简译版

利用 AI 解决网络安全人才短缺问题

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	Curbing the Cybersecurity Workforce Shortage with AI		
原文作者	Deborah Golden	**原文发布日期**	2017 年 8 月 18 日
作者简介	Deborah Golden 是 Deloitte & Touche 律师事务所咨询业务的主要负责人，拥有超过 20 年的信息技术、安全和隐私保护经验。 http://www.darkreading.com/author-bio.asp?author_id=4803		
原文发布单位	Dark Reading		
原文出处	http://www.darkreading.com/threat-intelligence/curbing-the-cybersecurity-workforce-shortage-with-ai/a/d-id/1329617?		
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。		

利用 AI 解决网络安全人才短缺问题

Deborah Golden

2017 年 8 月 18 日

高失业率固然不是什么好事，但接近 0%的行业失业率也不是件好事。极低或零失业率意味着：没有足够的网络安全专家填补职位空缺；对现有人才的需求旺盛，造成薪资上涨和较高的人才流失率；组织更有可能雇用技能不足的员工。这正是网络安全领域的现状，而且不太可能很快得到好转--到 2019 年全球预计将有超过 150 万个职位空缺。

无论组织如何努力，他们将无法聘请足够的大学毕业生、招聘足够的技术专业人员或者对现有员工进行再培训以减轻这种短缺。但他们可以采用另一种方法：认知计算（学习，思考和与人类交互的系统）。通过使用人工智能、机器学习、高级分析技术和自动化等认知技术，组织可以提高现有员工的生产力并优化支持流程来解决人才短缺问题。

道理很简单：认知计算可以使组织更好地利用网络安全人才的时间和技能，并提高安全性。员工不必再花费大量时间响应潜在威胁或普通管理任务，他们可以聚焦于主动安全和复杂的调查。

例如，认知技术可以通过改进组织的工作流程来解决人才短缺问题。一家领先的投资公司指出，通过实现日常活动的自动化，之前耗费网络专家约 40 分钟的任务现在可以在 40 秒内完成，分析师的生产力提高了三倍。这就是自动化的价值：在时间和人才已经不足的情况下，不需花太多的时间在普通任务上。

除了节省时间，它还能省钱。最近的一项研究发现，组织每年花费大约 21 万小时调查误报，每年的平均成本为 130 万美元。这些警报可以由认知系统来处理，只有在需要进行更多调查时认知系统才会通知网络安全人员。

自动化才刚刚开始。其更强大的应用之一是使用高级分析。这种技术使用超级计算机处理能力来筛选大量数据，以识别行为模式、恶意代码和不明显的网络异常。这可以帮助网络专业人士预测威胁最有可能发生的地方，然后在威胁发生之前予以阻止。

我们以一个大型有线和互联网服务提供商为例，该提供商每天接收超过 50 万个网络安全警报。它部署了一个行为分析应用程序，允许分析师设定基准网络活动，识别和关联安全

警报，以隔离最具威胁性的警报并改进安全阈值。结果是：六个月后，该提供商的警报减少了 99.8%，其网络安全专家可以将精力放在最高优先级的警报上。

如何使用

行为分析的应用是无止境的。银行可以使用这种技术来识别偏离个人用户典型行为的可疑在线账户活动，从而阻止盗用、欺诈或进一步的网络渗透。网络安全公司可以使用行为分析来检测新病毒或未知攻击，并在损坏发生之前阻止恶意行为，从而以机器速度进行响应。

行为分析是认知技术对网络安全的最大贡献之一，因为它允许组织采取主动的方法。从大量网络流量中筛选异常行为的能力是一个巨大的安全优势。能够预测威胁最有可能发生的地方，然后在威胁发生之前阻止它们，从根本上改变安全态势。

认知技术解决网络安全人才短缺的另一种方法是帮助减少人才流失(员工对工作感到不满意会导致人才流失)。典型的工作日充斥着无休止的、不具有挑战性的任务或活动，这会导致员工另寻高就。根据人力资源管理协会的报告，48%的员工认为工作本身对工作满意度至关重要。

自然地，有人担心认知计算意味着“机器人取代人类”，或认知技术的效率可能会导致人类失去工作。这种恐惧有些夸张了。当杂货店引进自助结账亭时，收银员也曾担心会失去工作。ATM 的出现和广泛采用使得许多人认为银行柜员会失业。但是实际情况是，杂货店收银员和银行柜员的数量仍然在不断增长。在网络安全领域，机器无法实现的人类交互和创造力仍然具有压倒性的需求。

关键是不要与机器对抗，而是与它竞争。认知技术可以管理安全任务、预测恶意攻击并帮助留住员工。这些能力使公司能够通过重新分配现有人员来解决人才短缺问题，而不必仅仅依靠雇用新的和有经验的人才，同时也能够改进流程并加强决策。

但是机器不是万能的。通过将机器与对组织网络的认识相结合，网络安全专家可以识别网络的弱点，了解组织易遭受的网络攻击类型，并优先处理相关的漏洞。通过这种方式，人机配合可以在更短的时间内产生更好的效果。