Umbrellaクラウドマルウェアスキャン用にMicrosoft 365の監査ロギングを設定する

内容

はじめに

このドキュメントでは、Umbrellaクラウドマルウェアスキャンのために Microsoft 365の監査ロギングを有効にする方法について説明します。

概要

クラウドマルウェアスキャンのためにCisco UmbrellaをMicrosoft 365（以前のOffice 365）と統合するには、Microsoft 365でユーザイベントの監査を有効にする必要があります（デフォルトでは有効になっていない場合があります）。 この記事では、Microsoft Purviewコンプライアンスポータルで監査ログを有効にする方法について説明します。

クラウドマルウェア機能の詳細については、Cisco Umbrellaのドキュメントを参照してください。

監査ログを有効にする

Microsoft 365で監査ログを有効にするには、次の手順に従います。

1. https://compliance.microsoft.comのMicrosoft Purviewコンプライアンスポータルで、Solutions > Auditの順に選択します。
    - または、直接Auditページに移動するには、https://compliance.microsoft.com/auditlogsearchを使用します。
2. 組織の監査がオンになっていない場合は、ユーザーと管理者のアクティビティの記録を開始するよう求めるバナーが表示されます。
3. Start recording user and admin activityバナーを選択します。

監査が機能し始めるまでに約24時間かかる場合があることに注意してください。監査ログの詳細については、Microsoftのドキュメントを参照するか、MSサポートパートナーにお問い合わせください。

Cisco Umbrellaでクラウドマルウェアレポートを機能させるには、ユーザ/ファイルアクティビティに関連する監査がMicrosoft 365のPurviewコンプライアンスポータルの監査ページに表示される必要があります。

例：

4404249123348

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。