的 MAEC 的使用示例

语言之间的关系

图 4 所示为 STIX、MAEC 和 CybOX 之间的概念性关系。如图所示，通过嵌入 MAEC，STIX 把详细的恶意软件特征数据封装到更广泛的恶意软件威胁信息中。并且，MAEC 和 STIX 均使用 CyBOX 来表示其网络可观察物。例如，MAEC 使用 CybOX 来描述恶意软件实例运行的各种对象，如文件、Windows 注册表键等。另一方面，STIX 使用 CybOX 作为一种标准化方式来表达定义特定网络威胁指标的对象和模式，如恶意 HTTP 流量中的特定用户代理字符串。

STIX 针对的核心用例

STIX 和 MAEC 共同利用 CybOX，极大地方便了恶意软件指标的构建。如图 5 所示，组织收到恶意软件样本后用 MAEC 工具进行分析。根据分析结果，分析师确定由恶意软件样本创建的特定的文件和注册表键为“好”指标。为了将这些指标分享给组织的合作伙伴，分析师只用从工具生成的 MCEA 文件中获取 CybOX 对象，将其作为 STIX 文档中的 STIX 指标元素。两种语言间共同使用 CybOX 消除了对分析数据进行转换、翻译或其他后期处理的需求，从而将恶意软件分析流程简化为指标定义流程。

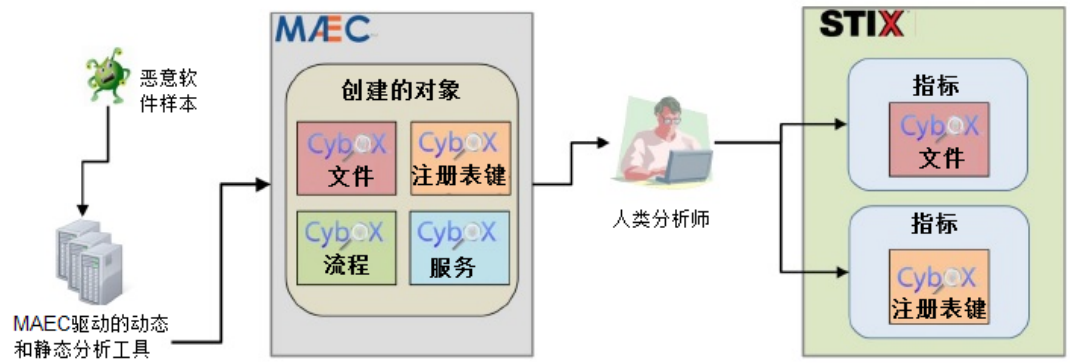

图 5 MAEC-STIX 指标工作流示例

运用 MAEC 和 STIX 描述恶意软件特征

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。