Cisco Security Integration v1 – インスタント デモ

最終更新日:2017 年 11 月 14 日

このデモンストレーションについて

この事前設定済みデモンストレーションのガイドには、次の内容が含まれています。

- 要件
- このソリューションについて
- はじめに
- シナリオ 1:シスコによる効果的なセキュリティ統合

要件

次の表に、本デモンストレーションに必要な要件の概要を示します。

表 1. 要件

必須	オプション
● ラップトップ	● なし

このソリューションについて

セキュリティに対するシスコの取り組みは、「最も効果的なセキュリティ アーキテクチャをどのように構築するか」という、純粋かつ実際的な問いかけから始まりました。

シスコでは、効果的なセキュリティは、セキュリティ スタックの各構成要素が連動することで達成されると考えています。そして、シームレスであることが重要です。

現状では、攻撃に対する対応の多くが、人が操作する複雑なワークフローに依存しています。侵害への対応を実行に移すまで、何ヵ月もかかる場合があります。なぜでしょうか。それは、その対応によって攻撃よりも破壊的な結果がもたらされることを恐れるからです。1 台のリモートのラップトップでマルウェアを見つけたときに、対応を全ネットワーク、全ラップトップに適用するとしたらどうでしょうか。自動的に、リアルタイムにです。1 ヵ所で発見したものを、他のあらゆる場所で阻止するのです。

お客様が一般的に費やす検出時間は数ヵ月から数時間にまで短縮されます。検出された脅威に対しては、ほぼ瞬時に体系的な対応がとられます。この考え方を他のドメインにも展開してみましょう。ネットワーク、マルウェア、Web、電子メールからのすべてのテレメトリを 1 ヵ所で監視できたらどうでしょうか。そこでは、容易にデータのピボットを行い、攻撃者の IT インフラストラクチャを分析して、攻撃の詳細を調査することができます。アナリストはすべてのインテリジェンスを 1 つの場所から確認できるため、スムーズに攻撃の調査フローを開始できます。そして脅威状況の進展に迅速に対応できます。簡単に言えば、シスコではそのテレメトリを蓄積し、まとめることで、ワークフローをシンプルにして対応を自動化できるようにします。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

はじめに

プレゼンテーションの前に

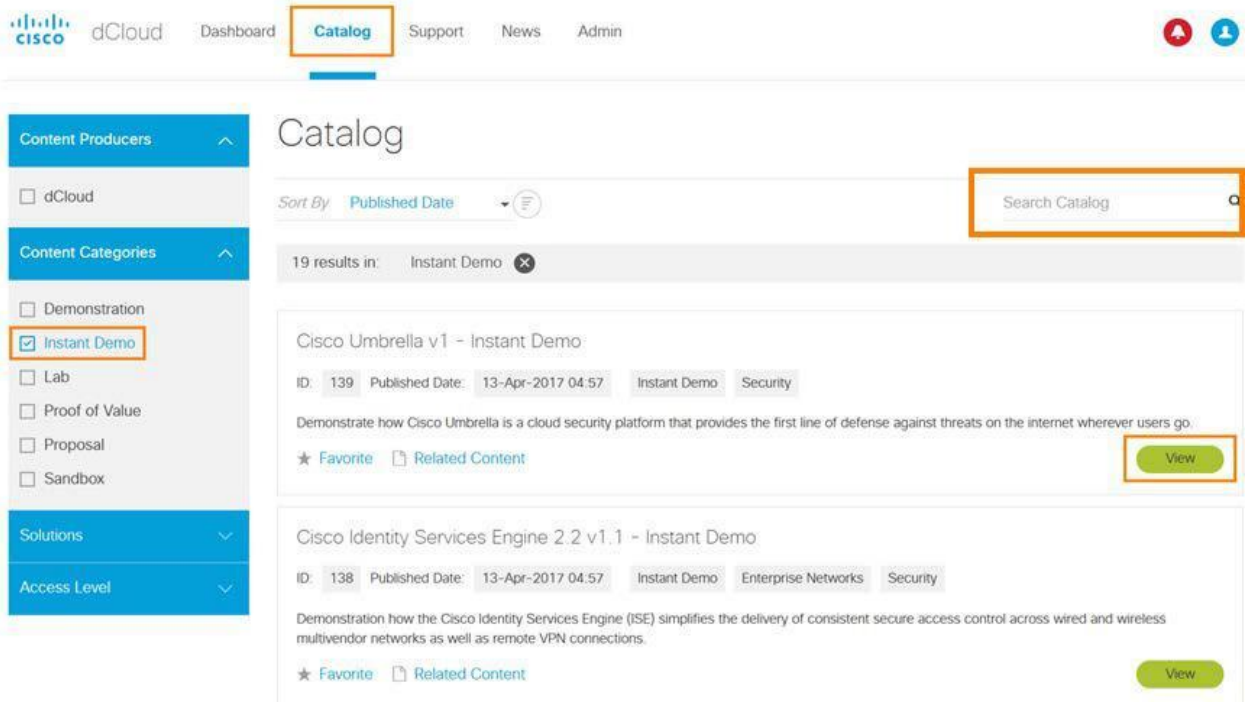
Cisco dCloud では、実際の対象者の前でプレゼンテーションを行う前に、アクティブなセッションを使用して、このドキュメントのタスクを実施しておくことを強く推奨します。そうすることで、ドキュメントとコンテンツの構成に慣れることができます。

