利用 AI 威胁情报工具改善攻击检测

■ 山东 姜建华 赵长林

编者按：他山之石，可以攻玉。威胁情报服务和工具可以从 AI 尤其是机器学习等高级技术中获得很大提升。如何利用 AI 改善攻击检测的过程从而提升安全性呢？

对于利用威胁情报的企业而言，下一步的发展是以机器学习技术的形式增加人工智能（AI）的威胁情报功能，用以提高攻击检测能力。

机器学习是可以使计算机分析数据并学习其意义的一种人工智能形式。将机器学习结合威胁情报使用的根本原因是，在攻击发生之前，使计算机能够以比人更快的速度检测并阻止攻击。此外，由于威胁情报的体量如此巨大，传统的检测技术不可避免地会产生很多虚假的情报。机器学习可以分析威胁情报并将其浓缩为更细小的要点，因而可以减少一些虚假情报的数量。

这听起来似乎很令人激动，但还存在问题。期望 AI 极大地提升安全性也不现实，而且在没有准备和后续支持的情况下部署机器学习可能使事情更糟。

企业可以采取哪些步骤才能更好地利用具有机器学习功能的 AI 情报工具，从而提高攻击的检测能力呢？

利用高质量的威胁情报源

利用机器学习的 AI 威胁情报产品是通过接收、分析输入并产生输出而工作的。对于攻击检测来说，机器学习的输入包括威胁情报，而其输出可能是指示攻击正在发生的警告，或者是阻止攻击的自动操作。如果威胁情报有错误，机器学习将把错误信息交给攻击检测工具，所以工具化的机器学习算法可能产生错误的结果。

很多企业都订阅了多个威胁源，其中包括机器可读取的攻击迹象的数据源，如发动攻击的计算机的 IP 地址和恶意软件使用的文件名等。其他的威胁情报源是服务，它一般提供可由人读取的描述最新威胁的文本信息。机器学习可以利用情报源，但无法使用服务。

企业应当将最高质量的威胁情报源用于机器学习。不妨从如下方面考虑如何选择威胁情报源。

首先，情报源多久更新一次？威胁的变化非常快，所以情报源应当持续更新。其次，情报源的数据准确性如何？例如，一个被报告称正在发动攻击的 IP 地址是否确实？第三，情报源的全面性如何？是否覆盖了全世界范围的威胁？是否包括了企业的检测工具所需威胁的信息类型？

直接评估威胁情报的质量是很难的，但是根据因使用威胁情报而导致的虚假情报的数量进行间接评估却是可行的。在直接由检测工具

使用而无需机器学习时，高质量的威胁情报应当带来最少量的虚假信息。

给予机器学习所需的场景，使虚假情报最少化

如果将威胁情报用于机器学习执行诸如自动阻止攻击等操作，虚假或错误情报可能是一个现实问题。错误可以破坏正常的活动，并有可能对运营产生负面影响。

从根本上说，威胁情报仅仅是评估风险的一部分而已。另一个部分是理解环境或场景，如角色、每台电脑的重要性和运营特性等。将环境信息提供给机器学习有助于从威胁情报中获得更多价值。假如威胁情报表明一个特定的外部 IP 地址是恶意的，那么检测从一个内部的数据库服务器向外传输到这个地址的网络通信，与检测一个每天将文件发送给订阅者的服务器向这个同一 IP 地址发出的网络通信相比，将产生不同的操作。

使用机器学习的最困难部分是提供真实的学习。机器学习需要知道哪些是好的，哪些是不好的，并且在犯错误时也能够从中学习。这就要求熟练技术人员的持续关注。向机器传授学习技术的一种常见方法是将其置于一个仅有监视的模式中，其中的机器可以识别恶意的东西但并不阻止任何操作。人类检查机器学习工具的警告，并加以验证，使其知道哪些是错误的。没有来自人的反馈，机器学习就不能改正错误和提升自身。

利用威胁情报和机器学习补充和提升对威胁的猎杀

传统理念是要避免依靠使用机器学习来检测攻击的 AI 威胁情报，主要是担心虚假情报问题。在有些环境中这是对的，但在其他环境中就是错的。较老的检测技术更有可能遗漏最新的攻击，因为它无法跟上这些攻击技术的新模式。机器学习有助于安全团队发现最新的攻击，但是可能存在较高的误报率。遗漏攻击与调查可能的虚拟情报所需要的资源相比，将是一个更大的问题，那么更多地依靠利用机器学习的自动化对于保护这些资产来说可能更有意义。

很多企业可能会发现最好是将无需机器学习的威胁情报用于某些目的，而将机器学习所生成的结果用于其他目的。例如，威胁猎手可能将机器学习用于获得一些操作上的建议，用于人们无法在海量的威胁情报数据集中调查并得到有重要价值的信息情况。

当然，不可忽视的是，威胁情报服务报告可以为威胁猎手提供一些关于最新威胁的珍贵信息。这些信息往往包括一些不能轻易地实现自动化从而使机器学习可以处理的东西。N