2016 の機能概要

この記事では、2016 年に Cisco Defense Orchestrator に追加された機能の一部について説明します

2016 年 12 月

2016年12月22日

NAT ポリシー管理

Cisco Defense Orchestrator は、使いやすいナビゲーションウィザードと高度なインターフェイスベースのダイアグラムを介してNATポリシーの読み取り、編集、検索、および作成をサポートし、ASA デバイスで定義された NAT ポリシーの完全なリスト（およびその順序）を表示するようになりました。

2016 年 12 月 15 日

廃止された名前（オブジェクト）の変換

お使いのデバイスの設定には、レガシーの（廃止された）名前が含まれていますか。Cisco Defense Orchestrator では、オブジェクトの問題の解決中に、オブジェクト、オブジェクトグループ、名前全体を調査して、ポリシーで使用されるすべてのオブジェクトに一貫性を持たせ、名前からオブジェクトへの変換を支援できるようになりました。

2016 年 11 月

2016 年 11 月 18 日

完全にシャドウされたルールのサポート

すべてのトラフィックはルールセットの順序でルールによって処理されるため、意図したトラフィックを処理しない余分なネットワークポリシーをフィルタリングして特定できるようになりました。ネットワークポリシーに変更を加えると、編集または追加されたルールが別のルールによってシャドウされている場合、CDO はアラートを出します。

2016 年 11 月 8 日

オンプレミスの Secure Device Connector

Cisco Defense Orchestrator は、CDO とサポートされているデバイスおよびサービスとの間の直接通信を可能にします。この通信は、リモートロケーションと CDO クラウドサービス間のプロキシとして機能する CDO Secure Device Connector（SDC）によって可能になります。このサービスは、次の 2 つの展開モデルで利用できるようになりました。

オンプレミス セキュア デバイス コネクタ – オンプレミス セキュア デバイス コネクタは、要求されたアカウント専用の事前構成された仮想アプライアンスです。

クラウド セキュア デバイス コネクタ – すべてのクラウド セキュア デバイス コネクタは自動的にプロビジョニングされ、Cisco Defense Orchestrator チームによって管理されます。

2016 年 9 月

2016 年 9 月 29 日

ログの変更

Cisco Defense Orchestrator を介して実行されたアプリケーション（レイヤ 7）とネットワーク（レイヤ 3）の両方のポリシー変更を、オンボードのデバイスとサービス全体で 1 つのビューで継続的にキャプチャします。新しい変更ログには、最新の変更がひと目でわかるビューが一覧表示されます。さらに、デバイス、変更ステータス、ユーザーなどでリビジョンを並べ替えたり、フィルタリングしたりできます。新しい変更ログ機能により、組織は次のことができます。

- ネットワークおよびアプリケーションポリシーの変更（新規、編集、および削除されたルール、オンボードまたは削除されたデバイスおよびサービスなど）の前後のインライン増分表示（差分）

- ポリシー変更の競合の検出（Cisco Defense Orchestrator の外部で発生）およびデバイスまたはサービスとの間の上書き
- インシデントの調査またはトラブルシューティング中に、誰が、何を、いつ、に回答可能
- 一般的な形式またはサードパーティの監視システムにエクスポート

（注） Cisco Defense Orchestrator によって現在管理されているデバイスとサービスは、最初の展開または読み取りの後にのみ、変更ログイベントの収集を開始します。詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Secure Logging Analytics for FTD Devices」を参照してください。

ヒット率。Cisco Defense Orchestrator により、ネットワーク運用ユーザーは、安全でスケーラブルなポリシーのオーケストレーションに加えて、ポリシールールの結果を評価できるようになり、より正確なポリシー分析のためのシンプルな視覚化と、根本原因への迅速な実用的なピボットをすべてクラウドから 1 つのペインで行うことができます。新しいヒット率機能により、組織は次のことができます。

- 古くて一致したことのないポリシールールを排除し、セキュリティ体制を強化
- ボトルネックを即座に特定し、正確で効率的な優先順位付けを実施することにより、ファイアウォールのパフォーマンスを最適化（トリガーされたポリシールールの優先順位が高くなります）
- 設定されたデータ保持（1 年間）のデバイスまたはポリシールールがリセットされても、ヒット率の履歴情報を維持
- 実用的な情報に基づいて、疑わしいシャドウおよび未使用のルールの検証を強化。それらの更新または削除についての疑問を解消
- 事前定義された時間間隔（日、週、月、年）と実際のヒットのスケール（ゼロ、>100、>100k など）を活用して、ポリシー全体のコンテキストでポリシールールの使用を視覚化し、ネットワークを通過するパケットへの影響を評価

2016 年 9 月 23 日

ユーザーインターフェイスの再設計：ライトテーマへの変更

Cisco Defense Orchestrator のユーザーエクスペリエンスを、軽量でまったく新しいユーザー エクスペリエンス テーマで再設計し、より直感的で自明の Cisco スタイルに合わせます。お試しください。

複数のオブジェクトのサポート

Cisco Defense Orchestrator オブジェクト管理により、オブジェクトおよびオブジェクトグループ値のインライン編集が可能になり、単一のアクセスリストパラメータで複数のオブジェクト

を参照できるようになりました。ユーザー定義のオブジェクトグループに自動的に割り当てます（dm_inline_* オブジェクトを作成する必要はありません）。

アウトオブバンドポリシーの変更を承認または拒否する

実行されたリモート変更または変更内容（デバイスまたはサービス上）を特定するだけでなく、特定されたアウトオブバンド変更をリアルタイムで承認または拒否する機能により、ポリシー オーケストレーションの実施が強化されました。

2016 年 8 月

2016 年 8 月 18 日

委任管理サポート

委任管理のサポート。Cisco Defense Orchestrator を使用すると、アカウントのセキュリティを維持し、アカウント（テナント）間の完全なデータ分離を維持しながら、ユーザーごとに複数のアカウント（テナント）を管理して、割り当てられたアカウント間のピボットをより簡単かつ迅速に行うことができます。

事前定義されたテンプレートのインポートとエクスポート

事前定義テンプレートのインポートを有効にします。組織内またはサードパーティから入手可能な事前定義されたデバイス構成テンプレートを活用して、組織内のすべてのデバイスとサービスをオンボーディングするスケーラブルなオーケストレーションを可能にします。

デバイスとサービスの接続ステータス管理

デバイス接続ステータスの評価。新しい [再接続（Reconnect）] ボタンが追加され、デバイスとサービスの可用性の状態を継続的に監視できるようになり、変更またはアクションを自動的にまたはオンデマンドで実行する必要がある場合にアラートが表示されます（デバイスログイン情報の更新、デバイス証明書の更新など）。

2016 年 8 月 11 日

テンプレート管理の強化

テンプレート管理の機能強化。新規のデバイステンプレート構成ファイルを作成するとき、または既存のデバイステンプレート構成ファイルを更新するとき、Cisco Defense Orchestrator ユーザーは、デバイス構成ファイル全体を簡単に検索し、アカウントのデバイス間で使用するために、新規または既存のパラメータに複数の値を割り当てることができるようになりました。

.テンプレートの作成と管理の詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Templates」を参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。