AI 和 ML 增强的安全用例

splunk>

此电子书旨在帮助读者寻找在 Splunk 中实现人工智能 (AI) 或机器学习 (ML)，进而获得价值的方法，简要介绍在其他地方成功实现的示例用例。本文将针对每个用例介绍业务挑战、推荐的 Splunk 方法和价值。此外，还将包括支持信息的链接，例如帮助在 Splunk 环境中重现用例的客户案例研究或文档。

目录

用例

立即开始使用

什么是人工智能和机器学习?

术语 “机器学习”(ML) 经常可与术语 “人工智能”(AI) 互换使用，但 ML 其实是 AI 的一个子领域。ML 是计算机科学的一个领域，研究方向是开发能够从经验中自主学习的计算机系统 (特别是通过处理接收到的数据) 并提高特定任务的性能。

人工智能是系统处理显式和隐式表示的能力，以及执行如果由人类执行将被视为智能的任务的能力。

机器学习是计算机系统利用算法和统计模型不断提高特定任务性能的能力。

深度学习是一种专门的 ML 算法，旨在模仿人脑的神经网络，允许机器使用大量的数据从自己的行为中学习，并改善未来的结果。

生成式 AI，也称为 GenAI，大致属于机器学习的范畴。它只是指可以创建内容的算法，包括文本、图像、视频、模拟、代码、音频等。生成式 AI 的示例包括 ChatGPT、DALL-E 和 Google Bard 等工具。

总的来说，AI 和 ML 领域正在不断发展。重要的是理解这些技术可以应用于解决业务问题，只要有数据可以训练它们。

为什么组织要对人工智能进行投入?

在过去几年中，组织不得不应对全球范围内的业务中断，业务韧性受到前所未有的考验。正如我们在数字韧性会带来回报报告中指出的那样，能够为变化做好准备是构建韧性以及在不确定时期保持蓬勃发展的关键因素。一个经常与变化和创新相关联的主题是 AI 和 ML。在网络安全方面，在事件发生之前预测和预防事件的能力是 ML 产生价值的关键领域之一；与那些可以对服务中断做出反应的公司相比，能够防止服务中断的公司具有更大的韧性。在所有产品和服务中采用 ML 和自动补救的组织针对经济衰退产生的需求做好准备的可能性 (66%)，是不采用这一做法的公司 (34%) 的两倍。

根据 Forrester 的总体经济影响报告，采用 Splunk 可观测性功能的组织报告了以下情况:

- **系统停机减少了 70%**
- **MTTR 下降了 75%**
- **正常运行时间延长 250 小时，投资回报率提高 243%**

如何在 Splunk 安全性中使用 ML/AI?

Splunk 可提供多种在产品组合中使用 AI/ML 的方法。大体上有两种使用 AI/ML 的方法: 通过集成到现有产品工作流中的现成功能，或通过定制。

ML 嵌入到 Splunk Cloud Platform 和 Splunk Enterprise 内部的 Splunk 平台中，可通过 Splunk Enterprise Security 订阅获得，允许用户:

- 检测异常情况，例如识别登录失败次数中的异常值。
- 生成预测，例如预测 VPN 使用情况以确定与正常活动的偏差。
- 进行预测，例如从网络活动中预测潜在的僵尸网络活动。
- 将数据分组，例如，将 Windows 事件日志分组以发现潜在的恶意异常值。

这些技术手段可以通过助手来应用，助手可以指导用户通过一系列步骤来训练、评估和实施 ML 模型。或者，还可以使用 Splunk 的搜索语言 — 搜索处理语言 (SPL) 直接创建基于 ML 的分析，并在核心搜索和报告中嵌入大量 ML 搜索命令，例如 *predict* 和 *cluster*。搜索和报告应用程序中的模式选项卡还可以显示嵌入式机器学习，以帮助识别搜索结果中的相似事件组。