ネットワーク セキュリティ アドバイザリの識別

セキュリティアドバイザリの概要

Cisco Product Security Incident Response Team（PSIRTT; プロダクト セキュリティ インシデント レスポンス チーム）は、シスコ製品セキュリティインシデントに対応し、セキュリティ脆弱性ポリシーを規制し、シスコのセキュリティアドバイザリとアラートを推奨します。

セキュリティ アドバイザリ ツールは、これらの推奨されるアドバイザリを使用して、Catalyst Center 内のインベントリをスキャンし、既知の脆弱性を持つデバイスを検出します。

前提条件

セキュリティ アドバイザリ ツールを使用するには、機械推論パッケージをインストールする必要があります。『Cisco DNA Center Administrator Guide』の「*Download and Install Packages and Updates*」を参照してください。

オブザーバとして Catalyst Center にログインすると、ホームページで [Security Advisories] ツールを表示できません。

セキュリティアドバイザリの表示

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Security Advisories] ウィンドウを初めて起動する場合は、[Scan Network] をクリックします。

Catalyst Center では、セキュリティの問題を特定して自動分析を改善するためにナレッジベースを使用します。最新のセキュリティアドバイザリを表示するには、定期的にナレッジベースを更新することをお勧めします。

a) 左上隅にあるメニューアイコンをクリックして次を選択します：**System** > **Settings** > **Machine Reasoning Engine** の順に選択します。
b) [Import] をクリックするか、[Download Latest] をクリックして最新の使用可能なナレッジベースをダウンロードします。ダウンロードが完了したら、[Import] をクリックしてください。
c) 自動更新に登録するには、[AUTO UPDATE] トグルボタンをクリックします。

（注） 上部に表示されるバナーの [here] リンクをクリックして、デバイス設定に基づいてカスタマイズされた Field Notice へのアクセスを提供する新しいトライアルを作成します。

ステップ 3 [ADVISORIES] 領域には、[Critical]、[High]、[Medium]、[Low]、[Informational]、[Unknown] など、ネットワークに対するそれぞれの影響の割合が表示されます。

ステップ 4 スキャンは、各デバイスに関連付けられたライセンスに基づいてデバイスで実行されます。[SCAN CRITERIA] 領域では、次の順序に従って、アドバイザリをデバイスと一致させる必要があります。

- [Software Version]：スキャンは、**Cisco DNA Essentials** ライセンスを持つデバイスでソフトウェアバージョンに基づいて実行されます。
- [Custom]：スキャンは、**Cisco DNA Advantage** ライセンスを持つデバイスで、ソフトウェアバージョンと、デバイスの実行コンフィギュレーションに対するアドバイザリ（ある場合）に関して入力されたカスタム設定に基づいて実行されます。
- [Advanced]：スキャンは、**Cisco CX Cloud Success Track** の利用資格を持つデバイスで、ソフトウェアバージョン、設定、および運用データに基づいて実行されます。

  試用期間中はライセンス資格が適用されず、すべてのデバイスが [Advanced] レベルでスキャンされます。

（注）
- セキュリティアドバイザリ ダッシュボードにはシスコが公開しているセキュリティアドバイザリが表示されます。アドバイザリは現行のソフトウェアイメージに基づいており、ネットワーク上のデバイスに影響する場合があります。脆弱性が実際に存在するかどうかを判断するには、設定、プラットフォームの詳細、またはその他の基準をさらに詳しく分析する必要があります。
- セキュリティアドバイザリ スキャンは、サポートされている最小ソフトウェアバージョン以上を実行しているルータおよびスイッチでのみ使用できます。詳細については、『Catalyst Center Compatibility Matrix』を参照してください。
- 表示されるセキュリティアドバイザリは、「シスコのセキュリティ脆弱性ポリシー」に基づいています。

