“威胁数据”转化为“威胁情报”是安全计划成功的关键

非官方中文译文·安天技术公益翻译组 译注

简译版

文档信息			
原文名称	Understanding how data becomes intelligence is central for any successful security program		
原文作者	Andrea Fumagalli	**原文发布日期**	2019 年 1 月 10 日
作者简介	Andrea Fumagalli 是 DFLabs 公司产品工程副总裁。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2019/01/10/how-data-becomes-intelligence/		
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。		

“威胁数据”转化为“威胁情报”是安全计划成功的关键

Andrea Fumagalli

2019 年 1 月 10 日

“威胁情报”是目前信息安全领域最热门的术语之一。但是，正如许多流行语一样，它经常被滥用，造成了很多混乱。

很多人认为“威胁数据”（即威胁信息源）就是“威胁情报”，但实际上，前者只是后者的一部分。当威胁数据添加了情境，就成为了威胁情报，从而生成相关的、“可转化为行动”的信息，使企业能够更好地调整其安全和业务目标。

威胁数据是恶意域、IP 地址或哈希值的原始集合，不包括任何攻击或威胁情境。

威胁数据确实有其用例。但是，威胁数据不包含情境信息，因此其用例是有限的，无法帮助安全团队制定决策。为了正确使用威胁情报，企业必须清楚：将威胁情报引入其安全计划的目的是什么。如果不清楚这一点，那么企业的安全计划只会带来严重的资源消耗，不会产生任何实际价值。

数据质量

虽然数据源对于威胁情报计划至关重要，但是并非所有数据源都“生而平等”。

企业拥有许多威胁情报源，最常见的来源包括：恶意代码处理、扫描/爬取、蜜罐、人工智能和内部监测。威胁情报的提供方式有三种：开源情报、免费资源或付费订阅。

为了从这些数据源中获得最大的收益，企业需要很好地了解这些来源，以便评估与其内部情报相关的数据。

最好的数据源会近乎实时地更新和转发。使用旧的或不完整的数据可能会误导企业关注错误的目标，最终导致数据过载和告警疲劳。在云计算时代，IP 地址每天都会被多次重用，因此上述情况尤其严重。

数据增强

成功的威胁情报计划的关键是：对每个数据源进行适当的分析，以获得相关情境信息，

从而改变运营方式并保护环境。

如果未进行认真的规划和执行 ,那么将威胁情报纳入现有的安全计划可能会导致令人失望的结果。例如，一家采用“金融服务行业信息共享和分析中心”（ FS-ISAC ）威胁情报的制造公司，将不太可能实现其预期的结果；这是因为，这类情报源具有金融服务行业情境，而非制造行业情境。

安全情报和业务目标

威胁情报计划成功的基础是 :确保该计划与企业的业务目标保持一致。而实现这一点的最佳方法是：评估数据源如何解决与特定业务运营相关的安全问题。

通常来说，当事件发生时，企业对其影响范围或严重程度知之甚少，其了解的信息通常仅限于单个告警或信标。因此，企业必须结合适当的情境和情报，以便更深入地了解事件，确定其影响范围。高级攻击隐藏在复杂的编码或恶意代码背后，因此这种模糊性是其典型特征。安全团队必须对每个事件进行分类和评估，以确定其真实性和严重性，以及其是否需要更多关注（调查）。

在这两个阶段中 ,安全运营团队通常依靠威胁情报来确定事件的可能范围及其可能造成的损害。例如，关于某个文件的告警可能只包含一个哈希信标。手动分析可能会发现其他信标，但是这种分析非常耗时。

正确使用自动化

更好的方法是部署自动化的威胁情报增强系统。

分析师可能需要几分钟甚至几小时，才能完成网络中的恶意代码和信标分析；而自动化方法只需几秒钟就能完成。自动化的威胁情报增强可以实现既快速又高效、可预测且可重复的流程。这种方法还能使分析师从繁琐且容易出错的任务(如收集和验证数据)中解放出来，使其专注于增值分析和威胁猎杀。

威胁情报的目标是使用数据来提高安全性并提供更高的可见性。因此，安全人员可以根据威胁的风险级别来确定补救措施的优先级。

选择“正确”的数据源只是第一步，更重要的问题是：设置数据挖掘机制和工作流程、增强数据并将其转化为威胁情报。

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，始终坚持自主先进能力导向，依托下一代威胁检测引擎等先进技术和工程能力积累，研发了智甲、镇关、探海、捕风、追影、拓痕等系列产品，为客户构建端点防护、边界防护、流量监测、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有机结合，推动客户整体安全能力建设的叠加演进。安天为网信主管部门、军队、保密、部委行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，产品与服务为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。

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厂商、IT 厂商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、超过十四亿部智能终端设备提供了安全检测能力。

安天技术实力得到行业管理机构、客户和伙伴的认可，已连续五届蝉联国家级安全应急服务支撑单位。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，为捍卫国家主权、安全和发展利益提供了有力支撑。

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的发言代表，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*