場合によっては、環境を元の構成にリセットするため、このガイドに従った後に新しいセッションをスケジュールする必要があります。

プレゼンテーションを成功させるためには、入念な準備が不可欠です。

次の手順に従ってコンテンツのセッションをスケジュールし、プレゼンテーション環境を設定します。

1. [カタログ（Catalog）] をクリックして、サイド バーから [インスタント デモ（Instant Demo）] を選択します。これで、すべての dCloud インスタント デモが一覧表示されます。
2. **検索またはスクロール**して、カタログから Cisco Security Integration を見つけます。該当する [表示（View）] ボタンをクリックします。



3. Cisco Security Integration のデモが自動的に開始されます。

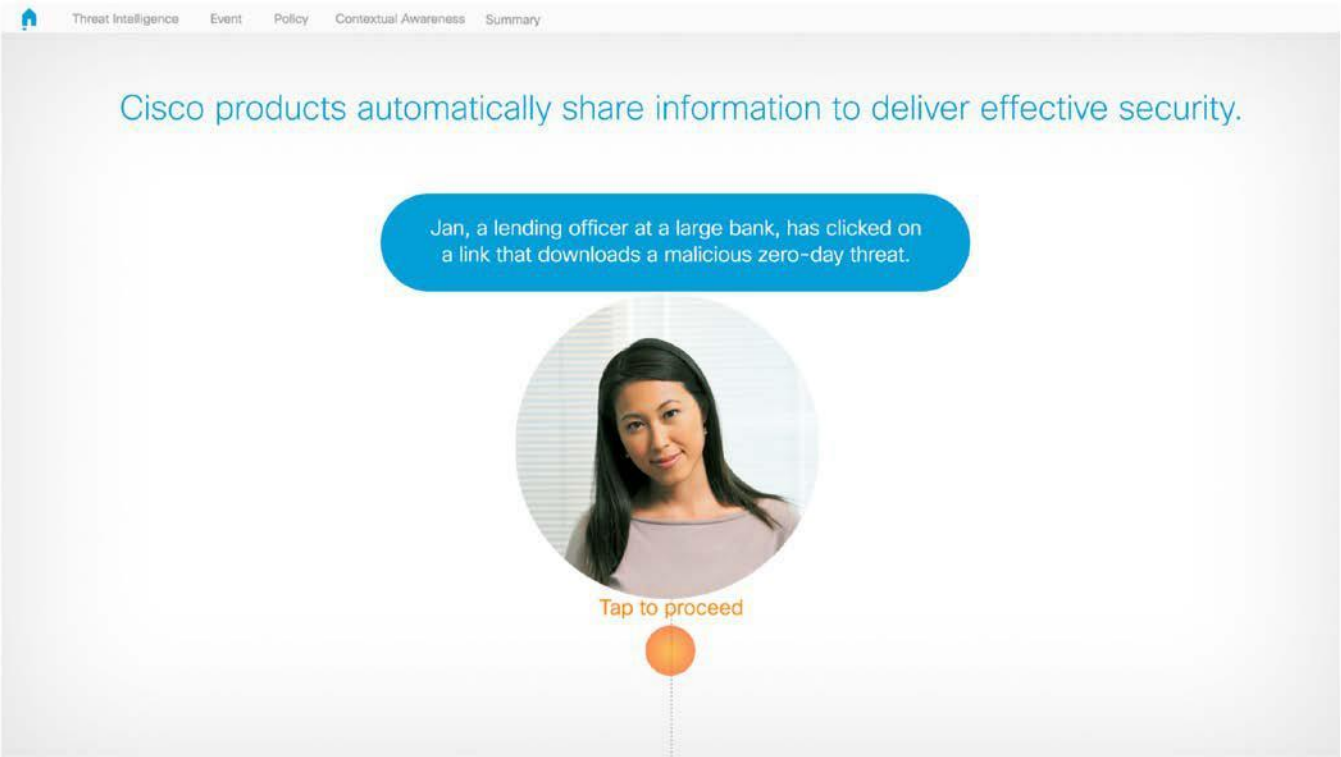
© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

