ライセンス変更後にSIEMから失われるセキュアアクセスファイルのイベントログ

内容

問題

DNSログが正常に配信され続けている間、SIEMがAWS S3ストレージからファイルイベントログを受信しなくなりました。ファイルイベントデータコネクタは、SIEMインターフェイスに「切断」アイコンを表示しました。表示されなくなったログは、DLP/IPS関連のファイルイベントレコードとして識別されました。DNS層のログは、問題が発生した期間を通じて機能し続けました。

移行時にUmbrellaとSecure Accessの両方を使用し、ログを同じAWSバケットに送信していました。キーは回転され、正常に動作していることが確認されました。スキーマのバージョンはバージョン10で、バージョン16が使用可能であることが判明しました。

環境

- UmbrellaとSecure Accessの両方の設定を備えたCisco Secure Access組織
- ログエクスポート用のAWS S3ストレージ統合
- Microsoft Sentinel SIEMプラットフォーム
- スキーマバージョン10は使用中です（バージョン16が使用可能）
- Secure Accessライセンスは、2026年6月23日にAdvantageからEssentialsに変更されました
- ファイルイベントログの最終観察日：2026年6月24日

解決方法

調査の結果、ファイルイベントログはDLP/IPS機能に関連していることが判明しました。これには特定のライセンス機能が必要です。根本原因は、次の分析で特定されました。

ステップ1：トラフィック分析

セキュアアクセスのアクティビティ検索を確認して、トラフィックパターンを確認します。

1.- Activity Searchに移動し、Webトラフィックや悪意のある廃棄イベントをフィルタリングします。分析では、DNSトラフィックは存在するものの、過去30日間のWebトラフィックイベントは表示されず、ファイルインスペクションが有効なルールは特定されませんでした。
2.- トラフィックフロー> CSAレポートのログ> S3バケット – SIEM。

ステップ2：ライセンス履歴の確認

1. – ファイルのイベントログの停止のタイミングに合わせて、Secure Accessのライセンス履歴を確認して変更を特定します。

2.- Secure Access > Admin > Subscriptionの順に移動し、現在のライセンスレベルと機能の要約を表示します。

調査の結果、2026年6月23日にSecure AccessライセンスがSecure Access AdvantageからSecure Access Essentialsに変更されたことが明らかになりました。この変更は、ファイルイベントログの表示が停止するタイミングに合わせて行われました。

ステップ3：機能の確認

現在のライセンスレベルにどの機能が含まれているかを確認します。ファイルイベントログを生成するDLPおよびIPS機能は、Secure Access Essentialsライセンス階層には含まれません。

ステップ4：確認と根本原因

ライセンス変更のタイミングは、ファイルイベントログの表示が停止した時点と完全に一致していました。DNSレイヤのロギングは機能し続け、それが主な要件であったため、現在のEssentialsライセンスではファイルイベントログを利用できないという理解で問題が解決しました。

原因

2026年6月23日にSecure Access AdvantageからSecure Access Essentialsにライセンスが変更されたため、ファイルイベントログの生成が停止しました。ファイルイベントログは、DLPおよびIPS機能に関連するもので、Essentialsライセンス階層には含まれません。ライセンスのダウングレードにより、これらの特定のログタイプを生成するファイルインスペクション機能へのアクセスが削除されました。

関連コンテンツ

- シスコのテクニカルサポートとダウンロード

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。