

简译版

2018 年“威胁猎杀”经验总结

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	More Than Just a Fad: Lessons Learned About Threat Hunting in 2018		
原文作者	Jake Munroe	原文发布日期	2018 年 12 月 21 日
作者简介	<p>Jake Munroe 是 IBM Security i2 团队的产品营销经理。</p> <p>https://securityintelligence.com/author/jake-munroe/</p>		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/more-than-just-a-fad-lessons-learned-about-threat-hunting-in-2018/		
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。 		

2018 年“威胁猎杀”经验总结

Jake Munroe

2018 年 12 月 21 日

2018 年已经接近尾声，一些曾经甚嚣尘上的“时尚”也将随之而去。例如，指尖陀螺（Fidget Spinner）将会被闲置，“假人挑战”（mannequin challenge）将只会出现在百货商店中，舞力全开（Nae Nae）将会在“舞林”中销声匿迹。

在网络安全领域，情况也是一样的。就像病毒式扩散的互联网表情包一样，热门工具和流行语总是来去匆匆。但是，“威胁猎杀”（threat hunting）将会继续发展。威胁猎杀是一种主动查找和缓解威胁的方法，已经存在了很长一段时间，现在正在成为全球安全运营中心（SOC）、政府和私营公司普遍接受的概念。这很大程度上归功于该方法的优点，以及迅速出现的现实用例。

在过去的一年里，我们了解了该方法的优缺点、注意事项等问题。下面，我们将对 2018 年威胁猎杀的经验教训进行总结。

应用威胁猎杀技术之前，应对员工进行猎杀方法的培训

当新的安全功能迅速发展时，大多数公司的第一笔投资是具备这些功能的工具。威胁猎杀方面的投资也是如此，其中，威胁猎杀方法和技术是最重要的投资领域。

SANS 2018 年威胁猎杀调查的一项重要发现表明，在威胁猎杀方面，企业的首要投资领域仍然是技术；尽管一些受访者表示，企业在许多领域缺乏训练有素的员工，导致他们无法执行（或者无法有效地执行）威胁猎杀。企业需要注意，威胁猎杀工具的有效性取决于“猎手”（受训专家）的技能水平。这与传统的建筑领域一样，只有经过专业训练的高水平的建筑工人才能将完美的蓝图变为现实。

威胁猎手需要具备情报分析知识并了解 SOC 技术，因此，培训和雇用合适的人员尤为重要。目前，企业在威胁猎杀方面存在技能差距，这意味着企业难以找到训练有素的威胁猎手来使用其购买的工具。

进入 2019 年，企业应该全面审视他们的威胁猎杀计划；如果没有威胁猎杀计划，则无法评判出现安全问题的原因是什么——究竟是花哨的工具，还是缺乏训练有素的威胁猎手。

同样，刚接触威胁猎杀的企业，在采用最新的工具之前，应该评估他们拥有或计划雇用的威胁猎手。

威胁猎杀的有效性取决于企业的情报框架

要启动有效的威胁猎杀计划，企业还需要获取适当的数据。为了提高威胁猎杀的效率和准确性，这些数据应该包括公司的内部数据，来自深网和暗网的数据，以及开源和第三方威胁情报。这些数据有助于企业了解威胁情境。

SANS 调查显示，企业将内部生成的情报与外部数据相结合，可以减少攻击者在其网络中驻留的时间。但是，这不仅仅是获取数据的问题。企业可以获取世界上所有的数据，但如果它无法提供情境并生成“可转化为行动”的假设，那么数据就是无用的。

在反恐领域，我们总是说“情报推动作战”。的确，我们需要获取适当的数据；但更重要的是，我们需要融合这些数据并为作战人员提供可转化为行动的建议。威胁猎杀也是如此：数据是关键，但还需要一种方法来收集、融合和分析数据，以生成威胁假设。

2019 年威胁猎杀将继续发展

在 2019 年，网络安全企业将继续了解威胁猎杀，以及如何实施有效的威胁猎杀计划。在新的一年里，新的“时尚”会不可避免地出现和消逝；同样，也会出现新的网络安全工具、方法和经验教训。企业已经看到了实施威胁猎杀计划的收益，很明显它不仅仅是一种安全“时尚”。

在采用威胁猎杀技术之前，企业应对员工进行猎杀方法的培训，探索如何弥补威胁猎手的技能差距、获取数据并生成可转化为行动的假设，以便发现威胁。在恰当实施的情况下，威胁猎杀计划的有效性如何呢，我们将继续关注。

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>