配置DLP以保護敏感資料不被ChatGPT使用

目錄

簡介

本文說明如何使用防資料丟失(DLP)來保護敏感資料不被ChatGPT使用。

概觀

人工智慧領域正在蓬勃發展，OpenAI的語言模型ChatGPT等創新引領著潮流。這個人工智慧強國一直在高速增長，通過智慧的情景感知對話改變了眾多行業。但是，隨著這些令人振奮的進步，也出現了一些潛在挑戰 — 具體來說，就是資料丟失風險。

將ChatGPT視為一個超級智慧的對話合作夥伴，根據您提供的內容生成文本。現在，如果混合中有敏感資訊，並且未正確處理，則存在資料洩露的風險。這突顯了為什麼實施全面的資料丟失防護(DLP)計畫如此重要。

您的Umbrella DLP解決方案旨在保護您的組織免受這些風險。這裡是三個最緊迫的使用情形，我們的解決方案可幫助您立即解決這些問題，只需大約5分鐘的時間即可實施。

A.遵守GDPR、HIPPA和PCI-DSS等資料隱私法規：

1. 轉到Umbrella控制面板中的Policies > Management > Data Loss Prevention Policy。
2. 開始建立新的DLP規則。只需按一下右上角的Add Rule，然後選擇Real Time Rule。
3. 為您的規則指定一個易於識別的名稱（如「ChatGPT保護」），然後選擇符合您需求的嚴重性級別（從低到嚴重的所有級別）。
4. 在「分類」部分，選擇一個或多個與您的組織相關的內建符合性分類。例如，這可以是「內建GDPR分類」或「內建PCI分類」。
5. 在身份部分，選擇要監視和保護的所有身份。如果可行，我們建議廣泛選擇全面覆蓋範圍。
6. 轉到Destinations部分，選擇Destination Lists and Applications for Inclusion，然後選擇OpenAI ChatGPT。
7. 現在，是時候採取行動了。在Action部分，可以選擇Monitor或Block。如果您對此不熟悉，我們建議從「監控」操作開始。這允許您觀察使用模式並對潛在風險和益處做出更明智的決策。
8. 如果您已選擇「Monitor」操作，請確保一週或一個月後檢視DLP報告。這將顯示誰正在與ChatGPT共用敏感資訊，以及何時幫助您確定是否需要「阻止」操作。

B.個人身份資訊保護：要保護組織中的PII免受ChatGPT風險，只需使用與上面相同的說明，但在步驟4中，選擇「內建PII分類」而不是合規性分類。

C.保護原始碼和智慧財產權： 如果您的組織將ChatGPT用於涉及原始碼或其他智慧財產權的活動，請使用以下步驟：

1. 首先，建立新的原始碼資料分類。導航到Policies > Management > Policy Components > Data Classification。按一下右上角的Add按鈕，為資料分類指定一個可識別的名稱，如「原始碼分類」。
2. 從內建資料識別符號清單中選擇Source Code。
3. 按一下「Save」。
4. 儲存之後，重新訪問上述「遵守資料隱私法規」的說明，但在步驟4中，選擇您新建立的原始碼資料分類，而不是內建的資料分類。

該過程非常簡單，只需幾分鐘時間，但為您的組織帶來的安全性和合規性益處卻非常寶貴。我們敦促您儘快採取這些步驟來加強資料保護。

要瞭解有關生成AI風險以及Umbrella如何保護您的更多資訊，請觀看網路研討會保護敏感資料免受ChatGPT使用。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。