コネクタによって読み取られるウィンドウイベント/イベントIDの理解

内容

はじめに

このドキュメントでは、コネクタによってデフォルトで読み取られるウィンドウイベント/イベントIDについて説明します。

概要

技術的には、Umbrella仮想アプライアンス(VA)は、DNSクエリの送信元IPアドレスのみを表示します。ユーザをDNS要求に関連付けるために、VAはコネクタと連携して動作し、その結果、ユーザとIPのマッピングが行われます。

コネクタは、ドメインコントローラのセキュリティイベントログから特定のイベントIDを持つイベントを読み取ります。次に、これらのイベントが解析され、ユーザ名と送信元IPアドレスがVAに送信されます。VAは、その送信元IPとユーザ間のマッピングを作成します。

これらのイベントがドメインコントローラによって監査されていない場合、VAのマッピングプロセスは正しく実行されません。この記事では、コネクタがデフォルトで監視するイベントIDのタイプについて詳しく説明します。

イベントID	説明
4624	イベント4624は、ログオンの種類、ユーザーの場所、またはアカウントの種類に関係なく、ローカルコンピューターへのログオン試行が成功するたびに記録されます。
528	イベント528は、ネットワークログオンの場合を除き、アカウントがローカルコンピュータにログオンするたびにログに記録されます。ログオンに使用されるアカウントがローカルSAMアカウントであるか、ドメインアカウントであるかにかかわらず、イベント528が記録されます。
540	イベント540は、ネットワーク上の他の場所にいるユーザーが、このコンピュー

	タ上のサーバーサービスによって提供されるリソース（共有フォルダなど）に接続するとログに記録されます。
4768	このイベントはドメインコントローラにのみ記録され、このイベントの成功および失敗の両方のインスタンスが記録されます。
4769	このイベントIDは、成功したサービスチケット要求と失敗したサービスチケット要求の両方に使用されます。

コネクタがドメインコントローラのセキュリティイベントログから直接イベントを読み取ることができない場合は、Umbrellaを使用してサポートチケットを発行し、これをWMIサブスクリプションに変更するように依頼することができます。WMIサブスクリプションの場合、コネクタは上記のすべてのイベントをサブスクライブします。また、コネクタは、次に示すようにEventIDを使用してログオフイベントをサブスクライブします。デフォルトでは、コネクタはセキュリティイベントログからこれらのログオフイベントを読み取らないことに注意してください。

イベントID	説明
538	ネットワーク接続、対話型ログオン、またはその他の種類のログオンのいずれからログオフするかに関係なく、イベント538が常にログに記録されます(ログオンの種類のグラフについては、イベント528を参照してください)。
4647	このイベントはログオンセッションの終了を通知し、ログオンIDを使用してログオンイベント4624に関連付けることができます。
4634	また、このイベントはログオンセッションの終了を通知し、ログオンIDを使用してログオンイベント4624に関連付けることができます。

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。