安全加社区

公益译文项目

2017

STIX Profile 概览白皮书

V0.1（草案）

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	MITRE		
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

本文讨论、阐述了 STIX Profile，并就其提出了相应要求。STIX 指“结构化威胁信息表达”，是由多人群策群力共同定义、开发的描述结构化网络威胁信息的标准化语言。STIX 语言用以描述各种潜在的网络威胁信息，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、合作的群体一起推动 STIX 及其 Profile 概念的发展。

本文假设读者已熟知 STIX 数据模型及其部件。

欲了解更多 STIX 相关信息，请访问 http://stix.mitre.org

何为“STIX Profile”？

STIX 针对的是各种网络威胁情报用例，因而数据模型覆盖范围相应宽泛。STIX 本身具有灵活性，可支持各种用例，这同时意味着许多的构造、字段和值对于单个用例来说也许是多余或无关的。例如，使用 STIX 共享基本指标信息的组织可能会选择仅使用指标、可观察物及 TTP 构造。STIX 的其余内容（如威胁源起方（Threat Actor））可能对其他用例有用，但是对于仅实施指标共享的组织来说就无所谓了。STIX Profile 是对这一范围裁剪概念的实践，指某群体、组织或实现（Implementation）采用的特定 STIX 子集。

STIX Profile 用以描述：

- 哪些字段和值必选；
- 哪些字段和值建议使用；
- 哪些字段和值可选；
- 哪些字段和值禁用。

应注意，Profile 仅是针对特定情境下的 STIX 使用范围限制。因此，STIX 中没有针对具体 Profile 的对象或元素，Profile 只是 STIX 的一个子集。本质上，STIX Profile 规定的是应包含 STIX 大框架中哪些元素。除了指定应包含的顶层 STIX 对象，Profile 还会明确应包含哪些网络可察表达（CybOX™）数据模型中所规定的网络可察对象。

Profile 可用于精简繁杂的构造（STIX 部件、CybOX 对象、词汇、关系、扩展等），还可在不同深度，精确描述允许或禁用哪些字段。

下图是一个 STIX Profile 简易视图，内含三个顶层 STIX 对象（指标、可观察物、TTP），并规定了应覆盖 80 多个 CybOX 对象类别中的哪些类别。

~~账户对象~~	地址对象	~~API 对象~~	工件对象
~~代码对象~~	~~自定义对象~~	~~设备对象~~	磁盘对象
~~磁盘分区对象~~	~~DNS 缓存对象~~	DNS 查询对象	~~DNS 记录对象~~
Windows 用户账户对象	~~Windows 卷对象~~	~~Windows 等待表定时器对象~~	~~X509 证书对象~~

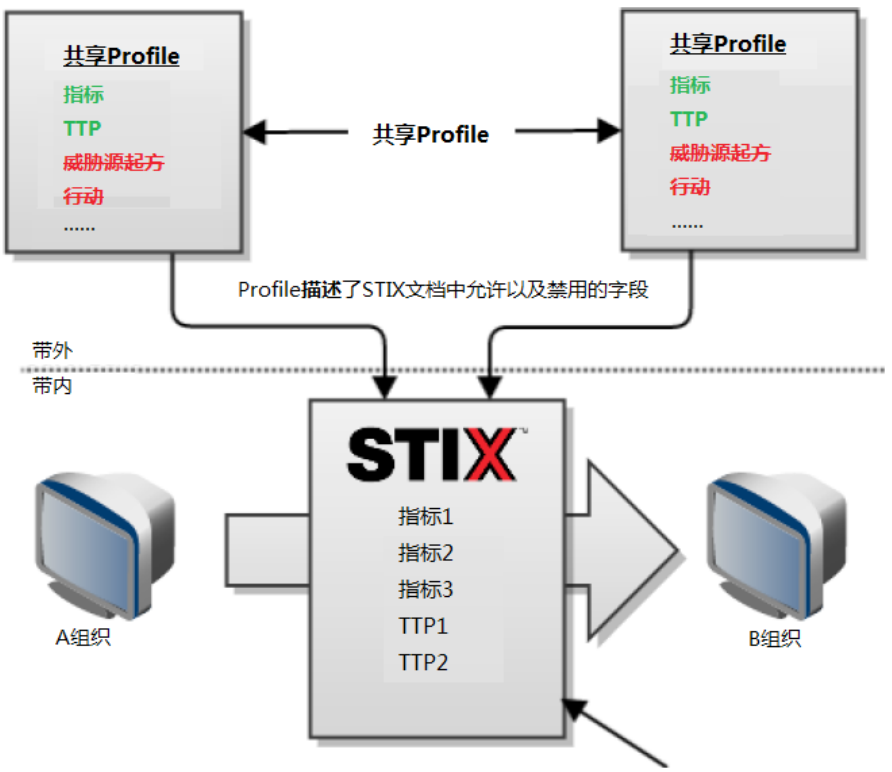
为何使用 Profile?