シナリオ 1.　シスコによる効果的なセキュリティ統合

手順

これから数分間で、シスコの各セキュリティ ソリューションがネイティブに連動することで、セキュリティを強化し、検出時間を短縮する例をお見せします。

Jan を紹介します。



オレンジ色の丸をクリックすると、デモンストレーションが開始します。

Jan は Francisco Bank の新入社員です。Jan は、マネージャから送信されたように見える電子メールを受信しました。新しい給与制度に関する内容です。メール内のリンクをクリックしましたが、ファイルが開きません。新しい職場で忙しかったため、Jan はウィンドウを閉じて仕事を続けます。

これは私たちが思う以上に一般的に起きていることです。意図的にではなく、あまりに忙しく、次の期限に気を取られているため、詳細に目が留まらなかったにすぎません。

不運なことに、Jan がクリックしたこのリンクは、スピアフィッシング キャンペーンによって配信されたもので、ゼロデイ マルウェア攻撃に通じていました。レガシー セキュリティ製品を使用していれば、この攻撃は成功したはずです。セキュリティ ソリューションが攻撃の一部しか検知できず、コントロール ポイントを通過すれば、1 つの脅威としか判断しないためです。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

脅威インテリジェンス

オレンジ色の丸をクリックするとデモンストレーションが進みます。

シスコでは、効果的なセキュリティは、各構成要素が連動することで達成されると考えています。シームレスであることが重要です。シスコはセキュリティ アーキテクチャを通じてイベント、ポリシー、脅威インテリジェンス、コンテキスト認識を共有しているため、高度な脅威に対して、優れた検出機能と迅速な修復を実現できます。

オレンジ色の丸をクリックするとデモンストレーションが進みます。

Jan がダウンロードしたファイルは、最初は未知のファイルでした。AMP はファイルを自動的に Threatgrid に送信し、Threatgrid は、ファイルの検出時にマルウェアであったことを示すレトロスペクティブ アラートをトリガーします。それにより AMP for Endpoints は感染を駆除し、NGFW は新たな攻撃をブロックできます。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

オレンジ色の丸をクリックするとデモンストレーションが進みます。

あらゆる脅威には多量の情報が含まれています。その情報をシスコのセキュリティ アーキテクチャ全体で共有することで、ネットワーク全体が学習し、スマート化を図ることができます。これが、最初に共有する情報タイプである脅威インテリジェンスです。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

オレンジ色の丸をクリックするとデモンストレーションが進みます。

共有するデータの種類の例として、Threatgrid は脅威から得た DNS 情報を Cisco Umbrella に提供します。Umbrella は、コマンド アンド コントロール サーバ（C2 または C&C とも呼ぶ）や新しいダウンロード試行など、それ以後の通信をブロックすることで、攻撃対象領域を縮小させます。この情報共有は、シスコがオープンであり、自動化を可能にし、セキュリティをシンプルにすることによって実現しています。

