すべての宛先に対するリアルタイムDLPフォームデータブロッキングのトラブルシューティング

内容

はじめに

このドキュメントでは、すべてのフォームデータをブロックするためのリアルタイムデータ損失保護(DLP)ルールの設定に関連する問題をトラブルシューティングする方法について説明します。

背景説明

すべてのフォームデータをブロックするようにリアルタイムのDLPルールを設定する場合、真の肯定と偽の肯定の両方がクラウドアプリケーションに意図しない結果を引き起こすリスクがあります。このような結果は、ユーザがログインページを使用できない可能性など、クラウドアプリケーションの正常な動作に影響を与える可能性があります。この記事の目的は、これらのリスクを強調し、発生する可能性のある問題に対処するためのトラブルシューティング手順を提供することです。

トラブルシュート

リアルタイムDLPルールですべてのフォームデータをブロックすることによって問題が発生した場合は、次の手順が問題のトラブルシューティングと解決に役立ちます。

1. データIDの調整：この手順は、機密データを効果的にブロックすることと、正当なフォームデータを中断せずに通過させることとの間でバランスを取るのに役立ちます。

    - Data Loss Preventionレポート(Reporting > Additional Reports > Data Loss Prevention)を介してブロックされたDLPイベントの詳細を確認し、DLPルールをトリガーする特定のデータ識別子を特定します。

    - 必要に応じて照合する機能を維持しながら、公差レベルを調整するか、近接条件を追加して誤検出を減らすことによって、データ識別子を調整することを検討してください。

2. ブロックされたURLを除外 – URLを除外することで、アプリケーションのログインページやその他の重要なコンポーネントが、ブロックしているDLPルールの影響を受けないようにすることができます。

    - Activity Search(Reporting > Core Reports > Activity Search)およびDLPイベントの詳細を使用してアクティビティログを分析し、ブロックされているURLを特定します。
    - これらのURLを、[除外する宛先リストとアプリケーションの選択]で構成した宛先リストに追加します。

3. DLPルールの動作の変更 – 問題が解決せず、予期しない結果がすべてのフォームデータをブロックする利点を上回る場合は、フォームデータのスキャンを停止するようにDLPの動作を変更する必要があります。単に「審査したアプリケーションのファイルアップロードとフォームデータのみ」を選択するだけで、動作を変更できます。

結論

すべてのフォームデータをブロックするようにリアルタイムDLPルールを設定する場合、意図しない結果に関連するリスクを認識することが重要です。これらのリスクは、ログインページの使用を含め、クラウドアプリケーションの円滑な運用に影響を与える可能性があります。このガイドに記載されているトラブルシューティングステップを使用して、データ保護を維持しながら、これらのリスクを軽減し、クラウドアプリケーションが正常に機能することを確認します。

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。