次の表に、使用できる情報を記載します。

カラム	説明
アドバイザリ ID	ネットワークで検出されたセキュリティアドバイザリの ID。ID をクリックして、それぞれのアドバイザリ Web ページに移動します。
アドバイザリタイトル	ネットワークデバイスに適用可能なセキュリティ脆弱性アドバイザリの名前。
CVSS スコア	共通脆弱性評価システム（CVSS）モデルに基づいて評価されたスコア。
Impact	脆弱性がネットワークに及ぼす影響。
CVE	脆弱性の Common Vulnerabilities and Exposures（CVE）識別子。
デバイス	脆弱性の影響を受けるデバイスの数。この特定のアドバイザリに基づいて脆弱性が存在する可能性のあるデバイスを表示するには、番号をクリックし、必要に応じてデバイスをアップグレードします。
Match Type	検出された脆弱性が [Image Version] の一致と [Configuration] の一致のどちらに基づくかを示します。
検出以降の期間（日数)	脆弱性が検出されてからの経過日数。
Last updated	アドバイザリが最後に更新された日付。

ステップ 5 [FAILED DEVICES] エリアには、将来の日付にスケジュールされたデバイススキャンに関する情報が表示されます。

（注） [FAILED DEVICES] エリアは、スキャンで失敗したデバイスがあり、システムがスキャンを自動的にスケジュールする場合にのみ表示されます。

ステップ 6 [Advisories] テーブルで、[All] タブをクリックして、すべてのアドバイザリをリストします。

ステップ 7 [Advisories] テーブルで、[Affecting Devices] タブをクリックして、影響するデバイスに基づいたアドバイザリを表示します。

[Devices] テーブルには、[Device Name]、[Device Family]、[Device Series]、[IP Address]、[Advisories]、[Advisories (Suppressed)]、[Platform]、[Image Version]、[Scan Status]、[Scan Criteria]、[Site]、および [Reachability] に基づいてデバイスが一覧表示されます。

ステップ 8 各デバイスに適用可能なアドバイザリの数を表示するには、[Devices] タブをクリックします。

a) デバイスに一致するものをすべて表示するには、アドバイザリの数をクリックします。

b) デバイストポロジを表示するには、右上隅にあるトポロジアイコンをクリックします。トポロジ内のデバイスをクリックすると、デバイスに一致するすべてのアドバイザリが表示されます。

デバイスの横にあるロックアイコンは、デバイスに適用可能な 1 つ以上のアドバイザリがあることを示します。

[Fixed Version] 列には、アドバイザリが適用されたバージョンが表示されます。この列に示されているバージョンにアップグレードすることで、デバイス上のアドバイザリを削除できます。

ステップ 9 [Re-scan Network] をクリックして、ネットワークのスキャンを再度実行します。

ネットワークを再スキャンして、自動構成スキャンに基づいてセキュリティアドバイザリを特定するには、ネットワークを再スキャンしてセキュリティアドバイザリを特定する （6 ページ）を参照してください。

セキュリティアドバイザリスキャンのスケジュール設定

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Scan Network] をクリックします。

[Scan Network] ウィンドウが表示されます。

ステップ 3 セキュリティアドバイザリをすぐにスキャンするには、[Now] オプションボタンをクリックし、[Start] をクリックします。

ステップ 4 スキャンを後で実行するようにスケジュールするには、[Later] オプションボタンをクリックし、日付と時刻を指定します。

ステップ 5 [Time Zone] ドロップダウンリストを使用して、スキャンのスケジュール設定に使用するタイムゾーンを選択します。

ステップ 6 繰り返しオプションとして [None]（デフォルト）、[Daily]、[Weekly] のいずれかを選択します。

ステップ 7 [Run at Interval] フィールドに、スキャンの繰り返しの間隔（日または週の数）を入力します。

ステップ 8 （オプション）スケジュールの終了日や終了までの回数を指定する場合は、[Set Schedule End] チェックボックスをオンにします。

a) スキャン終了日をスケジュールするには、[End Date] オプションボタンをクリックし、日付と時刻を定義します。

b) スキャンの繰り返し回数を定義するには、[End After] オプションボタンをクリックします。

ステップ 9 [Schedule] をクリックします。

ステップ 10 左上隅にあるメニューアイコンをクリックして次を選択します：**[Activities]** > **[Tasks]** の順に選択して、スキャンのスケジュールと繰り返しを確認します。

