简译版

基于机器学习的威胁检测面临的四种挑战

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	4 Machine Learning Challenges for Threat Detection		
原文作者	克里斯托弗·佩里（Christopher Perry）	**原文发布日期**	2020 年 5 月 4 日
作者简介	克里斯托弗·佩里是 BMC AMI 的首席产品经理。		
原文发布单位	Information Week		
原文出处	https://www.informationweek.com/strategic-cio/security-and-risk-strategy/4-machine-learning-challenges-for-threat-detection/a/d-id/1337639?		
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。		

基于机器学习的威胁检测面临的四种挑战

克里斯托弗·佩里

2020 年 5 月 4 日

机器学习（ML）的发展及其使用大数据提供深刻见解的能力仍然是热门话题。许多公司的高管都有意开发 ML 计划，希望从中获益，网络安全行业也不例外。大多数信息安全供应商都采用了某种形式的 ML，但显然，ML 并不是对于所有人来说都是灵丹妙药。

虽然针对网络安全的机器学习解决方案能够并且将提供可观的投资回报，但现在它们确实面临着一些挑战。企业应该意识到 ML 的一些潜在问题，并制定切合实际的目标以挖掘出 ML 的全部潜力。

误报与告警疲劳

ML 检测软件最大的弊端是它每天会产生数百万个告警，这是一个“不可能完成的”数量，就如同对分析师发起了拒绝服务攻击。严重依赖于威胁外观的“静态分析”方法尤其如此。

即使准确率为 97%的基于 ML 的检测解决方案可能也没有什么用处，简单地说，结果并不理想。

假设在企业网络上的 10,000 个用户中存在一个威胁。借助贝叶斯定律（Bayes’ law），我们可以计算出告警发展成真正攻击的概率——将 0.97（97%的准确率）乘以所有用户的实际威胁概率，即 1/10,000。这意味着即使有 97%的准确率，告警变成真正攻击的实际可能性也只有 0.0097%！

由于可能无法将准确率提高到 97%以上，所以解决此问题的最佳方法是通过白名单或者事先使用相关领域的专业知识进行筛选来限制接受评估的用户。这可能意味着要将重点放在可信度高、有特权的用户或业务部门的关键部分上。

动态环境稳定性

ML 算法的工作原理是学习环境并建立基线规范，然后监测可能表明攻击的异常事件。但是，如果 IT 企业不断进行调整以满足业务敏捷性需求，动态环境却没有稳定的基线，那

么该算法将不能有效地确定什么是正常情况，并可能会针对完全良性事件发出告警。

为了最大程度地减小这种影响，安全团队必须在 DevOps 环境中工作，以了解正在进行的更改，并相应地更新他们的工具。DevSecOps（开发、安全和运营）逐渐受到人们的关注，因为这些元素应该是同步的，并在同一个共享意识中发挥作用。

上下文

ML 的强大之处在于它能够通过大量的多变量相关性分析来进行预测。但是，当真正的告警进入安全分析人员的队列时，这种强大的关联却是以“黑匣子”的形式呈现出来，上面只显示着“告警”两个字。然后在此基础上，分析人员必须梳理日志和事件，找出触发告警的原因。

应对这一挑战的最佳方法是为安全运营中心提供工具，使其可以快速过滤触发实体上的日志数据。人工智能可以帮助自动化和加速数据语境化。数据可视化工具也可以通过提供事件的快速时间表以及对特定环境的理解来提供帮助。然后，安全分析人员可以快速确定 ML 软件为何发送告警以及告警是否有效。

反 ML 攻击

ML 面临的最后一个挑战是黑客能够快速适应并绕过检测。当这种情况发生时，可能会产生灾难性的后果。正如最近发生的事件中，黑客能够通过操纵自动速度检测系统，可以迷惑特斯拉，让它们把每小时 35 英里的限速标志看成是 85 英里。

ML 在安全上没有什么不同。ML 网络检测算法就是一个很好的例子，该算法使用字节分析非常有效地确定流量到底是良性的还是 Shellcode。黑客通过使用多态混合攻击，用额外的字节填充 Shellcode 攻击来改变字节频率并完全绕过检测算法，从而迅速适应了 ML 网络检测算法。越来越多的证据表明，没有哪个工具是无懈可击的，安全团队需要不断评估其安全状况，并及时了解最新的攻击趋势。

ML 能够有效赋能安全团队，其自动检测和关联数据的能力可以为安全从业人员节省大量时间。

但是，改善安全态势的关键是人机结合，其中机器（不断扩大的 IoC 库）与人类（渗透测试人员和大批白帽黑客）之间存在共生关系。ML 拥有保持领先优势所需的速度和灵活

性，而人类则拥有机器（目前）无法复制的特质—逻辑、情感推理和基于经验知识的决策技能。

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，为客户构建端点防护、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*