简译版

有意识进行威胁猎杀的理由以及具体操作

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	Hunt With Intention - Why You Should Adopt Threat Hunting and How to Get Started		
原文作者	Michael Kehoe	原文发布日期	2019 年 5 月 17 日
作者简介	Michael Kehoe 是 IBM WW i2 销售主管。https://securityintelligence.com/author/michael-kehoe/		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/hunt-with-intention-why-you-should-adopt-threat-hunting-and-how-to-get-started/		
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。		

有意识进行威胁猎杀的理由以及具体操作

Michael Kehoe

2019 年 5 月 17 日

在一些关于网络犯罪的新闻报道中，总是采用这样一种黑客形象：在昏暗的房间里，一个身穿黑色连帽衫的年轻人，疯狂地敲击电脑键盘。每次看到这种新闻时，我都会觉得很有趣。在提及网络攻击者时，大多数人会联想到 1983 年的电影《战争游戏》（WarGames）中年轻的马修·布罗德里克（Matthew Broderick）饰演的天才黑客少年。这可大错特错了。

现在的攻击者非常聪明，他们组织严密、动机强烈且专注于既定目标——这些目标可能包括你、你的企业和其他任何人。无论攻击者是谁，住在哪里或着装如何，他们都可能正潜伏在你的网络上或正在攻破你的网络。而“威胁猎杀”（threat hunting）的目的正是：在恶意行为对企业造成任何损害之前阻止它们。

如今，攻击者通过复杂的攻击方法来实现他们的目标。这些攻击可能来自各种威胁面，例如恶意内部人员、诈骗、资产挪用以及其他网络风险。从外部看，企业通常在多个层面存在漏洞，包括其网络、员工和公共信息等。开放网络上的信息，例如年度报告、运营保障、员工的电子邮件和社交媒体信息等，都可以成为攻击者打开公司网络的钥匙。通过这些数据，攻击者可以更好地了解目标，以便更精准地发动攻击。

不幸的是，企业并不知道何人将会对他们实施精心策划的攻击，以及将在何时、何地或如何实施。即使最好的基于规则的防御方案，也有其局限性。我们用于监控和检测攻击向量的嵌入式规则，通常很难预测攻击向量将会如何发展。要想主动和被动地缓解威胁，企业必须采取更具适应性的方法，并且比攻击者领先一步。简单地说，当颠覆现有规则的威胁向量出现时，就是时候进行威胁猎杀了。

什么是威胁猎杀，从何处着手进行威胁猎杀？

威胁猎杀正成为网络领域的流行语，但它确实适用于企业目前面临的威胁形势。在这方面，采用整体性的策略至关重要——通过这种战略，企业可以分析攻击者可能利用的资金、人员、被攻击对象的内部原有的脆弱性以及其他攻击向量。此外，“威胁猎手”（threat hunter）应采用“以人为主导”的情报方法来对抗人为攻击。通过将事件和行动关联起来，威胁猎手

可以快速识别经过模糊处理的模式，进而发现精心构造的攻击向量。为了有效地进行威胁猎杀，企业应制定有效的威胁猎杀计划。

在开始进行威胁猎杀之前，制定威胁猎杀计划非常重要。根据 IBM 赞助的 2019 年 SANS 研究院报告，威胁猎杀的两个主要目标是：

1. 主动搜索威胁，以限制攻击者的影响；

2. 更好地了解环境。

这两个目标适用于任何威胁猎杀计划——无论企业试图追踪网络威胁、金融犯罪还是任何物理攻击。接下来，我们将深入探讨一些更好的实践，以帮助企业制定威胁猎杀计划。

有意识地进行威胁猎杀

有意识地进行威胁猎杀意味着：了解将要进行威胁猎杀的环境，以及这些环境中过去、现在和未来的威胁。这样一来，威胁猎杀团队就能识别以前未知的威胁并进行缓解。此外，通过响应既有威胁，团队可以发现其信标，从而采用更主动的防御方法。

正如 SANS 研究院在报告中所述，“攻击者很可能在企业环境中创建了据点，但不会触发安全团队惯于响应的任何告警。或者更糟糕的是，攻击者存在于一个监控“盲区”，即，他们钻了防御的“空子”，因而规避了检测。

当进行威胁猎杀时，团队合作至关重要

分析师们喜欢对威胁穷追猛打，直到走进死胡同——这已经不是什么秘密了。对于网络分析师、反洗钱专家和反恐官员来说，情况确实如此。这些分析师经常忘记的是，他们可以利用其他资源使猎杀更容易、更成功。例如，如果分析师整天都在处理内部数据，而没有利用外部情报丰富内部数据，那他们就会缺乏塑造威胁猎杀的关键情境。威胁猎杀非常适合团队活动，内部和外部资源可以很好地协同运作。

SANS 还建议企业向有助于进行威胁猎杀的解决方案（例如链接分析工具）适当投资，以丰富数据，识别内外部主机与网络数据点之间的关联。通过实时情报持续增强防御能力至关重要，企业应采用最值得信赖的情报分析工具，以协助以人为主导的网络威胁调查。

积累被动响应的经验，进而形成主动猎杀的防护策略

当你开始考虑制定威胁猎杀计划来查找和修复网络威胁、金融犯罪、物理攻击等风险时，请务必有意识地进行猎杀，并开展团队合作。只要牢记这两个原则（有意识猎杀以及团队合作），企业的安全团队首先能从被动响应当前威胁基础上，增强其防护能力；进而能形成其主动的防护策略，以在类似威胁出现前，主动拦截其进攻。

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*