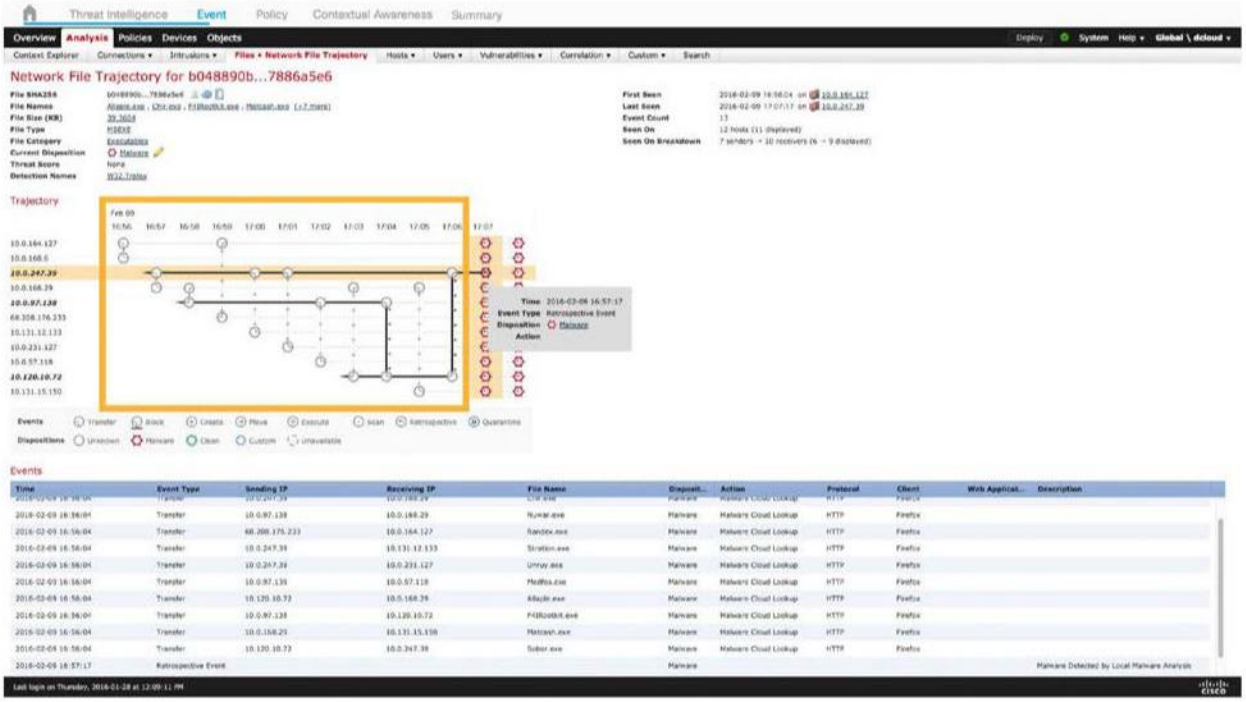
イベント

オレンジ色の丸をクリックするとデモンストレーションが進みます。

次世代ファイアウォールで起きたことを見てみましょう。ここでわかるように、Jan がファイルをダウンロードした当初は、そのファイルはゼロデイ攻撃だったため、「不明」としてリストされていました。このファイルはその後、AMP Threatgrid に自動的に送信され、分析されます。Threatgrid は、そのファイルがマルウェアであることを検出し、ファイアウォールと AMP for Endpoints の両方で AMP による処理を変更し、それによってレトロスペクティブ アラートがトリガーされました。

