Cisco Secure Endpointsカバレッジ要求のベストプラクティス

内容

概要

このドキュメントでは、既知の脅威が特定されているが、現在セキュアエンドポイントで検出されていない場合にTalosカバレッジを要求する際に使用する必要があるプロセスについて説明します。

さまざまな情報源

これらの脅威は複数のソースから特定され、公開される可能性があります。一般的に使用されるプラットフォームの一部を次に示します。

- 公開されたCisco CVE
- 公開されたCVE(Common Vulnerabilities and Exposures)
- Microsoftアドバイザリ
- サードパーティ製の脅威インテリジェンス

シスコは、Talosに情報のレビューと関連カバレッジの特定を依頼する前に、データソースが正規のものであることを確認したいと考えています。

問題となっている脅威に対するシスコの姿勢とカバレッジを確認するために、シスコとTalosのさまざまなソースを用意しています。これらは、新しいカバレッジリクエストをリクエストする前に確認する必要があります。

Cisco脆弱性ポータル

シスコ製品に関連するCVEの詳細については、次のポータルを参照してください。
https://sec.cloudapps.cisco.com/security/center/publicationListing.x

Talosポータル

この脅威がTalosによって調査されたか、現在調査中であるかを確認するには、Talos Intelligence Portalを最初に参照する必要があります。https://talosintelligence.com/

ターロスブログ

Talosによって評価および調査された脅威に関する情報は、Cisco Talosブログでも提供されています。https://blog.talosintelligence.com/

関連する情報の大部分は「脆弱性情報」で確認できます。この中には、公開されている「Microsoftアドバイザリ」も含まれています。

シスコ製品を使用した追加調査

シスコは、脅威ベクトル/ハッシュを確認し、セキュアエンドポイントが脅威のカバレッジを提供するかどうかを特定するのに役立つ複数の製品を提供しています。

Cisco SecureX Cisco Threat Response Investigation(CTR)

CTR調査の一環として脅威ベクトルを調査できます。詳細については、https://docs.securex.security.cisco.com/Threat-Response-Help/Content/investigate.htmlを参照してください。

Cisco XDR調査

Cisco XDRは、脅威ベクトルを調査するための拡張機能を提供します。機能の詳細については、https://docs.xdr.security.cisco.com/Content/Investigate/investigate.htmを参照してください。

シスコの役立つブログ

これらのブログでは、前のセクションで説明した機能の一部について確認してください。

https://blogs.cisco.com/tag/relevant-and-extended-detection-with-securex

次の手順

上記の手順でカバーされている脅威ベクトルが見つからない場合は、TACサポートリクエストを提出して、脅威のTalosカバレッジをリクエストできます。

https://www.cisco.com/c/en/us/support/index.html

カバレッジリクエストの評価と調査を迅速化するために、脅威に関する次の情報を要求します。

- 脅威インテリジェンスのソース(CVE/アドバイザリ/サードパーティによる調査/テクニカルノート/ブログ)
- 関連付けられたSHA256ハッシュ
- ファイルのサンプル（ある場合）

情報が入手可能になると、Talosは評価を行い、それに応じてリクエストを調査します。

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。