（注） Catalyst Center リリース 2.1.1.x 以降では、シスコによるテレメトリの収集を許可するかどうかを選択できます。収集を許可すると、cisco.com ID、システムテレメトリ、機能使用状況テレメトリ、ネットワーク デバイス インベントリ、およびソフトウェア利用資格の情報が収集されます。テレメトリは、アプリケーションごとや機能ごとではなく、Catalyst Center 全体について開示されます。Catalyst Center 2.1.1.x 以降では、テレメトリの収集は必須です。収集されたテレメトリは、ユーザーが使用している機能の開発に役立てられます。収集されるデータの詳しいリストについては、「*Cisco DNA Center* のデータシート」を参照してください。

セキュリティ アドバイザリ スキャンの実行時に収集されるテレメトリデータは次のとおりです。

- ナレッジパッケージの自動更新が設定されているかどうか。
- 繰り返しのスキャンおよび繰り返しのレポートが設定されているかどうか。
- 実行されたレポートの数。
- ソフトウェアのバージョンと設定に基づいて一致するセキュリティアドバイザリがあるデバイスの数。
- 各スキャンの受理と拒否の数。
- 検索で入力された手動設定とそれに関連するアドバイザリ。
- ソフトウェアのバージョンと設定（製品ファミリを含む）が一致するアドバイザリの数。
- 他のカテゴリ（アドバイザリなし、不明、サポート対象外）に基づくデバイスの数。
- スキャンの成功、失敗、終了の数。
- 平均スキャン時間。

セキュリティアドバイザリのために呼び出される CLI コマンド

Catalyst Center は、ネットワークデバイスで CLI コマンドを実行してネットワークデバイスの構成と運用データを収集し、その情報を CX Cloud に送信して処理され、可能性があるセキュリティアドバイザリやバグのリスクを可視化します。Catalyst Center はセキュリティアドバイザリのための次の CLI コマンドを呼び出します。

- **show inventory**
- **show running-config**

- **show version**

ネットワークを再スキャンしてセキュリティアドバイザリを特定する

次の手順では、ネットワークを再スキャンして、自動構成スキャンに基づいてセキュリティアドバイザリを特定する方法について説明します。

始める前に

Cisco CX Cloud サービスを有効にする必要があります。詳細については、*Cisco Catalyst Center Administrator Guide*の「**Update the Machine Reasoning Knowledge Base**」を参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Tools]** > **[Security Advisories]** > **[Advisories]** の順に選択します。

ステップ 2 [Re-Scan Network] をクリックして、ネットワークスキャンを再度開始します。

ステップ 3 セキュリティアドバイザリをすぐに再スキャンするには、[Now] オプションボタンをクリックし、[Start] をクリックします。

ステップ 4 再スキャンを後で実行するようにスケジュールするには、[Later] オプションボタンをクリックし、詳細を指定します。詳細については、セキュリティ アドバイザリ スキャンのスケジュール設定 （4 ページ）を参照してください。

[Device] テーブルで、[Advisories] 列がアドバイザリの数で更新されます。

- Catalyst Center ネットワークの再スキャンは、プラットフォームの詳細や CX Cloud ソフトウェアのバージョンなどの他の詳細とともに、デバイスの実行コンフィギュレーションを送信します。情報は処理され、Catalyst Center に返送されます。Catalyst Center 上で実行されている Machine Reasoning Engine（MRE）は、Cisco CX Cloud によって提供されるデバイスに対してアドバイザリをマッピングします。
- Catalyst Center で特定のデバイスの正しいライセンスレベルを判断できない場合、セキュリティ アドバイザリ スキャンはソフトウェアバージョンごとのスキャンにフォールバックします。

アドバイザリに対するデバイスの表示/非表示

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。

ステップ 3 [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。

ステップ 4 デバイスのアドバイザリを非表示にするには、次の手順を実行します。

a) [Focus] ドロップダウンリストから、[Advisories] を選択します。
b) [Devices] 列で、デバイスを非表示にするアドバイザリに対応するデバイス数をクリックします。

