简译版

“以用例为中心”的威胁情报需要深思熟虑的方法

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Use Case-Centric Threat Intelligence Requires a Considered Approach		
原文作者	Josh Lefkowitz	原文发布日期	2019 年 9 月 23 日
作者简介	Josh Lefkowitz 是 Flashpoint 的首席执行官。https://www.securityweek.com/authors/josh-lefkowitz		
原文发布单位	Security Week		
原文出处	https://www.securityweek.com/use-case-centric-threat-intelligence-requires-considered-approach		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

“以用例为中心”的威胁情报需要深思熟虑的方法

Josh Lefkowitz

2019 年 9 月 23 日

在过去一年左右的时间里，威胁情报方面最有前景的发展之一是更加强调用例。这很容易理解：“以用例为中心”（case-centric ）的威胁情报策略如果执行得当，能够产生明显的收益，如与业务目标更好的结合、更有效的资源分配、更强的安全性和降低风险等。

但是，也有一些方面不尽如人意。例如，尽管我们强调“用例是有益的”这一事实，但对于在何处、如何以及将哪些用例集成到威胁情报行动中，以便产生我们一直吹捧的收益的讨论却很少。

如果我们对这些细节没有给予足够的重视，就会很容易将用例视为一个标准化的“复选框”项目，而非一种策略。而这种量身定制的策略，可以帮助我们更有效地实现情报行动的目标。

我们以一种相当普遍的用例“品牌监控”（brand monitoring）为例。品牌监控团队通常需要监控各种在线途径，以获取与公司品牌相关的负面信息或其他值得注意的信息。传统上看，此用例只属于品牌保护团队。但是，越来越多的企业开始采用融合的方法，将品牌保护和威胁情报团队的活动和品牌监控目标整合在一起。

假设，有来自两家全球 500 强银行的两位威胁情报从业者，我们分别称之为简（Jane）和约翰（John）。他们的工作都涉及公司的品牌监控活动，但是他们针对此用例所采用的方法却大不相同。

简最近与品牌保护团队一起工作，以满足一项新情报行动——该情报行动旨在解决针对该银行员工的鱼叉式网络钓鱼攻击——的情报要求（IR）和相应的收集要求（CR）。在过去的 30 天中，报告的大多数网络钓鱼电子邮件都试图通过伪造域名来传播银行恶意软件，而这些伪造域名模仿银行员工登录门户的合法域名。此行动的 IR 和 CR 包括：

IR 1：攻击中使用了哪些伪造域名？

-CR 1.1：使用域名置换引擎或类似工具，来识别攻击可能使用或已经使用的伪造域名，以及相应的 IP 地址。

-CR 1.2：监控对网络钓鱼、银行恶意软件和相关网络犯罪活动感兴趣的攻击者经常光顾的非法在线社区，以监控潜在的伪造域名或其 IP 地址。

IR 2：攻击者是如何获得员工信息的，他们获得了哪些信息？

-CR 2.1：监控对网络钓鱼、银行恶意软件和相关网络犯罪活动感兴趣的攻击者经常光顾的非法在线社区，以监控与被攻击员工有关的内容。

-C2.2：评估网络日志，确认是否存在导致员工信息泄露的数据泄露信标或其他攻击信标。

IR 3：哪些攻击者参与了攻击活动，其动机是什么？

-CR 3.1 监控对网络钓鱼、银行恶意软件和相关网络犯罪活动感兴趣的攻击者经常光顾的非法在线社区，以监控与公司、品牌、产品或员工有关的内容。

-CR 3.2 监控对网络钓鱼、银行恶意软件和相关网络犯罪活动感兴趣的攻击者经常访问的非法在线社区，以监控这些攻击使用的恶意软件变种，以及针对银行行业的网络钓鱼攻击或其他攻击手段。

-CR 3.3 将报告的网络钓鱼邮件中的签名与已知的攻击信标（IOC）进行比较。

这些 IR 及其相应的 CR 都包含一些对品牌监控用例至关重要的细节。首先，需要注意，尽管每个 IR 都有至少一个需要满足的 CR，但某些 CR 仍需要来自其他用例的输入，例如网络日志分析和威胁猎杀。

其次，品牌监控的 CR 非常具体，这让简能够清楚地了解她需要监控的资源类型以及需要监控的内容。第三，由于这些 IR、CR 和简的预期目标都被明确阐述，因此简了解其工作的总体目标、其工作将如何支持该行动，以及该行动将如何为其公司提供支持。

然而，约翰的品牌监控方法结构性较差，其方法不受企业的 IR、CR 或任何情报部门的约束。他的任务是监控任何消息源，以了解与其公司品牌有关的任何贬低信息。

约翰完全依赖 18 个月前设置的自动告警功能（至今尚未更新），来获取冗长的关键字列表，导致他经常被大量的误报和非相关告警淹没。他认为，由于告警中没有任何恶意攻击迹象，因此他的公司和品牌受攻击的风险很小。

这两种情况的主要区别在于：简将品牌监控作为一种手段，帮助实现特定情报行动中的

IR 和 CR；而约翰只是为了进行品牌监控。简的目标明确，因此能够相应地调整自己的方法，而且清楚她需要提供什么情报来支持公司的情报部门。而约翰缺乏明确的目标，因此他不确定自己的工作如何为公司提供支持、其工作的有效性如何以及其方法是否需要进行任何调整。最终，简为公司提供了有价值的情报，而约翰却没能提供。

这个例子说明，在应用和讨论用例时需要深思熟虑。正如本文所述，以用例为中心的威胁情报方法可以带来巨大的收益，该方法确实值得采用——但是需要适当的方式。需要注意，用例不是一种简单的选项，不是通用的；它应被视为一种实现目标的手段，而不是局限于其自身的目标。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十五亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： http://www.antiy.com（中文）

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com