Umbrellaダッシュボード：新機能とファイルインスペクション

内容

はじめに

このドキュメントでは、新しいUmbrellaダッシュボードについて説明します。

Umbrellaダッシュボードに何か違いがありますか。さて、私たちは素晴らしいUmbrella機能の新しいセットに人々を移動するプロセスを開始していることを発表します。最初に紹介する機能は、ファイル検査です。ファイルインスペクションは、IDのダウンロードをスキャンして、悪意のあるコードが含まれているかどうかを確認し、含まれている場合はブロックします。

この新機能を活用していただくために、新しいセキュリティレポートと更新されたセキュリティレポート、および新しいポリシー作成エクスペリエンスもリリースされています。 この機能は、ユーザにさらにクラウドベースのセキュリティを提供するために、Intelligent Proxyインフラストラクチャの拡張を中心に構築された将来のリリースに向けて計画している機能の1つです。

これらの機能は、お客様に対して少しずつ展開されています。これらの機能に関するアラートをダッシュボードで受信した場合は、その機能を使用できます。これらの機能を早期に導入したい場合は、umbrella-support@cisco.comまでお問い合わせください。

ファイルインスペクション機能は、Umbrella InsightsまたはUmbrellaプラットフォームパッケージを使用しているお客様だけが利用できます。 パッケージの詳細については、ここをクリックし、ご不明な点がございましたら、シスコの代理店までお問い合わせください。

ファイル検査の利点を活用するには？

ポリシーウィザードでは、サマリーページから、または新しいポリシーの作成時にファイルインスペクションを有効にできます。

レポート側では、Umbrellaダッシュボードのレポートナビゲーションセクションが更新され、新しいレポートや更新されたレポートを簡単に見つけることができます。この機能を有効にする方法と、いくつかのレポートを確認する方法について説明します。

ファイルインスペクションの有効化

ファイルインスペクションはインテリジェントプロキシの機能で、疑わしいドメインでホストされる悪意のあるコンテンツをファイルでスキャンする機能を追加することで、範囲と機能を拡張します。疑わしいドメインは信頼されておらず、悪意があるようにも認識されておらず、ドメインの「グレーリスト」にリストされています。

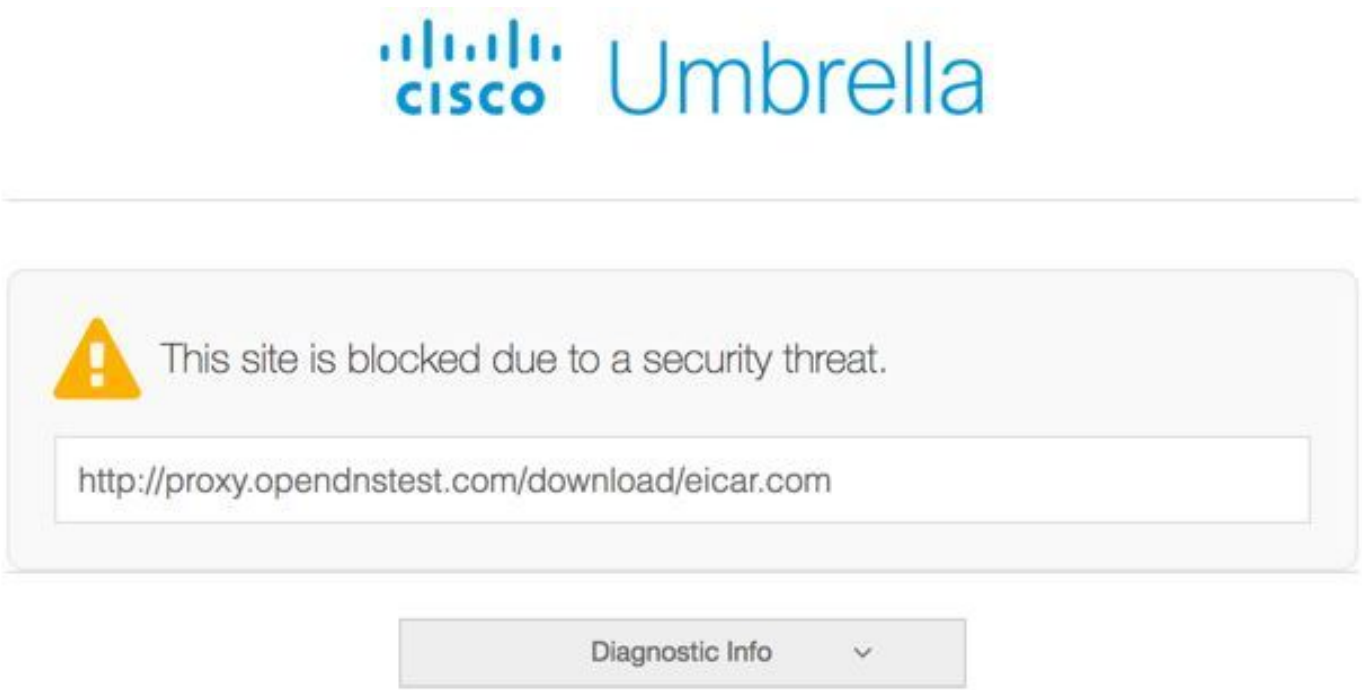
Umbrellaポリシーウィザードを使用すると、ファイルインスペクションを簡単に実装できます。ポリシー>ポリシーリストに移動し、ポリシーを展開するか、+（追加）アイコンをクリックして新しいポリシーを作成します。ポリシーウィザードで、[概要]ページの[ファイルインスペクション]が有効になっていることを確認します。または、[詳細設定]の[インテリジェントプロキシ]を有効にした後で、[ファイルの検査]を新しいポリシーで必ずオンにしてください。 この機能の詳細なドキュメントについては、https://docs.umbrella.com/deployment-umbrella/docs/file-inspectionを参照してください。

