SlackとServiceNowでのSaaS API DLPの自動修復の有効化と設定

内容

はじめに

このドキュメントでは、SlackテナントとServiceNowテナントでSaaS API DLPの自動修復を有効にし、設定する方法について説明します。

概要

SlackおよびServiceNowテナントの機密データの漏洩を検出し、自動的に修復できるようになりました。これにより、コンプライアンスを維持し、他のシステムの知的財産や資格情報などの機密データの漏洩を防ぐことができます。

サポート対象プラットフォームの新しいテナントの許可

管理者は、UmbrellaダッシュボードのSaaS APIデータ損失防止(DLP)機能を使用して、SlackとServiceNowの新しいテナントを認証できます。

1. Umbrellaダッシュボードで、ADMIN > AUTHENTICATION > PLATFORMSの順に選択します。
2. プロンプトに従って新しいテナントを認証します。

SaaS API DLPでサポートされる自動修復

- サービス開始：
  SaaS API DLPは自動隔離をサポートします。隔離されたファイルは、シスコの隔離テーブルに保存されます。このテーブルにアクセスできるのは、テナントを認証した管理者だけです。

- 余裕期間：
  SaaS API DLPは、ファイルとメッセージの自動削除をサポートします。

感染したファイルの自動修復の設定

管理者は、機密データの漏洩を自動的に修復するようにSaaS API DLPを設定できます。

SaaS API DLPルールで応答アクションを設定します。

1. Umbrellaダッシュボードで、POLICIES > MANAGEMENT > DATA LOSS PREVENTION POLICYの順に選択します。
2. 「規則を追加」をクリックします。
3. SelectSAAS API RULE』を参照してください。
4. 自動修復を有効にするには、Response Actionセクションで desiredACTIONを設定します。

詳細情報の検索

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。

- SlackテナントのSaaS APIデータ損失保護を有効にする
- ServiceNowテナントのSaaS APIデータ損失保護を有効にする

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。