简译版

共享威胁情报的六个步骤

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	6 Steps for Sharing Threat Intelligence		
原文作者	Steve Zurier	**原文发布日期**	2017 年 11 月 10 日
作者简介	Steve Zurier 是一名自由撰稿人，拥有 30 多年的新闻和出版经验。 https://www.darkreading.com/author-bio.asp?author_id=2460		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/threat-intelligence/6-steps-for-sharing-threat-intelligence-------/d/d-id/1330386?		
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。		

共享威胁情报的六个步骤

Steve Zurier

2017 年 11 月 10 日

9.11 恐怖袭击事件之后，威胁信息共享开始受到网络安全行业的更多关注。

你可能认为这是一个例行的过程，特别是考虑到在过去几年中发生了大量的数据泄露事件。尽管联邦政府和信息共享分析中心（ISAC）在这一方面已经取得了很大的进展，但是许多组织仍然将威胁信息共享放在次要位置。

“目前的情况是，首席信息安全官（CISO）非常忙碌！尽管他们知道信息共享能够帮助自己更胜任现在的岗位，或者至少是更好的人，但是他们却把它推迟了。” TruStar Technology 创始人兼首席执行官保罗·库尔茨（Paul Kurtz）说，“他们并不总是能认识到信息共享的好处。”

库尔茨称，威胁信息共享的主要原则是：

1、信息共享不是利他主义的。数据交换的目的是更快地发现问题并缓释攻击。当一个行业纵向共享威胁数据时，该行业内的其他公司就不必再做重复性的工作了，每个人都会从中受益。

2、信息共享不是入侵通知。在事件发生之前，组织需要在安全周期的早期共享事件数据，例如有关可疑活动的信息。

3、只要不共享个人身份信息，与其他组织共享有关漏洞利用代码和漏洞的数据就是合法的。例如，受害者的电子邮件地址通常不被共享。共享的典型信息类型包括：可疑的 URL，哈希标签和 IP 地址。2015 年的《网络安全信息共享法案》提供了更多的细节。

4、共享系统必须易于使用。确保系统是人性化的，并且可以轻松地与安全运营中心（SOC）、威胁猎捕团队或欺诈调查团队的工作流程进行整合。

金融服务信息共享和分析中心（FS-ISAC）的首席信息风险官格雷格·泰姆（Greg Temm）警告说，企业在进行威胁信息共享时需要有足够的耐心。

“威胁共享共享需要时间”，泰姆说。“我们可能有一些可疑活动的清单，但是我们真正

想要的是威胁源进行攻击的原因。真正重要的信息是威胁源是否为国家效力，网络犯罪分子是为了赚钱还是服务于某个政治观点。要想深入了解这些信息，需要结合共享的数据、分析方法和威胁情报技术。”

零售业网络情报共享中心（R-CISC）的高级行业信息共享和分析中心（ISAC）分析师尼尔·丹尼斯（Neal Dennis）表示，那些不知道从哪里开始或者没有大量安全工具的公司应该联系其 ISAC。“我们的很多成员都是小型零售公司，他们没有 Target 或 Home Depot 的资源，所以他们寻求零售 ISAC 的威胁信息和指导来部署潜在的工具是很有意义的。”丹尼斯说。

以下是有关如何共享威胁情报的一些建议。

了解企业内部的威胁事件

顾好自己的企业：首先了解企业内部的事件以及它们之间的联系。除非您了解自身组织内部正在进行的活动，否则您无法与他人分享信息。如今有很多工具可以帮助您了解事件数据。该领域的一些供应商包括 TruStar Technology（该公司专门从事威胁情报集成，以便与其他企业和地域共享情报）以及威胁情报提供商 Anomali 和 ThreatConnect。

更有效地利用情报

确保能够使用其他提供商共享的情报，无论这些情报是来自 CrowdStrike 还是 ISAC，无论是来自金融、航空航天领域还是零售业。企业通常无法轻易使用来自专有威胁提供商或共享中心的外部威胁资源。通常他们会收到一封列出 20 个可疑 IP 地址的电子邮件，但他们无法筛选这些信息。当选择一个工具时，请询问该工具是否可以帮助完成这个过程，因为筛选列表是非常耗时的，会占用安全专家的大量时间和精力。

开始信息共享

现在您已经准备好与行业和业务伙伴的同行交换数据了。但是在共享信息之前，一定要选择一个返回即时值的系统，让你看到自身事件数据与他人数据有何关联。例如，如果你的事件与另一家公司或行业 ISAC 相关联，则可以与他们共享信息并获得他们的信息。除非您确定威胁是真实的，否则就没有分享的动力。

如果可以，尽量不要限制威胁情报来源

选择一个允许您加入任意数量的共享组织或合作关系的系统，同时保护您认为合适的归因。一些事件可以广泛地共享，而其他事件可能需要更多的特殊处理。寻求与其他行业共享信息的好处是，您可以根据不良 URL、IP 地址或浏览器数据找到共同的模式。

选择一个可以参与美国政府的系统

与国土安全局的自动指标共享（AIS）服务部门共享信息可能有益于你的组织。在过去几年中，国土安全部一直致力于开发共享威胁情报的合作伙伴生态系统。AIS 旨在广泛分享公共和私营部门的威胁情报，使组织能够更有效地保护自己免受网络攻击。

小型组织：向 ISAC 寻求帮助

中小型企业根本没有购买更复杂的威胁情报的经济实力，他们也无法聘请威胁捕手。这些组织应该与其行业 ISAC 合作，建立一个低成本的威胁情报系统。多半的可能是，您的行业 ISAC 与供应商有联系，甚至可能有与专门的威胁情报公司建立关系的特殊交易。