この機能を最大限に活用するために、SSL復号化を有効にすることをお勧めします。

ファイル検査のテスト

ファイルインスペクションが有効なポリシーに登録されているデバイスから：

1. http://proxy.opendnstest.com/download/eicar.com を参照します。
2. 次のようなブロックページが表示されます。



ファイルインスペクションのレポート

ブロックされた内容（およびブロックされた日時、理由、方法）の可視性を高めるための支援の

一環として、Umbrellaの一部のレポートを更新しました。これには、改訂されたセキュリティアクティビティレポートが含まれます。

- セキュリティ概要レポート
  グラフやチャートを使用して、ネットワークアクティビティのスナップショットを簡単に読むことができます。IDとそのトラフィックの状況を迅速に確認し、問題が発生している可能性のある場所を特定できます。詳細については、ここを参照してください。

- セキュリティアクティビティレポート
  Umbrella脅威インテリジェンスによってフラグ付けされているが、必ずしもブロックされていないセキュリティイベントを強調表示します。これには、インテリジェントプロキシおよびファイルインスペクションを使用してフィルタリングされたセキュリティイベントが含まれます。このレポートは、ブロックされた内容、ブロックされた理由とその方法を示す上で特に重要です。詳細については、ここを参照してください。

- アクティビティ検索レポート
  さまざまなIDからのすべてのDNS、URL、およびIP要求の結果を日時の降順に並べて検索できます。このレポートには、選択した期間におけるUmbrella内のすべてのアクティビティが一覧表示されます。フィルタを使用すると、検索対象を絞り込んで必要なアイテムのみを表示できます。詳細については、ここを参照してください。

新しく更新されたナビゲーションにより、これらのレポートにも簡単にアクセスできます。 左側のメニューペインを展開し、ダッシュボード内の他の場所から直接レポートにジャンプするだけです。

私の考えを君にわかってもらうにはどうすればいい？

これらの新機能についてのご意見をお聞かせください。ご質問やご意見がありましたら、お寄せください。フィードバックをumbrella-support@cisco.comに送信し、できるだけ詳細な情報をお知らせください。たとえば、スクリーンショット、使用しているブラウザ、OS、およびこれらの機能を使用しているシナリオなどがあります。

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。