

Configura DLP per proteggere i dati sensibili dall'utilizzo con ChatGPT

Sommario

[Introduzione](#)

[Panoramica](#)

Introduzione

In questo documento viene descritto come utilizzare Data Loss Prevention (DLP) per proteggere i dati sensibili dall'utilizzo da parte di ChatGPT.

Panoramica

Il mondo dell'intelligenza artificiale è in fermento, con innovazioni come il modello linguistico di OpenAI, ChatGPT, che guida la carica. Questa potenza dell'intelligenza artificiale sta crescendo a un ritmo vertiginoso, trasformando numerose industrie con le sue conversazioni intelligenti e sensibili al contesto. Ma con questi progressi entusiasmanti si presentano alcune potenziali sfide, in particolare i rischi di perdita dei dati.

Pensate a ChatGPT come un partner di conversazione super-intelligente che genera testo basato su ciò che gli fornite. Ora, se il mix contiene informazioni riservate che non vengono gestite correttamente, c'è il rischio di una violazione dei dati. Ecco perché è importante disporre di un piano completo di prevenzione della perdita dei dati (DLP).

La soluzione Umbrella DLP è stata progettata per proteggere l'organizzazione da questi rischi. Ecco tre casi di utilizzo pressanti che la nostra soluzione può aiutare a risolvere immediatamente e richiede solo circa 5 minuti per l'implementazione.

A. Conformità alle norme sulla privacy dei dati, quali GDPR, HIPPA e PCI-DSS:

1. Accedi a Politiche > Gestione > Politica di prevenzione della perdita dei dati nel dashboard Umbrella.
2. Avvia la creazione di una nuova regola di prevenzione della perdita dei dati. È sufficiente fare clic su Add Rule (Aggiungi regola) nella parte superiore destra e selezionare Real Time Rule (Regola in tempo reale).
3. Assegnare alla regola un nome facilmente riconoscibile, ad esempio 'Protezione GPT chat', e scegliere il livello di gravità (da Basso a Critico) più adatto alle proprie esigenze.
4. Nella sezione Classificazioni selezionare una o più classificazioni di conformità predefinite rilevanti per l'organizzazione. Potrebbe trattarsi, ad esempio, della classificazione GDPR incorporata o della classificazione PCI incorporata.
5. Nella sezione Identità, selezionare tutte le identità che si desidera monitorare e

- proteggere. Se possibile, si consiglia una vasta selezione per una copertura completa.
6. Passare alla sezione Destinazioni, selezionare Elenchi di destinazioni e Applicazioni per inclusione, quindi scegliere OpenAI ChatGPT.
 7. Ora è tempo di agire. Nella sezione Azione è possibile scegliere tra Monitoraggio o Blocco. Se non si ha familiarità con questa operazione, si consiglia di iniziare con l'azione 'Esegui monitoraggio'. Ciò consente di osservare i modelli di utilizzo e di prendere una decisione più informata sui potenziali rischi e vantaggi.
 8. Se hai scelto l'azione "Monitor", controlla il report di prevenzione della perdita dei dati dopo una settimana o un mese. Questo mostra chi condivide informazioni riservate con ChatGPT e quando, aiutandoti a decidere se è necessaria un'azione 'Blocca'.

B. Protezione delle informazioni personali: Per proteggere i PII dell'organizzazione dai rischi di ChatGPT, è sufficiente utilizzare le stesse istruzioni di cui sopra, ma al passo 4, selezionare la 'Classificazione PII incorporata' invece delle classificazioni di conformità.

C. Protezione del codice sorgente e della proprietà intellettuale: Se l'organizzazione utilizza ChatGPT per attività che coinvolgono il codice sorgente o altre proprietà intellettuali, eseguire la procedura seguente:

1. Creare innanzitutto una nuova classificazione dei dati del codice sorgente. Passare a Criteri > Gestione > Componenti dei criteri > Classificazione dati. Fare clic sul pulsante Add in alto a destra e assegnare alla classificazione dei dati un nome riconoscibile, ad esempio 'Source Code Classification'.
2. Scegliere Codice sorgente dall'elenco degli identificatori dati predefiniti.
3. Fare clic su Save (Salva).
4. Dopo il salvataggio, rivedere le istruzioni per la "Conformità alle norme sulla privacy dei dati" sopra riportate, ma al passo 4, scegliere la classificazione dei dati del codice sorgente appena creata invece di quelle incorporate.

Il processo è semplice e richiede solo pochi minuti, ma i vantaggi per la sicurezza e la conformità dell'organizzazione sono inestimabili. Esortiamo i clienti ad adottare queste misure il più presto possibile per rafforzare la protezione dei dati.

Per ulteriori informazioni sui rischi dell'intelligenza artificiale generativa e su come Umbrella può proteggerti, guarda il webinar [Proteggi i tuoi dati sensibili dall'utilizzo di ChatGPT](#).

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).