DLPを使用したAWS S3およびAzureストレージでの機密データ漏えいの監視

内容

はじめに

このドキュメントでは、データ損失防止(DLP)を使用してAWS S3およびAzure Storageの機密データの漏洩を監視する方法について説明します。

概要

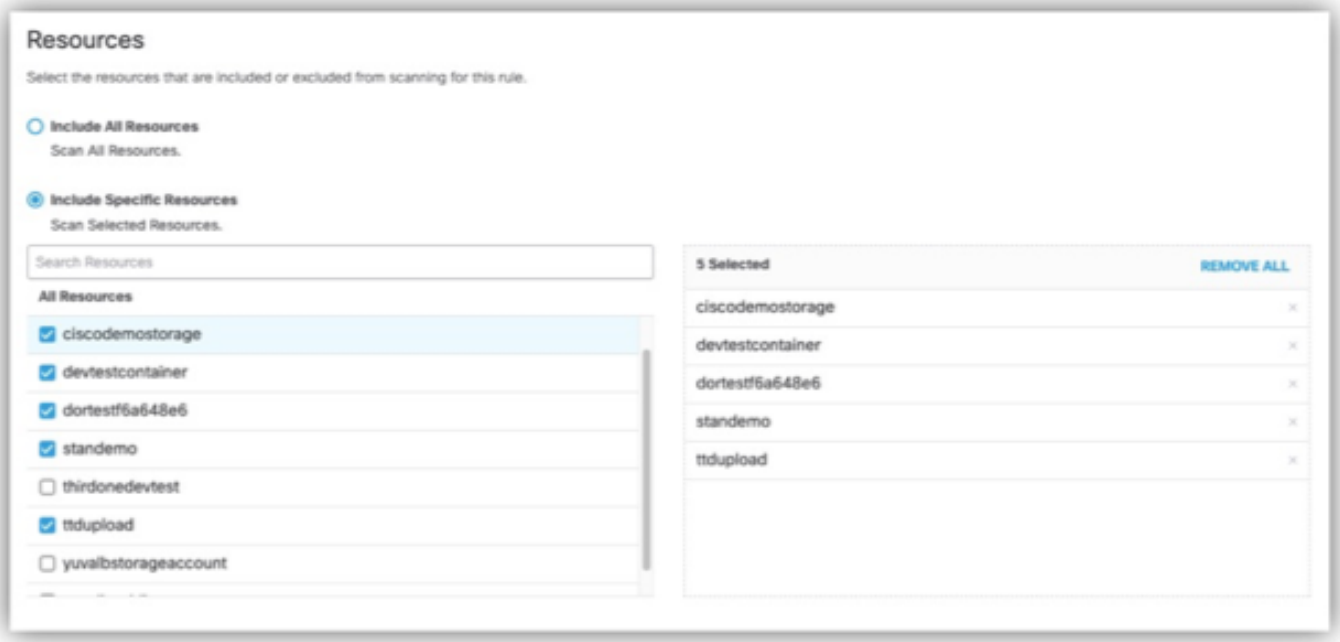
AWS S3とAzure Storageの新しいコネクタを使用すると、クラウド環境内の機密データの漏洩をスキャンできます。これらの機能により、APIキー、シークレット、トークンなどの公開された認証情報や、PII（個人特定可能な情報）、財務記録、パブリックWebに公開される医療情報などの機密データを検出して監視できます。

AWS S3とAzureファイルストレージでスキャンされる内容

- AWS S3:
  DLPは、既存の機密データに対する初期検出スキャンと、新規または更新されたファイルに対する継続的な監視の両方を実行します。スキャンするS3バケットを指定するには、DLPルールでS3バケットを選択します。

- Azureファイルストレージ：
  DLPは、新規または更新されたファイルの初期検出と継続的な監視をサポートします。DLPルール内でスキャンする特定のAzureコンテナーを選択できます。

ニーズと優先順位に合わせてAWS S3バケットまたはAzureコンテナを選択することで、DLPスキャンをカスタマイズできます。



AWSおよびAzureでサポートされる応答アクション

現在、AWS S3およびAzure Storageのレスポンスアクションとしてサポートされているのはモニタリングのみです。ファイルの削除や検疫などの自動修復アクションは使用できません。このアプローチにより、ミッションクリティカルなIaaS環境を中断するリスクを回避しながら、機密データの漏えいを効果的に監視できます。

手動修復のためのAWS S3バケットとAzure Storage Blobの検索

手動による修復を支援するために、DLPレポートには次の詳細情報が含まれます。

- レポートには実際のS3バケットまたはBLOBの名前が表示され、AWSまたはAzureコンソールでの検索が簡単になります。
- 各DLP違反イベントは、リソース名、宛先URL、および可能であればリソースIDを提供します。
- この情報を使用して、AWS S3バケットおよびAzureストレージBLOB内でDLP違反を効率的に見つけて対処します。

関連するリソース

詳細なガイダンスについては、Umbrellaのドキュメントを参照してください。

- AWSテナントのSaaS APIデータ損失保護を有効にする
- AzureテナントのSaaS APIデータ損失保護を有効にする
- データ損失防止ポリシーへのSaaS APIルールの追加
- データ損失防止レポート

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。