[Active] タブには、これらのアドバイザリが発行されたデバイスの数が表示されます。

c) 非表示にするデバイスを選択し、[Suppress Device] をクリックします。

非表示にしたデバイスは、[Suppressed] タブで確認できます。

d) アドバイザリウィンドウを閉じ、このアドバイザリのデバイス数の変化を確認します。

ステップ 5 デバイスをアドバイザリに復元するには、次の手順を実行します。

a) [Focus] ドロップダウンリストから、[Advisories] を選択します。
b) [Devices] 列で、デバイスを再表示するアドバイザリに対応するデバイス数をクリックします。
c) [Suppressed] タブをクリックして、非表示のデバイスを表示します。
d) 再表示するデバイスを選択し、[Mark as Active] をクリックします。

復元されたデバイスは、[Active] タブで確認できます。

e) アドバイザリウィンドウを閉じ、このアドバイザリのデバイス数の変化を確認します。

デバイスに対するアドバイザリの表示/非表示

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。

ステップ 3 [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。

ステップ 4 デバイスのアドバイザリを非表示にするには、次の手順を実行します。

a) [Focus] ドロップダウンリストから、[Devices] を選択します。
b) [Advisories] 列で、アドバイザリを非表示にするデバイスに対応するアドバイザリカウントをクリックします。

[Active] タブには、このデバイスに対して発行されたアドバイザリの数が表示されます。

c) 非表示にするアドバイザリを選択し、[Suppress Advisory] をクリックします。

非表示のアドバイザリは、[Suppressed] タブで確認できます。

d) デバイスウィンドウを閉じ、このデバイスのアドバイザリカウントの変化を確認します。

ステップ 5 デバイスのアドバイザリを復元するには、次の手順を実行します。

a) [Focus] ドロップダウンリストから、[Devices] を選択します。
b) [Advisories] 列で、アドバイザリを再表示するデバイスに対応するアドバイザリカウントをクリックします。

c) [Suppressed] タブをクリックして、非表示のアドバイザリを表示します。
d) 再表示するアドバイザリを選択し、[Mark as Active] をクリックします。

復元されたアドバイザリは、[Active] タブで確認できます。

e) デバイスウィンドウを閉じ、このデバイスのアドバイザリカウントの変化を確認します。

新しいセキュリティアドバイザリ KB の通知の追加

セキュリティアドバイザリのナレッジバンドル（KB）は、機械推論エンジン（MRE）を使用してネットワークをスキャンします。新しいセキュリティアドバイザリの KB が利用可能になったときに通知するように Catalyst Center を設定できます。通知を有効にすると、新しいセキュリティアドバイザリの KB が利用可能になるたびに、Catalyst Center から視覚的な通知と実用的なアラートが表示されます。

次の手順では、新しいセキュリティアドバイザリの KB の通知を追加する方法について説明します。

始める前に

- Catalyst Center のコアパッケージをインストールする必要があります。*Cisco Catalyst Center Administrator Guide* の「パッケージと更新のダウンロードとインストール」を参照してください。
- 機械推論（MRE）パッケージをインストールする必要があります。*Cisco Catalyst Center Administrator Guide* の「パッケージと更新のダウンロードとインストール」を参照してください。
- 次のコンテナがシステムに存在している必要があります。
  - cnsr-reasoner
  - cloud connectivity/download

ステップ 1 Catalyst Center GUI の右上隅にある通知アイコンをクリックします。ドロップダウンメニューから、歯車のアイコンを選択して通知設定を表示します。

ステップ 2 [My Profile and Settings] ウィンドウで、[Security Advisories] オプションを選択してセキュリティアドバイザリ通知を有効にします。

ステップ 3 [保存（**Save**）] をクリックします。

ステップ 4 [Machine Reasoning Engine] ウィンドウで、[Download Latest] リンクをクリックして最新のナレッジバンドルをダウンロードします。