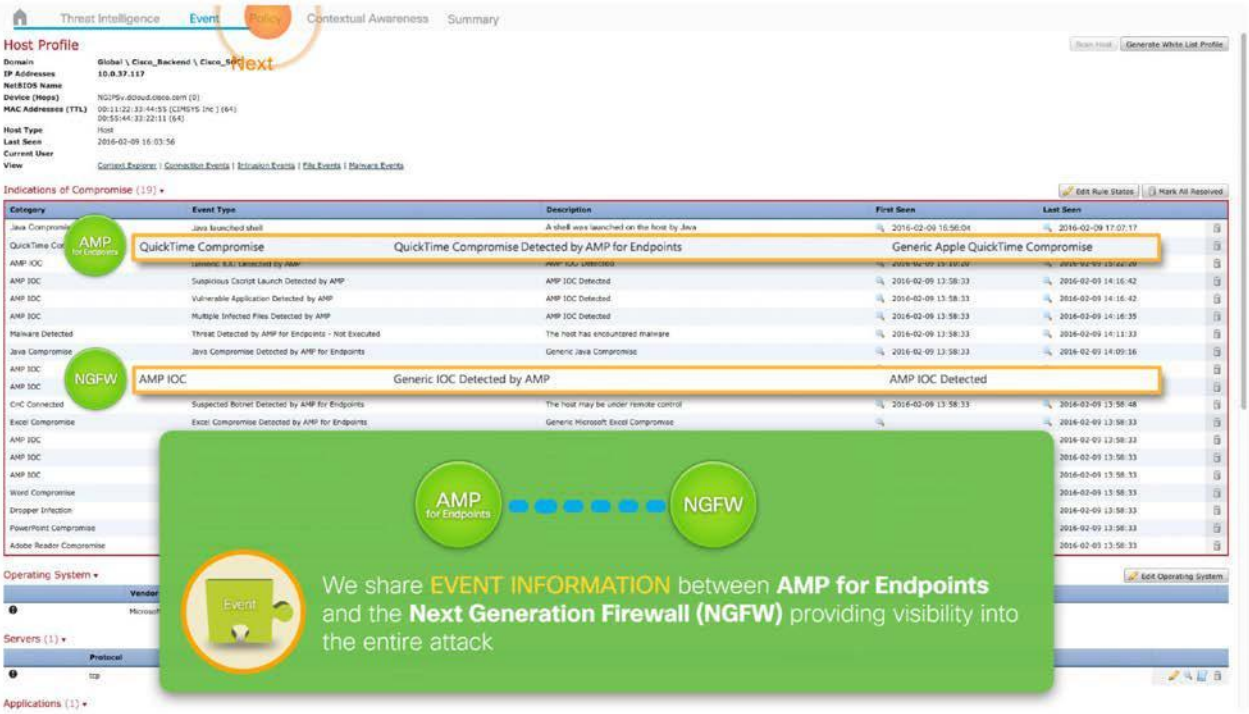
AMP では長時間にわたってファイルを追跡できるため、ファイルがネットワーク内をどのように移動したかを確認できました。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.



オレンジ色の丸をクリックするとデモンストレーションが進みます。

2 番目に共有するデータのタイプはイベント情報です。AMP は、ネットワークとエンドポイントの両方で使用できるプラットフォームです。この場合は次世代ファイアウォール（NGFW）と AMP for Endpoints 間でイベント データを共有することで、ネットワーク内外のシステムに対する攻撃全体の可視性が得られます。この情報共有は、シスコがオープンであり、自動化を可能にし、セキュリティをシンプルにすることによって実現しています。