Profile 有两个主要用途：（1）为使用 STIX 进行信息交流定义共享情境；（2）为工具 / 业务实施能力界定范围。若信息交流各方就 Profile 达成一致或某实现规定了适用 Profile，则 Profile 应将 STIX 范围缩小至只包含必要元素。

对共享模型用户及定义者来说，Profile 有助于就共享内容达成一致认识。群体或用户组可使用 Profile 禁用某些构造，例如，规定不会共享此类信息。

对开发者来说，Profile 的好处体现在可以缩小工作中须参考的 STIX 范围，不把时间浪费在了解无关信息上。基于 Profile 开展工作的开发人员无需了解全套 STIX 构造以及每个构造中所有的字段，只需关注 Profile 中允许的字段，实现用户也很清楚实现处理的是何类信息。

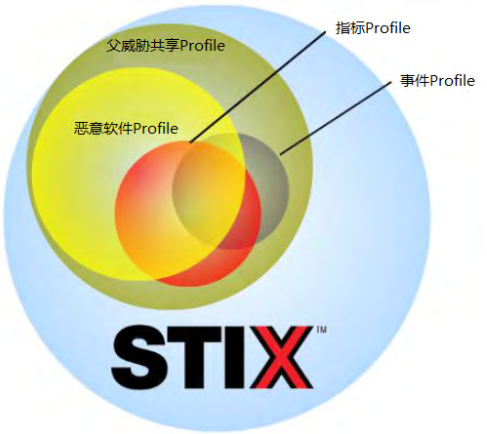
下图中，两个组织使用了相同的 Profile，促进了 STIX 子集共享。本例中，Profile 规定应包含 STIX 指标与 TTP，而不包含其他顶层 STIX 对象。从这点上说，Profile 可协助组织进行治理，制定共享政策，还可以为实施基于 Profile 所定义的 STIX 子集开发的解决方案提供指导。



Profile 对威胁信息使用者尤其有用，因为它确定了使用者的数据库及处理模型必须支持的字段及值集。若某些字段或值被禁用，则数据库无需了解如何存储、代码无需了解如何处理这些字段或值。另一方面，若有些字段或值为必选，使用者则基本上一定能找到这些字段或值，并据此采取行动。

分层 Profile

因为每个 Profile 都是 STIX 的缩减版，有些 Profile 可能为其他 Profile 的子集。以共享用例为例，范围较大的“威胁共享” Profile 会详细描述在某一特定群体内共享威胁信息时允许使用哪些构造，而范围较小的“指标共享” Profile 则基于威胁共享 Profile 制成，对指标共享用到的字段或值进行限定。这就是“分层” Profile，“父”层为限制宽松的父集，仅规定子 Profile 中允许、建议、必选或禁用的字段和值。



子 Profile 可：

1. 禁用父 Profile 中建议或可选的字段；
2. 要求必选父 Profile 中建议或可选的字段;
3. 对父 Profile 中定义的允许类型或值进行进一步限定（但不能扩充）。

关键之处在于，子 Profile 是对父 Profile 的进一步限制，而非放宽或扩充。

因为这些规定，任何满足子 Profile 的 STIX 文档也同时满足父 Profile（乃至父 Profile 的父 Profile），原因就是越往上层，限制就越宽松。无疑，对于 STIX 文档使用者，只要充分支持了父 Profile，也一定支持根据其子 Profile 产生的 STIX 内容；反过来，对于 STIX 文档开发者，只要使用者支持父 Profile，也一定能解释根据相关子 Profile 产生的内容。

Profile 呈现方法

目前，Profile 以人类可读的电子表格形式制成并分发。这种方式成本低，工作量小，方便各群体浏览并了解 Profile 所允许以及禁用的元素，以便讨论共享计划形成共识。Profile 定稿后，开发者可通过电子表格了解需要、应该或不应该赋值的字段，使用者可通过它来了解需要使用的信息。

现用电子表格格式

电子表格的第一个页签包含 Profile 的一些基本信息以及允许及禁用的概要信息。STIX 组件、扩展、CybOX 对象、受控词汇会一一列举，并说明允许还是禁用。

其他页签会详细说明每个构造。对于各个构造（类型），相关字段按照必选、建议、可选及禁用分别列举并编码。若这些字段包含更深层次的信息（如具有自己的构成），该类型的每个字段会用相似编码方法；若字段并无更深层次信息（如，只是一个简单的值或可被视为独立单元），则会被简单编码，不做过多讨论。可为每个字段指定值、类型实现及扩展。

机器可处理 Profile

理想情况下，Profile 应可以由机器处理，这样 STIX 内容可以自动验证或过滤，以确定是否符合 Profile 或去除无效内容。通过机器可处理 Profile，开发者可确保所生成的内容有效，使用者可验证所收到并处理的内容是否确为之前一致同意的内容。

STIX 团队目前正在调研呈现机器可处理 Profile 的可行方法。这需要反复权衡，不管选择哪个方法，都必须符合多数人的需要，以避免大范围出现格式不同且相互抵触的 Profile。

