AWS S3およびAzure Storageでのマルウェアのリスクをクラウドマルウェアで監視

内容

はじめに

このドキュメントでは、クラウドマルウェアを使用してAWS S3およびAzure Storageのマルウェアリスクを監視および対処する方法について説明します。

概要

この機能を使用すると、AWS S3およびAzure Storage環境内のマルウェアリスクを検出および監視できます。主な使用例は、資格情報を盗んだり脆弱性を悪用したりする可能性のあるマルウェアに感染したファイルを特定し、環境内や他の環境に移動するリスクを高めることです。

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。この制限により、ミッションクリティカルなサービスの偶発的な中断を防止しながら、機密データの漏洩やマルウェアのリスクを監視できます。

関連するリソース

- AWSテナントのクラウドマルウェア防御を有効にする
- Azureテナントのクラウドマルウェア防御を有効にする

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。