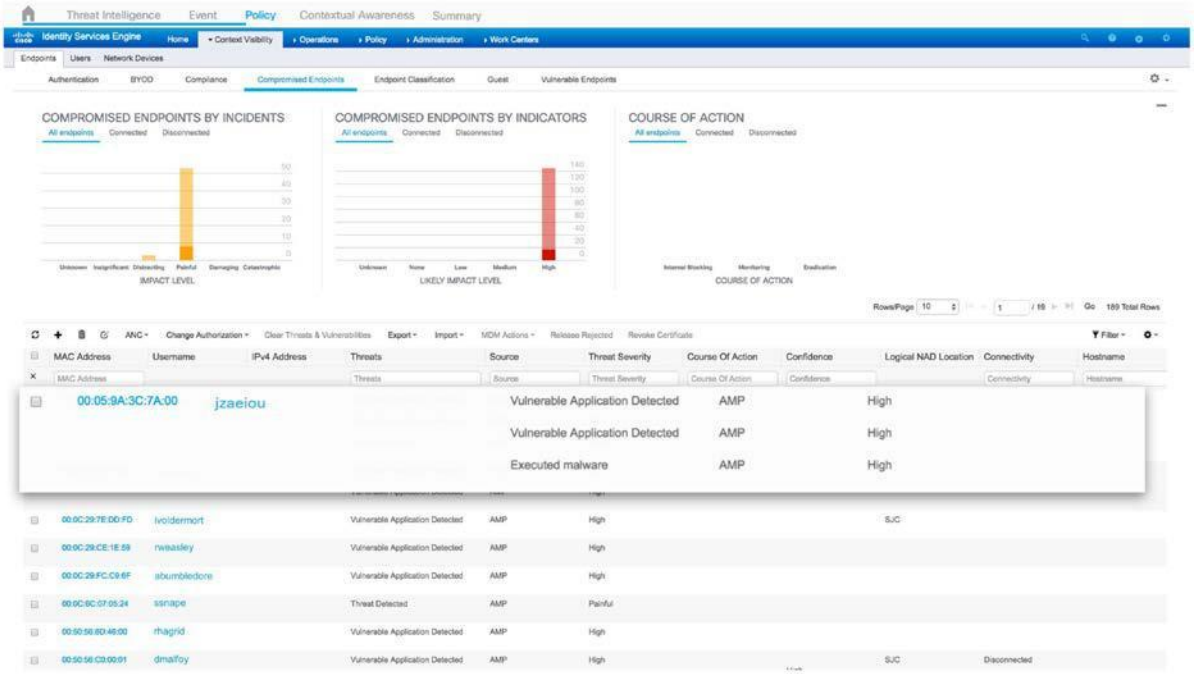


© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

ポリシー

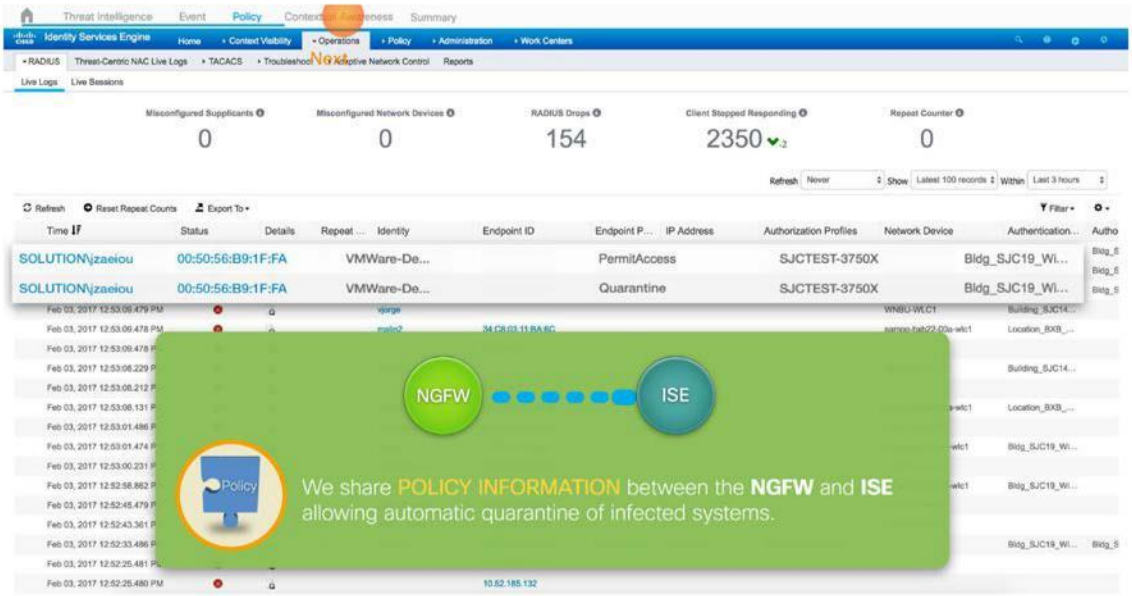
オレンジ色の丸をクリックするとデモンストレーションが進みます。

シスコの Identity Services Engine（ISE）を使用して、さらに脅威への対応を自動化し、ネットワーク アクセスを制御することも可能です。



オレンジ色の丸をクリックするとデモンストレーションが進みます。

3 番目に共有する情報タイプはポリシー情報です。次に示すように、NGFW と ISE がポリシー情報を共有することで、システムを自動的に検疫できるようになります。これが、先に述べた体系的な対応です。ワークフローを自動化することで、脅威がほぼリアルタイムに阻止されるため、アウトブレイクを封じ込め、損害を最小にすることができます。この情報共有は、シスコがオープンであり、自動化を可能にし、セキュリティをシンプルにすることによって実現しています。