支持与开发 Profile

开发 Profile 的一个常见担忧是，为每个特定用例实例化制定 Profile（这其实完全没有必要），这些 Profile 用户之间很难形成一致的 STIX（因为每个用例遵循的 Profile 不同）。这个担忧不无道理，但是可以通过如下方法或多或少地化解：围绕实际操作，为规范及使用合理抽象化的分层 Profile 集提供指导，将重点放在限制不必要的特定 Profile 上，所谓“不必要”是指有现成的、基本适用的综合 Profile。

例如，在制定自己的 Profile 之前，特定共享群体应首先确认是否有现成的综合 Profile（如“指标共享”Profile）以及是否适用。若需要开发专门的 Profile，该 Profile 应尽可能从属于综合 Profile。这样，遵循综合 Profile 的人才可以理解根据该子 Profile 产生的内容。

开发及使用 Profile

下面举例说明如何新建、写作、使用人类可读的 Profile。

1. 收集 Profile 需求

开发 Profile 的第一步是与相关利益各方合作，了解必须要呈现的数据。这里，应考虑须呈现数据的广度，大致确定用以呈现信息的 STIX 构造及字段。对于某些 Profile 来说，区分“必选”、“建议”、“可选”及“禁用”字段很有必要。而对于更为宽泛的群体驱动的或综合的 Profile，去掉“必选”、保留“建议”、“可选”及“禁用”的说法可能更为合适。

对于 Profile 中的“必选”、“建议”或“可选”（但是非禁止）字段，可能需要进一步限制字段中的数据。例如，STIX 中的许多字段提供选项，要求使用受控词汇来枚举及 / 或限定值。还可以限制只使用特定词汇表的词汇，或甚至对特定词汇表进行限制。对于包含扩展点的其他字段，限制每个扩展点允许使用的扩展实现集。最后，对于简单字符串字段或具有简单值的字段，可将值限定在某一范围。

2. 写作 Profile

上述决策以电子表格格式记录下来。这种格式用于整个 STIX 数据模型，对每个字段的决策均有记录：

- 构造或字段是否“必选”、“建议”、“可选”或“禁用”；
- 若字段存在，对于该字段的限制。

若被标为“必选”、“建议”或“可选”的字段存在任何结构（不只是一个简单的值），Profile 会展示全部结构，记录下为其中每个字段所做的决策。对于“禁用”字段，无需记录其子字段，因为顾名思义，这些子字段也是禁用的。

3. 利用 Profile 进行数据交换

在使用 Profile 进行数据交换时，第一步最可能是带外交换 Profile 本身。这样，所有的 Profile 开发者及使用者才可以对 Profile 进行开发或访问 Profile。这并非必要步骤，但是：Profile 仅仅是一种文档记录方法，对于任何数据交换它们都并非必须。

接下来，开发者构造符合 Profile 的 STIX 文档。所有必选字段都必须存在，建议或可选字段存在与否都可以，禁用字段则一定不能存在。对于字段的任何进一步限制都必须满足。

接下来，通常开发者与使用者会交换 STIX 文档：交换方式包括 TAXII 服务、贴到网上和 Email。这时的 STIX 文档仅仅是一个 STIX 文档而已。

最后，使用者在处理文档时会假设文档符合事先商定的 Profile。文档不会包含禁用字段，但会提供建议或可选字段，而所有的必选字段一定会涵盖其中。未来，机器可处理 Profile 规范会允许验证并管理商定的 Profile，这样就彻底避免了使用时须基于一定的假设。

Profile 要求 / 规定

Profile 应符合以下规定：

1. Profile 可以要求必选、建议、允许或禁用字段或构造；
2. Profile 可以限制或设置字段或构造的值；
3. rofile 可要求字段按某种方式实现（如，要求使用 CIQ 来确定身份）；
4. Profile 可以要求必选、建议、允许或禁用 STIX 的特定扩展；
5. 在不会产生无效内容的前提下，Profile 可以要求必选、建议、允许或禁用扩展（包括 CybOX）内的字段；
6. 根据构造在 STIX 文档中出现的不同位置，Profile 可以对其有不同要求，例如，“信息源”元素在一个地方可以有名称和日期，而在另一个地方则可能只有名称；
7. Profile 不得对 STIX 进行增删，造成最终输出文档符合 Profile，但不符合 STIX，例如，Profile 不能在指标模型中添加额外字段，因为这不符合 STIX 指标构造要求。
8. 与第一条类似，子 Profile 不得扩充父 Profile 的内容或放松其限制，造成最终输出文档符合子 Profile，却不符合父 Profile；父 Profile 必须为子 Profile 的父集，后者不得与前者冲突：
    a. 子 Profile 可以禁用父 Profile 中建议或可选的字段；
    b. 子 Profile 可以要求必选父 Profile 中建议或可选的字段；
    c. 子 Profile 不得将父 Profile 禁用或要求必选的字段列为建议或可选；
    d. 子 Profile 不得禁用父 Profile 中的必选字段或将父 Profile 中禁用的字段列为必选；
    e. 子 Profile 可以对父 Profile 中定义的允许类型或值进行进一步限定（但不能扩充）。

STIX Profile 概览白皮书

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。