Umbrellaアプリケーション検出レポートでのアプリケーション属性の使用

内容

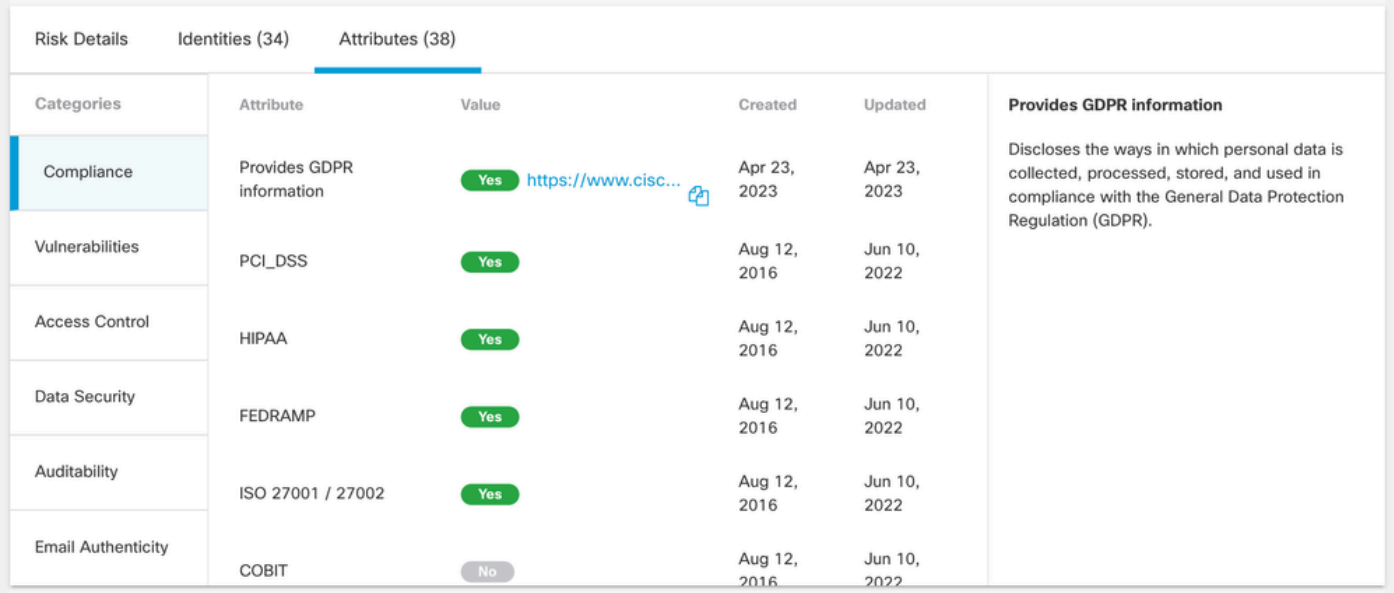
はじめに

このドキュメントでは、Cisco Umbrellaアプリケーション検出レポートのアプリケーション属性機能を使用する方法について説明します。

概要

Cisco Umbrellaアプリケーションディスカバリレポートのアプリケーション属性機能は、リスクアセスメント機能に役立ちます。

アプリケーション属性は、特定されたすべてのアプリケーションに対してCisco Umbrellaが提供するコンテキスト情報を大幅に拡大し、Cisco Umbrellaのお客様が、ニーズに合わせて十分な情報に基づいてポリシーを決定できるようにします。



18263606083476

これらのアプリケーション属性により、Cisco Umbrellaの管理者は、環境内で新しく検出された

アプリケーションに関する追加のコンテキストを構築できると同時に、リスクの高いアプリケーションを判断してブロックするまでの時間を大幅に短縮できます。

Cisco Umbrellaの管理者は、6つのカテゴリで最大38のアプリケーション属性を使用して、アプリケーションに関する幅広い補足的な洞察を得ることができ、既存のリスク分類を補完します。これらの洞察には、次のものが含まれます。

- コンプライアンス：ベンダーとアプリケーションの両方に対する、PCI-DSS、GDPR、HIPPA、FEDRAMPなどの認定の存在。
- 脆弱性：PODDLEやBEASTなどのアプリケーションに関連する既知のTLS/SSL脆弱性。
- アクセスコントロール:SSOやMFAなどのアクセスコントロールメカニズムをサポートします。
- データセキュリティ：TLSバージョンのサポート、弱い暗号などの転送中データの仕様。
- 監査機能：可用性の監査。
- Eメールの信頼性：Eメールの信頼性を制御する手段。

属性情報が更新されたかどうかを確認するにはどうすればよいですか。

各アプリケーション属性には作成日と更新日の両方があり、管理者は情報が意思決定に関連しているかどうかを判断できます。

この機能にアクセスするには、どうすればよいですか。

アプリケーション属性にアクセスするには、レポート>コアレポート> App Discovery > [アプリケーション] > Attributesの順に選択します。

追加情報

Cisco Umbrella SIGガイド

Cisco Umbrella DNSガイド

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。