Überwachung vertraulicher Daten in AWS S3 und Azure Storage mit DLP

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie vertrauliche Daten in AWS S3 und Azure Storage mithilfe von Data Loss Prevention (DLP) überwachen.

Überblick

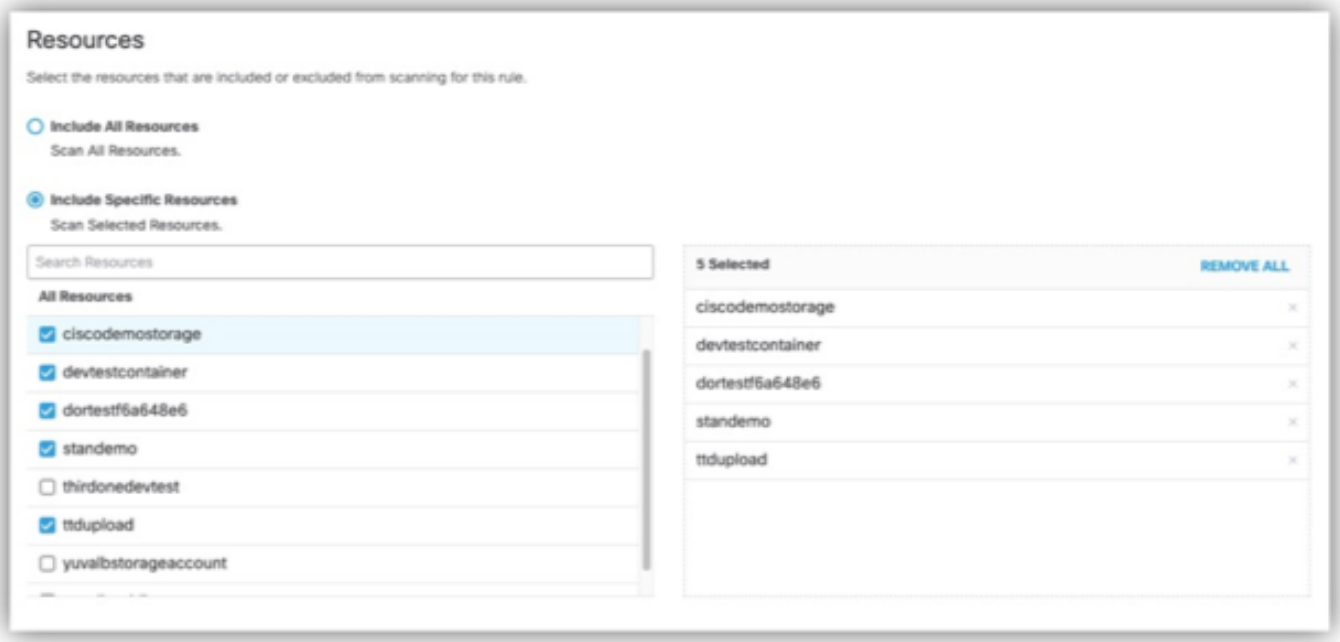
Mit neuen Connectors für AWS S3 und Azure Storage können Sie jetzt in Ihren Cloud-Umgebungen nach vertraulichen Daten suchen. Mithilfe dieser Funktionen können Sie freigegebene Anmeldeinformationen (z. B. API-Schlüssel, Schlüssel und Token) sowie vertrauliche Daten (z. B. personenbezogene Daten, Finanzdaten und Informationen aus dem Gesundheitswesen) erkennen und überwachen, die über das öffentliche Internet zugänglich sind.

Was wird in AWS S3 und Azure File Storage gescannt?

- AWS S3:
  DLP führt sowohl eine erste Suche nach bereits vorhandenen vertraulichen Daten als auch eine fortlaufende Überwachung für neue oder aktualisierte Dateien durch. Sie können angeben, welche S3-Buckets gescannt werden sollen, indem Sie sie in Ihrer SvD-Regel auswählen.

- Azure-Dateispeicher:
  DLP unterstützt die anfängliche Erkennung und laufende Überwachung neuer oder aktualisierter Dateien. Sie können die spezifischen Azure-Container auswählen, die in Ihrer SvD-Regel gescannt werden sollen.

Sie können DLP-Scans anpassen, indem Sie die genauen AWS S3-Buckets oder Azure-Container auswählen, die Ihren Anforderungen und Prioritäten entsprechen.



Unterstützte Reaktionsaktionen für AWS und Azure

Derzeit wird nur die Überwachung als Reaktionsaktion für AWS S3 und Azure Storage unterstützt. Automatische Wiederherstellungsaktionen, wie das Löschen oder Quarantäne von Dateien, sind nicht verfügbar. Dieser Ansatz vermeidet das Risiko, geschäftskritische IaaS-Umgebungen zu stören, und ermöglicht Ihnen gleichzeitig die effektive Überwachung der Gefährdung durch vertrauliche Daten.

Suchen Sie nach AWS S3-Buckets und Azure-Speicher-Blobs für die manuelle Problembehebung.

Zur Unterstützung der manuellen Korrektur enthält der SvD-Bericht detaillierte Informationen:

- Der Bericht zeigt den tatsächlichen S3-Bucket- oder Blobnamen an, sodass die Suche in AWS- oder Azure-Konsolen vereinfacht wird.
- Jedes SvD-Verletzungsereignis enthält den Ressourcennamen, die Ziel-URL und, falls verfügbar, die Ressourcen-ID.
- Verwenden Sie diese Informationen, um DLP-Verletzungen in Ihren AWS S3-Buckets und Azure-Speicher-BLOBs effizient zu finden und zu beheben.

Zugehörige Ressourcen

Detaillierte Anleitungen finden Sie in der Umbrella-Dokumentation:

- Schutz vor Datenverlust für AWS-Tenants für SaaS-API aktivieren
- Schutz vor SaaS-API-Datenverlust für Azure-Tenants aktivieren

- Hinzufügen einer SaaS-API-Regel zur Richtlinie zum Schutz vor Datenverlust
- Bericht zum Schutz vor Datenverlust

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.