配置DLP以保护敏感数据不被ChatGPT使用

目录

简介

本文档介绍如何使用防数据丢失(DLP)保护敏感数据不被ChatGPT使用。

概述

人工智能世界正在轰然兴起，OpenAI的语言模型ChatGPT等创新引领着潮流。这个人工智能强国一直在以惊人的速度增长，通过智能的情景感知对话改变了众多行业。但是，随着这些令人激动的进步，也出现了一些潜在挑战 — 具体来说，就是数据丢失风险。

将ChatGPT视为一个超级智能对话合作伙伴，根据您提供的内容生成文本。现在，如果混合中存在敏感信息，且未正确处理，则存在数据泄露的风险。这突显了为什么实施全面的数据丢失防护(DLP)计划如此重要。

您的Umbrella DLP解决方案旨在保护您的组织免受这些风险。以下是我们的解决方案可以帮助您立即解决的三大紧迫使用案例，并且只需要5分钟时间即可实施。

A.符合GDPR、HIPPA和PCI-DSS等数据隐私法规：

1. 转至Umbrella控制面板中的Policies > Management > Data Loss Prevention Policy。
2. 开始创建新的DLP规则。只需点击右上角的Add Rule并选择Real Time Rule。
3. 为您的规则提供一个易于识别的名称，例如“ChatGPT保护”，并选择适合您需求的严重性级别（从低到严重）。
4. 在分类部分，选择一个或多个与您的组织相关的内置合规性分类。例如，这可能是“内置GDPR分类”或“内置PCI分类”。
5. 在身份部分中，选择要监视和保护的所有身份。如果可行，我们建议广泛选择全面覆盖范围。
6. 转到Destinations部分，选择Destination Lists and Applications for Inclusion，然后选择OpenAI ChatGPT。
7. 现在，是时候采取行动了。在操作部分中，可以选择监控或阻止。如果您对此不熟悉，我们建议从“Monitor”操作开始。这允许您观察使用模式，并对潜在风险和益处做出更明智的决策。
8. 如果您已选择“Monitor”操作，请务必在一周或一个月后查看DLP报告。这将显示您与ChatGPT共享敏感信息的人员以及时间，帮助您确定是否需要“阻止”操作。

B.个人身份信息保护：要保护您组织中的PII免受ChatGPT风险，只需使用与上面相同的说明，但在步骤4中，选择“内置PII分类”而不是合规性分类。

C.保护源代码和知识产权： 如果您的组织将ChatGPT用于涉及源代码或其他知识产权的活动，请使用以下步骤：

1. 首先，创建新的源代码数据分类。导航到策略>管理>策略组件>数据分类。单击右上方的Add按钮，为数据分类指定一个可识别的名称，例如“Source Code Classification”。
2. 从内置数据标识符列表中选择Source Code。
3. Click Save.
4. 保存后，重新访问上述“遵守数据隐私法规”的说明，但在步骤4中，请选择您新创建的源代码数据分类，而不是内置的分类方法。

此过程非常简单，只需花费几分钟时间，但为您的组织提供安全性和合规性带来的好处非常宝贵。我们强烈建议您尽快采取这些步骤来强化您的数据保护。

要了解有关生成AI风险以及Umbrella如何保护您的更多信息，请观看网络研讨会从ChatGPT使用中保护您的敏感数据。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。