Cisco XDRの既知の問題

内容

はじめに

この記事では、Cisco XDRの既知の技術的な問題について説明します。

技術的な問題は、シスコが確認中、解決保留中、または期待どおりに動作していると見なすことができます。

既知の問題：

[インシデント（Incidents）]

現時点では、このXDR機能に関する既知の問題はありません。

調査

現時点では、このXDR機能に関する既知の問題はありません。

Control Center

1. – コントロールセンターのMTTRタイルは、「Closed: False Positive」、「Closed: Confirmed Threat」などの新しい状態のいずれかを使用して解決されたインシデントの不正確な数を示します。

ステータス：問題が特定され、解決が保留中

詳細：新しいインシデント状態が1月15日に導入されましたが、タイルはこれらの状態を考慮

していません。新しい解決状態は作業中と解釈されるため、そのインシデントが新しい状態の1つを使用して終了された場合でも、そのインシデントは作業中と見なされます。

回避策：なし

次のステップ：なし

予想される解決策：未定

シスコの統合

1.- Cisco XDR - Cisco Secure Endpoint integration link not working on Cisco XDR Portal

ステータス：問題が特定され、解決が保留中

詳細： Admin > Integrationsタブで、セキュアエンドポイントの「Enable」リンクが壊れています。イネーブルボタンを押すと、Threat Responseページにリダイレクトされ、セキュアエンドポイントコンソールに移動せずにXDR org selectorページにループします。

回避策：統合はCisco Secure Endpoint Portalから実行できます

次のステップ：シスコでは、この問題の修正の実装に取り組んでいます

予想される解決策：未定

2. Cisco XDR:Cisco Secure Firewallの完全統合

詳細：Cisco Defense Orchestrator(CDO)、Security Services Exchange(SSX)、およびSecurity Analytics and Logging(SAL)間のシームレスな統合を確実にするには、手動マッピングが必要です。このプロセスでは、Cisco TACに連絡して、必要な設定とマッピングを実行します。

回避策：TACに連絡して、関連するアカウントのリンクを作成し、システムが適切に統合されていることを確認してください。

予想される解決策：未定

サードパーティ製品との統合

1.- G-typeライセンスを持つMicrosoftのお客様は、XDR Microsoft統合を利用できません。

ステータス：設計通りの作業

詳細：Microsoft Gタイプの権限は、政府機関専用の制御環境でのみアクセスがプロビジョニングされます。

次のステップ：シスコはMicrosoftと協力して、Microsoft Gタイプの権限が提供されているMicrosoft GCC環境と統合するための要件を理解しています。可能であれば、Cisco XDRは、Microsoft Defender for Endpoint、O365、およびEntraIDのMicrosoft Gタイプのライセンスと統合する予定です。

予想される解決策：未定

資産

現時点では、このXDR機能に関する既知の問題はありません。

XDR自動化

1.- XDR Automate Incident Automation Rulesの実行が予期せず停止する

ステータス：問題が特定され、解決が保留中

詳細：ワークフローとトリガーを利用したインシデント自動化ルールが予期せず停止します。XDRユーザインターフェイスでは、ワークフローの実行時間のメトリックを確認する場合を除き、これは示されません。 これにより、お客様は問題の継続期間に応じて、実行されるワークフローの数が減少するか、またはゼロになります。

次のステップ：シスコは、これをXDRバックエンド内の問題として特定し、解決に取り組んでいます。また、この問題が今後発生しないように、モニタリング機能と状態追跡機能を追加で実装する予定です。

回避策：ルールを無効にしてから再度有効にして、トリガーと処理を行うワークフロールールの再起動を開始します。

予定解像度：2025年3月

アプライアンス/センサー

1.- Cisco XDR-Analytics - ONAの仮想環境でのインストールが、「checksum verification failed」を示すエラーで失敗する

ステータス：問題が特定され、解決が保留中

詳細：仮想環境にONAセンサーを導入すると、ISOがインストールプロセスを完了できず、エラーが発生します。

回避策：Ubuntu ISOを使用してUbuntu Server 24.04を個別にインストールし、高度なインストール手順に従ってONAをサービスとして実行します。 7.0 U2互換を使用する

次のステップ：シスコでは、この問題の修正の実装に取り組んでいます

解決策：次回のXDRセンサーバージョンのリリース

2.- Cisco XDR-Analytics:ETAプローブのみが設定されている場合に、ONAのセンサー詳細のトラフィックグラフが入力されない

ステータス：問題が特定され、解決が保留中

詳細：トラフィックグラフは、ONAがETAプローブのみで設定されている場合はトラフィックを示しません。

回避策：なし

次のステップ：シスコでは、この問題の修正の実装に取り組んでいます

3.- Cisco XDR-Analytics:シスコテレメトリブローカー(CTB)からのETAテレメトリは、ETAダッシュボードの入力には使用されません。
ステータス：問題が特定され、解決が保留中

詳細：CTBによって生成された、またはCTBを通じてアップロードされ、他のデバイスによって生成されたETAテレメトリは、ETAダッシュボードの入力には使用されません

回避策：ETAプローブを使用したONAの使用

次のステップ：なし

解決策：次回のXDRセンサーバージョンのリリース

セキュアクライアント

セキュアクライアントの問題を確認するには、記事に従ってください。

XDR-A

1. - XDR-Aでは、複数のIPアドレスや複数のホスト名を1つのデバイス名に関連付けることができます

状態：未解決/延期

詳細：複数のアクティブなIPアドレスをSNA/XDR-Aポータル内の1つのデバイスに関連付けることができます。これには、NVMデバイスと非NVMデバイスの両方を含めることができます。デバイスによっては、複数のホスト名を持つものもあります。 現在の実装に基づいて、デバイスの登録は複数のIPアドレス（ロケーション）を持つデバイスになる可能性があります。 これらのIPアドレスの一部は、ユーザのホームネットワークから取得され、組織のネットワークのIPアドレスと競合する可能性があります。

回避策：現在のところ、この問題の回避策はなく、問題は現在のアーキテクチャにまだ存在します。新しいアーキテクチャが実装されると、ONAとNVMの両方のソースからのネットワークアクティビティをOCSFに正規化してまとめることができるため、この問題の解決が将来的により適切になる可能性があります。

次のステップ：該当なし

解決策：将来/未定

解決済みの問題

1.- Mark Task Not Applicableオプションは、XDRインシデントの作成時にのみ考慮され、インシデントの更新時には考慮されません。

ステータス：解決済み

詳細：Cisco XDR Guided Response Playbookには、現在のインシデントに該当しないタスクを非表示にするオプションが用意されています。2024年10月、シスコはCisco XDRに対して、適用可能なオブザーバブルのないタスクを自動的に非表示にする機能拡張をリリースしました。この拡張機能は、インシデントが作成されると機能しますが、更新されても該当するタスクは評価されません。

次のステップ：修正の実装

Ciscoサポートに連絡する必要がある場合は、このリンクに記載されている指示に従ってください。

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。