ステップ 5 ナレッジベースの設定を確認して更新します。

ステップ 6 [Security Advisory Settings] セクションで、繰り返しオプションとして [None]（デフォルト）、[Daily]、または [Weekly] を選択します。

ステップ 7 **[Notification Center]** > **[Go to Security Advisories]** の順に選択して、[Security Advisories] ツールウィンドウを直接表示します。

ステップ 8 新しくダウンロードしたセキュリティアドバイザリでネットワークを再スキャンします。詳細については、セキュリティ アドバイザリ スキャンのスケジュール設定 （4 ページ）を参照してください。

[Inventory] でのセキュリティアドバイザリの表示

Catalyst Center のセキュリティ フォーカス ビューでは、前回のセキュリティスキャンで取得したデータに基づいて、デバイスのセキュリティアドバイザリのリストを表示します。[Security Advisories] ツールから取得したデバイスデータは [Inventory] ウィンドウに表示されます。

次の手順を使用して、セキュリティアドバイザリを表示します。

始める前に

- Catalyst Center のコアパッケージをインストールする必要があります。*Cisco Catalyst Center Administrator Guide* の「パッケージと更新のダウンロードとインストール」を参照してください。
- 機械推論パッケージをインストールする必要があります。*Cisco Catalyst Center Administrator Guide* の「パッケージと更新のダウンロードとインストール」を参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Scan Network] をクリックします。

ステップ 3 セキュリティアドバイザリをすぐにスキャンするには、[Now] オプションボタンをクリックし、[Start] をクリックします。

ステップ 4 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

ステップ 5 [FOCUS: Inventory] ドロップダウンメニューから [Security] を選択します。
[Inventory] テーブルに [Advisories] 列が表示されます。

ステップ 6 [Device Details] ウィンドウで、デバイスを選択し、アドバイザリデータを確認します。

ステップ 7 [Manage All] をクリックして**セキュリティアドバイザリ** ツールに移動します。

一致パターンの追加

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。

ステップ 3 [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。

ステップ 4 アドバイザリを選択し、[Match Type] 列で [Add match pattern] をクリックします。

ステップ 5 [Add Configuration Match Pattern] ウィンドウで、[CONDITIONS] テキストボックスにデバイスと一致する条件を入力します。

ステップ 6 **[保存（Save）]** をクリックします。

一致パターンがアドバイザリに追加されます。

ステップ 7 [Scan Network] をクリックして、一致パターンに一致するデバイスの数を確認します。

一致パターンの AND/OR の定義

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。

ステップ 3 [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。

ステップ 4 アドバイザリを選択し、[Match Type] 列で [Add match pattern] をクリックします。

ステップ 5 [Add Configuration Match Pattern] ウィンドウで、次の手順を実行します。

a) [CONDITIONS] テキストボックスに条件を入力し、[Add] アイコンをクリックします。

b) ドロップダウンリストから、[AND] または [OR] を選択し、次の条件を入力します。

c) 条件を削除する場合は、[Remove] アイコンをクリックします。

d) **[保存（Save）]** をクリックします。
一致パターンがアドバイザリに追加されます。

ステップ 6 [Scan Network] をクリックして、一致パターンに一致するデバイスの数を確認します。

一致パターンの編集

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。

ステップ 3 [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。

ステップ 4 すでに一致パターンがあるアドバイザリを選択し、[Match Type] 列で [Edit match pattern] をクリックします。

ステップ 5 [Edit Configuration Match Pattern] ウィンドウで、[CONDITIONS] テキストボックスにデバイスと一致する条件を入力します。

ステップ 6 **[保存（Save）]** をクリックします。

一致パターンが変更されます。

ステップ 7 [Scan Network] をクリックして、一致パターンに一致するデバイスの数を確認します。

一致パターンの削除

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。

ステップ 3 [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。

ステップ 4 すでに一致パターンがあるアドバイザリを選択し、[Match Type] 列で [Edit match pattern] をクリックします。

ステップ 5 [Edit Configuration Match Pattern] ウィンドウで、[Delete] をクリックします。

一致パターンが削除されます。

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。