

高度な脅威ソリューションのビデオポータルリンクを理解する

内容

概要

このドキュメントでは、Cisco Secure Endpoint、Cisco SecureXなどの高度な脅威ソリューション(ATS)製品のCisco Video Portal(CVP)リンクについて説明します。

問題

TACエンジニアは、ユーザが一般的なタスクやトラブルシューティングシナリオを実行できるように共有できる、ATS製品の承認済みカタログを1つ必要とします。

環境

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、ラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。ネットワークが稼働中の場合は、作業を進める前にコマンドの潜在的な影響を評価します。

解決方法

適切なビデオを選択して共有するには、次の手順を使用します。

1. 製品の領域(たとえば、セキュアエンドポイント、SecureX、Secure Malware Analytics)を特定します。
2. タスクまたはトラブルシューティングのシナリオを、表の中で最も近いビデオタイトルにドラッグしてください。
3. 宛先リンクのタイプを選択します。

- シスコがホストするバージョンのCisco Video Portal。
 - YouTube (YouTubeリンクが優先または必須の場合)
4. 選択したリンクを共有し、ユーザがビデオにアクセスして目的のタスクを完了できることを確認します。

Secure Endpoint

タイトル	シスコビデオポータルリンク	YouTubeリンク
Windowsのセキュアエンドポイントに必要なルート証明書のリストのトラブルシューティング	リンク1	リンク2
Windowsポリシーの設定	適用外	リンク2
Windowsでのエンドポイント用AMPのインストール	適用外	リンク2
MAC用AMPコネクタのインストールと設定	適用外	リンク2

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、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。