Umbrella DLPの一般提供について

内容

[はじめに](#)
[背景説明](#)
[定義と制御](#)
[検出と適用](#)
[モニタとレポート](#)

はじめに

このドキュメントでは、Umbrellaデータ損失防止(DLP)の一般的なアベイラビリティについて説明します。

背景説明

Cisco Umbrellaは、シスコのSASEアーキテクチャのコアコンポーネントの1つです。以前はスタンドアロンのセキュリティサービスやアプライアンスであった複数のコンポーネントを、クラウドネイティブの単一のソリューションに統合します。

本日は、Umbrella DLPの一般提供を開始します。データ保護の概念は確かに新しいものではありませんが、ユーザがインターネットやクラウドアプリケーションに直接接続し、従来のオンプレミスセキュリティを回避するようになるにつれ、より複雑になっています。Cisco Umbrellaのデータ損失防止は、この複雑さを簡素化するのに役立ちます。インラインでWebトラフィックを検査するため、柔軟な制御によって機密データをリアルタイムで監視およびブロックできます。

定義と制御

- PII（個人を特定できる情報）、財務詳細、PHI（個人の健康情報）などのコンテンツをカバーする80以上のデータ識別子を活用し、特定のコンテンツを対象にして誤検出を減らすようにカスタマイズ可能
- プロジェクトコード名などのカスタムキーワードを使用してユーザー定義辞書を作成する
- きめ細かい制御を可能にする柔軟なポリシーを作成し、組織固有のデータ識別子をターゲットの特定のユーザ、グループ、ロケーション、クラウドアプリケーション、および宛先に適用

検出と適用

- 高スループット、低遅延、柔軟なスケールで機密データをインライン分析
- スケーラブルなSSL復号化にUmbrella SWGプロキシを活用
- 機密データフローを分析して、クラウドアプリケーションと任意の宛先へのファイルアップロードを選択

- 不要な宛先に送信される機密データや、認定アプリケーションで機密データが漏洩する可能性を検出してブロックし、データ漏洩イベントの発生を防止

モニタとレポート

ID、ファイル名、宛先、分類、パターン一致、抜粋、トリガーされたルールなどの詳細情報を含むドリルダウンレポートを取得できます。

詳細については、Umbrellaのドキュメントを参照してください。

- データ分類の管理
- データ損失防止ポリシーの管理
- データ損失防止レポート

Umbrellaサブスクリプションにクラウドネイティブの DLP機能を統合することで、コンプライアンスの目標を達成すると同時に、セキュリティスタックを簡素化し、SASEへの移行において次のステップを踏み出すことができます。

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。