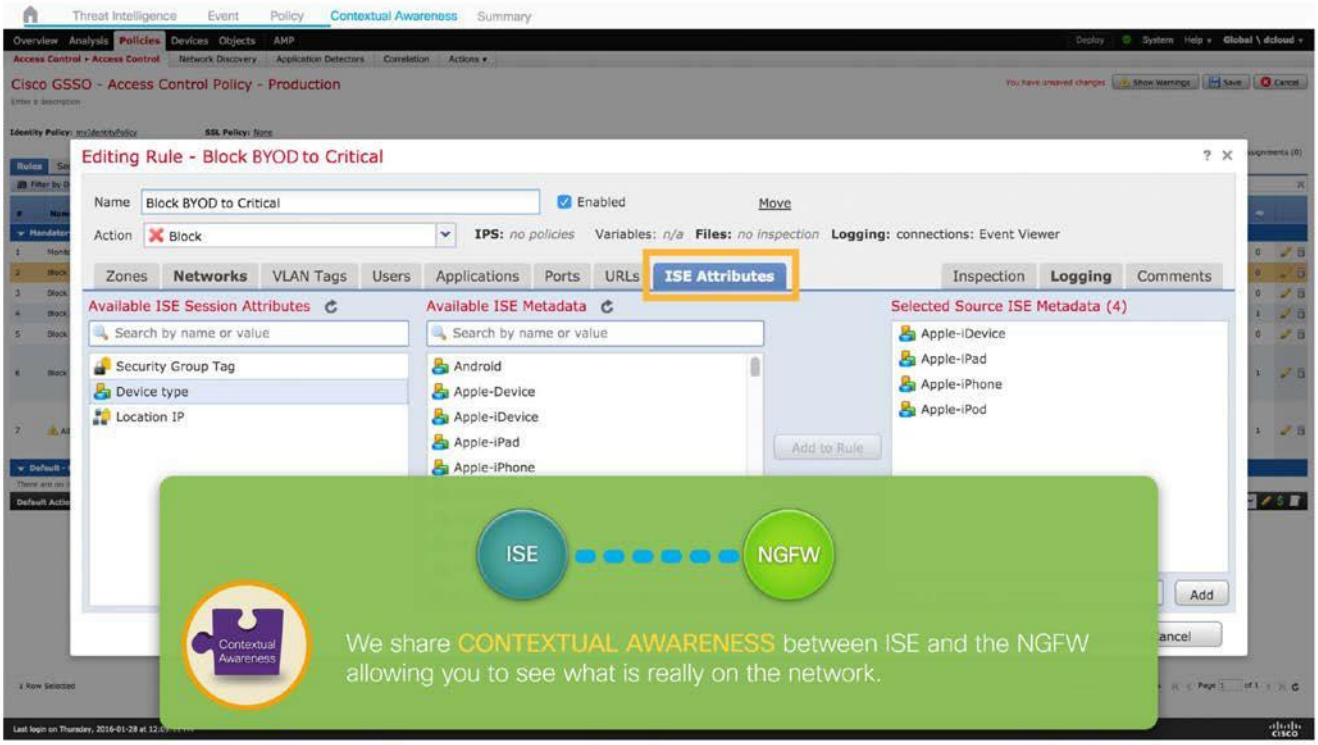
© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

注:このデモンストレーションではシステムの全体的な検疫を実施していますが、お客様によっては他の修復オプションのほうが適切な場合もあります。

コンテキスト認識

オレンジ色の丸をクリックするとデモンストレーションが進みます。

NGFW に戻ると、ISE と NGFW 間の通信が双方向に機能していることがわかります。NGFW がポリシー情報を共有することで ISE が処理を行うことができ、ISE はファイアウォールに接続されているネットワークに実際存在するデバイスに関してコンテキスト認識を共有できます。コンテキスト認識は、4 番目に共有する情報タイプであり、管理者がよりスマートにポリシーを決定するために役立ちます。この情報共有は、シスコがオープンであり、自動化を可能にし、セキュリティをシンプルにすることによって実現しています。



© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

まとめ

オレンジ色の丸をクリックするとデモンストレーションが進みます。

まとめると、シスコはより効果的なセキュリティを実現し、検出時間を短縮する、唯一の統合されたポートフォリオを提供しています。それはシスコの製品がオープンであり、ネイティブに連動してセキュリティ対応を自動化し、ワークフローをシンプルにしてさらに効果的なセキュリティ アーキテクチャを構築できるためです。

オレンジ色の丸をクリックするとデモンストレーションが進みます。

最初に「最も効果的なセキュリティ アーキテクチャをどのように構築するか」と問いかけたことを思い出してください。

最後の数分間では、シスコのセキュリティ ソリューションが相互に通信し、セキュリティの有効性を高め、検出時間を短縮することを確認しました。

これは、シスコが 4 つのタイプの情報を共有する複数のサービスを提供することで、エンドポイント、ネットワーク、そしてクラウドの全体にわたってセキュリティをシンプルにし、対応を自動化し、検出時間を短縮している 1 つの例にすぎません。

