Konfigurieren von DLP zum Schutz vertraulicher Daten vor der Verwendung durch ChatGPT

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie mithilfe des Schutzes vor Datenverlust (DLP) vertrauliche Daten vor der Verwendung durch ChatGPT schützen.

Überblick

Die Welt der künstlichen Intelligenz brummt, und Innovationen wie das OpenAI-Sprachmodell ChatGPT führen die Kampagne an. Dieses KI-Kraftpaket wächst rasant und verändert mit seinen intelligenten, kontextsensitiven Gesprächen zahlreiche Branchen. Diese spannenden Fortschritte bringen jedoch auch einige potenzielle Herausforderungen mit sich - insbesondere das Risiko von Datenverlusten.

Stellen Sie sich ChatGPT als einen superintelligenten Gesprächspartner vor, der Text basierend auf dem generiert, was Sie ihm zuführen. Wenn es also sensible Informationen gibt, die nicht richtig verarbeitet werden, besteht das Risiko von Datensicherheitsverletzungen. Dies unterstreicht, warum es so wichtig ist, einen umfassenden Plan zum Schutz vor Datenverlust (Data Loss Prevention, DLP) zu haben.

Ihre Umbrella DLP-Lösung wurde entwickelt, um Ihr Unternehmen vor diesen Risiken zu schützen. Hier sind drei drängende Anwendungsfälle, die Sie mit unserer Lösung sofort angehen können und die nur ca. 5 Minuten in Anspruch nehmen.

A. Einhaltung von Datenschutzbestimmungen wie DSGVO, HIPPA und PCI-DSS:

1. Gehen Sie zu Policies > Management > Data Loss Prevention Policy in Ihrem Umbrella Dashboard.
2. Erstellen Sie eine neue SvD-Regel. Klicken Sie einfach oben rechts auf Add Rule (Regel hinzufügen), und wählen Sie Real Time Rule (Echtzeitregel).
3. Geben Sie Ihrer Regel einen leicht zu erkennenden Namen, z. B. "ChatGPT Protection", und wählen Sie den Schweregrad (von Niedrig bis Kritisch) aus, der Ihren Anforderungen entspricht.
4. Wählen Sie im Abschnitt Klassifizierungen eine oder mehrere für Ihr Unternehmen relevante integrierte Konformitätsklassifizierungen aus. Dies könnte beispielsweise die "integrierte DSGVO-Klassifizierung" oder die "integrierte PCI-Klassifizierung" sein.
5. Wählen Sie im Abschnitt Identitäten alle Identitäten aus, die überwacht und geschützt

werden sollen. Wenn möglich, empfehlen wir eine große Auswahl für eine umfassende Abdeckung.
6. Gehen Sie zum Abschnitt Ziele, wählen Sie Ziellisten und Anwendungen für die Integration aus, und wählen Sie dann OpenAI ChatGPT aus.
7. Jetzt ist es Zeit zu handeln. Im Abschnitt Aktion können Sie entweder Überwachen oder Blockieren auswählen. Wenn Sie neu sind, empfehlen wir Ihnen, mit der Aktion "Überwachen" zu beginnen. Auf diese Weise können Sie Nutzungsmuster beobachten und eine fundiertere Entscheidung über die potenziellen Risiken und Vorteile treffen.
8. Wenn Sie die Aktion 'Überwachen' ausgewählt haben, überprüfen Sie den SvD-Bericht nach einer Woche oder einem Monat. Dies zeigt Ihnen, wer sensible Informationen mit ChatGPT und wann teilt, und hilft Ihnen zu entscheiden, ob eine 'Block' Aktion erforderlich ist.

B. Schutz von personenbezogenen Daten (PII): Um die PII in Ihrem Unternehmen vor ChatGPT-Risiken zu schützen, verwenden Sie einfach die gleichen Anweisungen wie oben, aber in Schritt 4, wählen Sie die "Integrierte PII-Klassifizierung" anstelle der Compliance-Klassifizierungen.

C. Schutz des Quellcodes und des geistigen Eigentums: Wenn Ihr Unternehmen ChatGPT für Aktivitäten verwendet, die Quellcode oder anderes geistiges Eigentum betreffen, gehen Sie wie folgt vor:

1. Erstellen Sie zunächst eine neue Quellcodedatenklassifizierung. Navigieren Sie zu Richtlinien > Verwaltung > Richtlinienkomponenten > Datenklassifizierung. Klicken Sie oben rechts auf die Schaltfläche Hinzufügen, und geben Sie Ihrer Datenklassifizierung einen erkennbaren Namen wie "Quellcodeklassifizierung".
2. Wählen Sie Quellcode aus der Liste der integrierten Datenbezeichner aus.
3. Klicken Sie auf Speichern.
4. Lesen Sie nach dem Speichern die Anweisungen für "Einhaltung der Datenschutzbestimmungen" weiter oben, wählen Sie jedoch in Schritt 4 die neu erstellte Quellcode-Datenklassifizierung anstelle der integrierten.

Der Prozess ist einfach und dauert nur wenige Minuten. Die Vorteile für die Sicherheit und Compliance Ihres Unternehmens sind jedoch von unschätzbarem Wert. Wir bitten Sie, diese Schritte so schnell wie möglich zu unternehmen, um Ihren Datenschutz zu stärken.

Möchten Sie mehr über Generative KI Risiken und wie Umbrella kann Sie schützen, sehen Sie sich das Webinar Schützen Sie Ihre sensiblen Daten vor ChatGPT Nutzung.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.