

简译版

关于威胁情报的三个误解

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	3 Modern Myths of Threat Intelligence		
原文作者	Anton Chuvakin	原文发布日期	2019 年 12 月 2 日
作者简介	<p>Anton Chuvakin 是 Chronicle 公司安全解决方案战略负责人。</p> <p>https://www.darkreading.com/author-bio.asp?author_id=5309</p>		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/threat-intelligence/3-modern-myths-of-threat-intelligence/a/d-id/1336452		
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	<ul style="list-style-type: none"> 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。 		

关于威胁情报的三个误解

Anton Chuvakin

2019 年 12 月 2 日

更多的情报并不一定会带来更高的安全性。本文将介绍原因。

关于数据泄露的新闻层出不穷。在 2019 年的前三个季度，我们看到了 1152 起数据泄露事件的报告，这些事件导致银行、医院、社交媒体网站和餐馆等机构的 1.6 亿条记录被泄露。

诚然，过去十年左右的大多数安全文章都以类似的统计数据开头。但是，鉴于过去几年安全投资的增加，如今此类新闻更加令人头疼了。

这些新闻说明：我们尚未确定了解威胁，采取应对措施并保护系统免受未来攻击的最佳方法。尽管许多安全专家都认为“了解敌人”很重要，但是很少有人付诸实践。

在担任安全分析师的八年中，我经常看到这一问题。企业拥有情报，但没有能力使用这些情报来实现其目标。在威胁情报方面，我也看到了相同的问题和误解。下面，我将介绍三种常见的威胁情报误解，这些误解阻碍了企业充分发挥其安全潜力。

误解 1：使用威胁情报来阻止威胁很容易。

安全团队试图将情报纳入预防控制措施中，但是其中许多控制措施是静态的，无法有效解决情报的不确定性。使原本静态的预防控制措施更加敏捷，通常会带来无法解决的挑战。另一方面，安全团队可以并且应该在检测和可见性控制措施中使用威胁情报，以便进行快速调整。有时候，使用新的威胁情报来保护数据会比一味地增强防御要容易一些。

在某些情况下，静态防御可以很好地阻止攻击。例如，应用程序白名单或网络访问控制有助于提高安全性，而且不需要深入分析攻击者。你也可以尝试在 IP 或哈希阻止列表中使用威胁情报数据，但结果会有所不同。

但是，在这些用例中，威胁情报被大材小用了。甚至有人说 IP 和哈希阻止列表并非真正的威胁情报。利用威胁情报意味着一定程度的敏捷性，而高度依赖这些静态防御的团队通常浪费了这种敏捷性。相比于与攻击者玩“打地鼠”的游戏，使用威胁情报进行检测、告警分类和事件响应能够实现更高的安全性。

误解 2：收集的威胁情报越多，安全性就越高。

许多企业不知道如何从威胁情报中获取价值，而情报（无论是否是网络情报）无法帮助那些不愿意自助的人。如果有人告诉你，今晚有小偷会抢劫你家，你会采取什么措施来阻止抢劫呢？你可以锁上门，藏起贵重物品，甚至可以住在朋友家中。但是，这些都不能保证犯罪活动不会发生。

我注意到，企业在使用威胁情报时并没有真正理解“敏捷”的含义。以我的经验，敏捷的安全团队可以快速将情报整合到检测流程中，并部署可以快速运行以进行检测的工具。如果你了解到，某个组织计划使用某种方法来入侵你的系统，但是你无法调整基础架构或现有控制措施来进行防御，那么情报就浪费了。在了解威胁之后，安全性取决于你在威胁发生之前采取的下一步措施。

我曾经听说，一家公司得知其电子商务网站面临攻击。该公司无法在一夜之间联系到新的托管服务提供商或更改其配置，因此该公司无法保护自己。最终，该公司所遭受的损失几乎与不知道攻击即将来临时所遭受的损失相同。更有效的方法是：安全团队迅速对托管服务提供商的配置或网站进行直接更改。

误解 3：每个人都需要威胁情报。

尽管威胁情报很诱人，但是安全运营流程不会在一夜之间变得“情报感知”。实际上，“获取更多情报”的任务通常会使安全团队分心，尤其是当此类情报无法投入运营时。在这些情况下，企业最好专注于安全措施，例如删除管理权限和应用程序白名单，以及在几乎完全没有威胁情报的情况下有效运作的其他措施。

关联新的威胁情报数据，比加快变更管理流程、帮助企业快速找到受影响的资产要容易得多。但是，更多的情报并不能带来更高的安全性，而且“情报包-打地鼠方法”存在机会成本。

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 endpoint 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,截止到 2019 年 9 月 30 日,安天的威胁检测引擎为全球超过六十万台网络设备和网络安全设备、超过十七亿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>