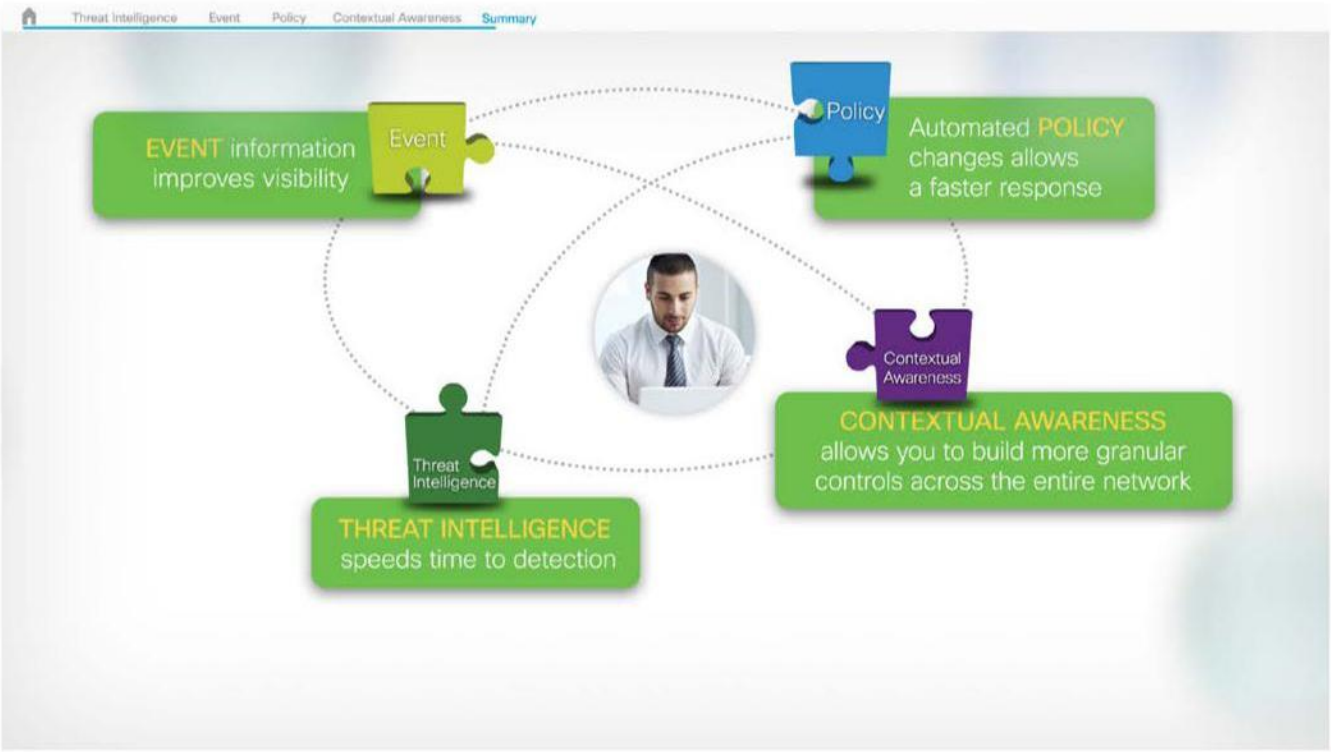
最初の情報タイプはイベント情報でした。これは脅威に対する可視性を高めます。

2 番目の情報タイプはポリシー情報です。迅速な対応を可能にします。

3 番目の情報タイプは脅威インテリジェンスです。セキュリティ アーキテクチャ全体がさらにインテリジェントになります。

共有する 4 番目の情報タイプがコンテキスト認識です。さらにインテリジェントで一貫性があり、精度の高いポリシーをネットワーク全体に適用できるようになります。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.



それにより、強力なセキュリティ アーキテクチャが確立され、検出がシンプルになり、対応が自動化され、効果的なセキュリティが可能になります。そして、シームレスであることが重要です。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

©2017 Cisco Systems, Inc. All rights reserved.
Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。
本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。
「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1502R)
この資料の記載内容は 2017 年 12 月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

お問い合せ先

シスコシステムズ合同会社
〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp