



グローバル セールス
トレーニング

仮想チーム プログラム



AMP for Endpoints

導入のベスト プラクティス

スピーカーおよび監督者 :

Jesse Munos

Evgeny Mirolyubov

Brian McMahon

3月24～29日、セキュリティ SEVT

このラボについて

AMP for Endpoints は、包括的なエンドポイント セキュリティ ソリューションです。スタンドアロン ツールとしても機能しますし、シスコおよびサード パーティのソリューションとネイティブに統合してアーキテクチャの一部としても機能します。そのため、お客様とパートナーは、自社の環境に AMP for Endpoints を導入して設定する前に、多くの考慮事項に注意する必要があります。このハンズオン トレーニングの目的は、受講者に、導入方法、セットアップ、設定、および全般的なベスト プラクティスについて学んでいただくことです。

AMP for Endpoints を使用した経験がなく、予備知識もない場合は、ラボに進む前に、付録を一通りお読みください (10 分)。このハンズオン トレーニング用のラボ ガイドは、AMP for Endpoints の導入に関するベスト プラクティスについて説明していますが、<https://console.amp.cisco.com/docs> で入手できる公式の製品ドキュメントに代わるものではありません。

エンドポイント セキュリティの導入をリードする役割を担い、正しく計画を策定して実行してください。

健闘を祈ります。

Jesse Munos、Evgeny Mirolyubov、Brian McMahon

要件

次の表に、このハンズオン トレーニングの要件を示します。

表 1. 要件

必須	推奨
• ラップトップ	• Cisco AnyConnect

目次

このラボについて.....	2
要件.....	2
トポロジ.....	5
はじめに.....	7
シナリオ.....	8
導入プロセス.....	9
ステージ 1：情報収集.....	10
考慮事項：環境データの収集.....	10
考慮事項：セキュリティ製品のデータ収集.....	10
考慮事項：監査およびコンプライアンス.....	11
ステージ 2：導入計画.....	12
考慮事項：パブリック クラウドとプライベート クラウドの比較.....	12
考慮事項：AMP for Endpoints の設定計画.....	13
考慮事項：ファイアウォールとプロキシの設定.....	13
ステージ 3：コンソール セットアップ.....	14
演習：ユーザ設定.....	14
演習：ポリシー管理.....	15
演習：グループ.....	22
演習：拡散度.....	26
演習：除外リスト.....	27
演習：アウトブレイク コントロール.....	29
演習：AMP Update Server.....	31
ステージ 4a：アルファ導入.....	36
演習：監査導入（アルファ グループ）.....	36
演習：コネクタのチューニング（アルファ グループ）.....	41
演習：コネクタのアクティベーション（アルファ グループ）.....	45

ステージ 4b : ベータ導入	47
演習 : 監査導入 (ベータ グループ)	47
演習 : コネクタのチューニング (ベータ グループ)	49
演習 : コネクタのアクティベーション (ベータ グループ)	50
ステージ 5 : 全体導入.....	52
演習 : 全体導入	52
考慮事項 : コネクタのチューニング	53
ステージ 6 : 統合	54
演習 : Threat Response.....	54
演習 : Threat Grid	56
演習 : Cognitive Intelligence.....	57
一般的なベスト プラクティス.....	59
演習 : コネクタのアップデート	59
演習 : トラブルシューティング	61
接続テスト	62
デバイストラジェクトリ テスト	62
不適切な除外リストのチェック	63
考慮事項 : 仮想デスクトップ インフラストラクチャ	65
まとめ	66
付録 AMP for Endpoints の概要	67

トポロジ

このコンテンツには、Cisco AMP for Endpoints の導入プロセスを説明するために、事前に設定されたユーザとコンポーネントが含まれています。この環境内のほとんどのシステムにアクセスできるように、ブラウザのブックマークとデスクトップのショートカットが事前に作成されています。また、トポロジ ビューのコンポーネント アイコンをクリックすれば、IP アドレスを確認することもできます。次の表とシナリオのステップには、使用するクレデンシャルが記載されています。

図 1. dCloud のトポロジ

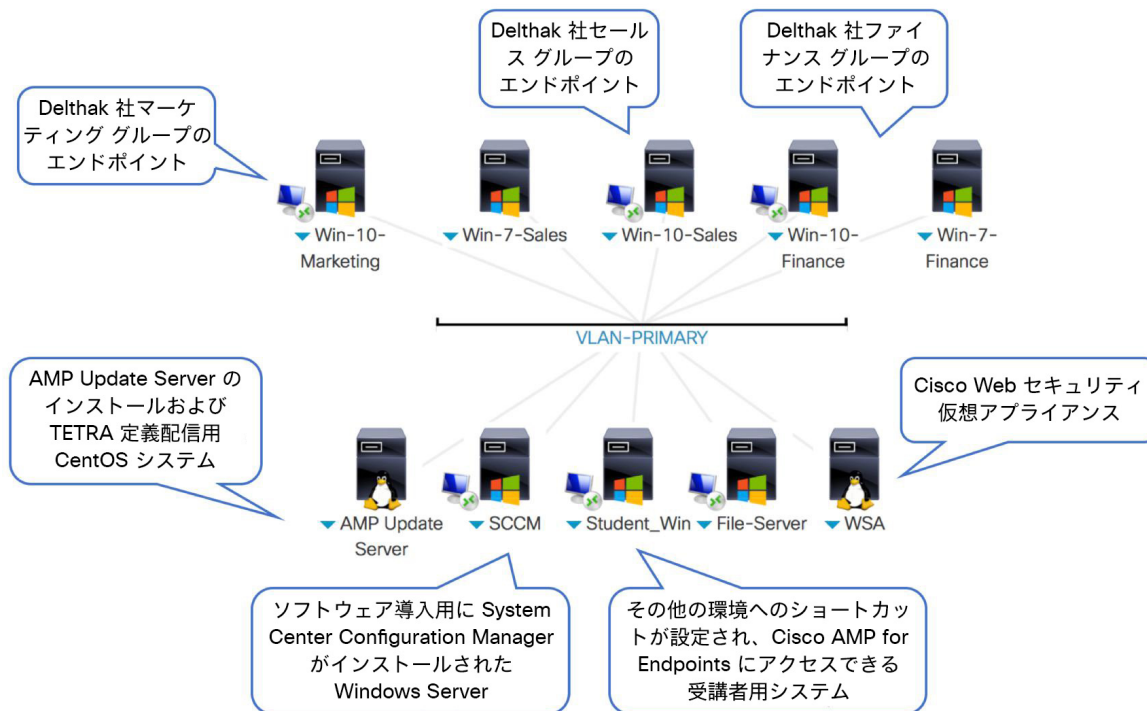


図 2. ラボ トポロジ

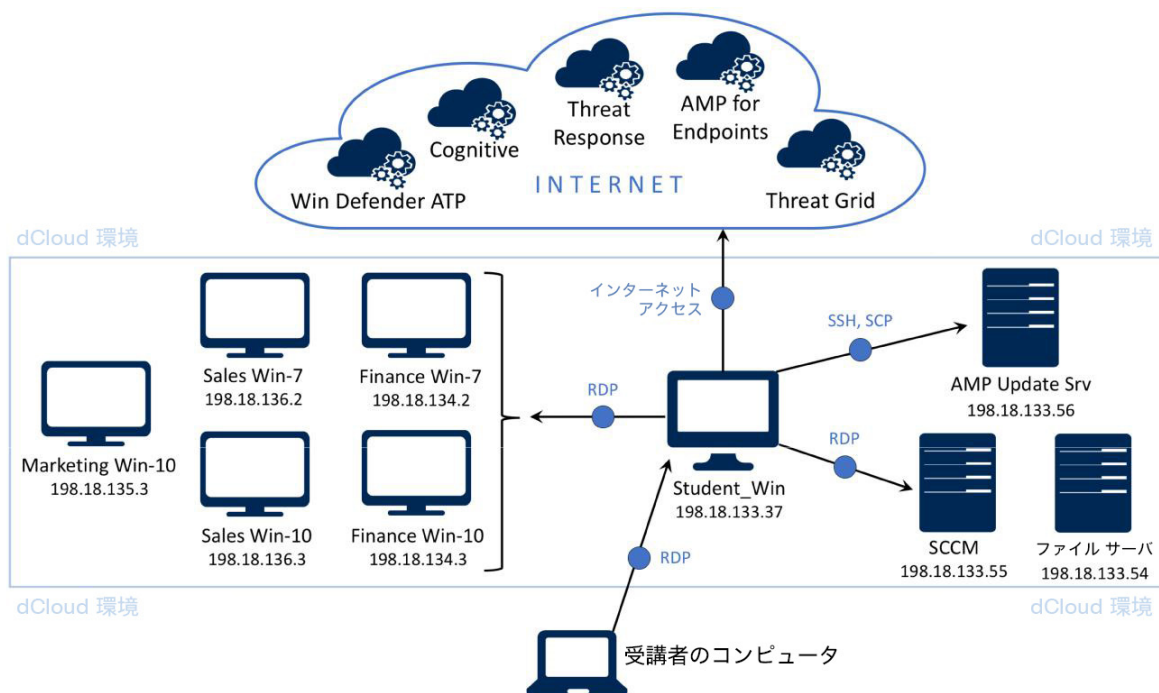


表 2. アカウントおよびパスワード

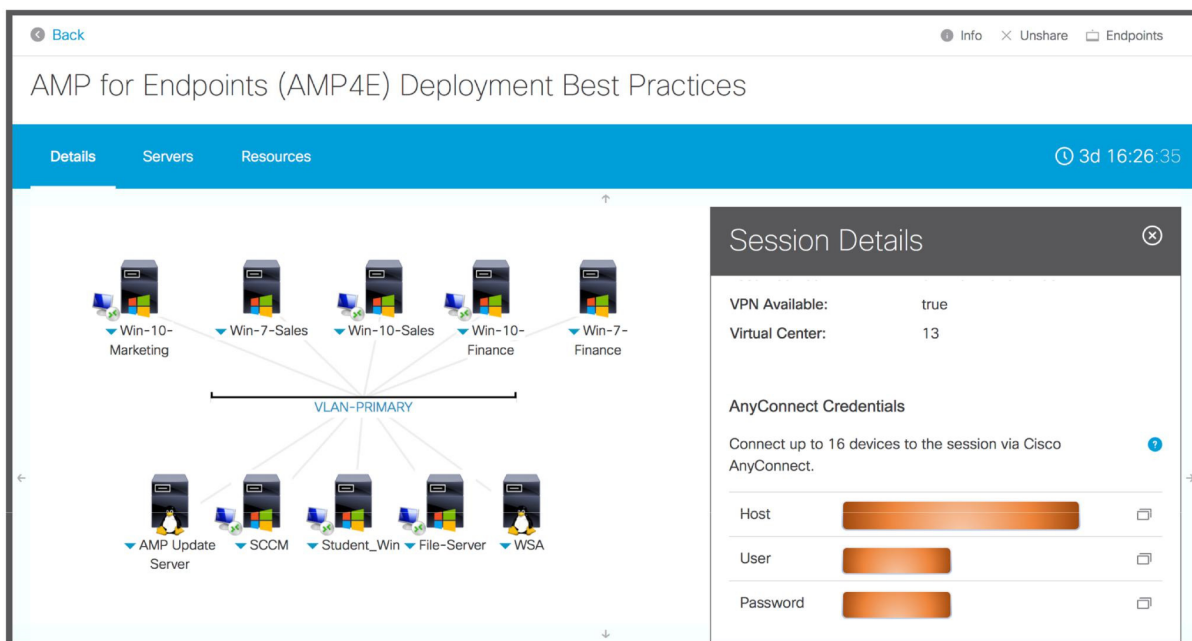
アクセス先	アカウント (ユーザ名/パスワード)
Student_Win – 198.18.133.37	ReadyUser/C1sco12345
SCCM	administrator/C1sco12345
マーケティング、セールス、 ファイナンス VM	administrator/C1sco12345
ファイル サーバ	administrator/C1sco12345
AMP Update Server	root/C1sco12345
WSA	admin/ironport
AMP for Endpoints	studentXXX@sfsnort.com/@mp_Tr41n
Threat Response	studentXXX@sfsnort.com/@mp_Tr41n
Threat Grid	student/C1sco12345
Windows Defender ATP	SEVT@ATSTME.onmicrosoft.com/C1sco12345

注：使用する AMP for Endpoints および Cisco Security (Threat Response) にログインする際は、XXX の部分を、監督者から各自に割り当てられた受講者 ID (100 ~ 200) に置き換えます。

はじめに

1. dCloud RTP にログインする

dCloud (<https://dcloud2-rtp.cisco.com>) にログインすると、[マイハブ (My Hub)] に共有セッションが表示されます。セッションを確認後、[詳細 (Details)] タブに移動すると、接続に必要な AnyConnect のホスト アドレスとクレデンシャルが表示されます (下にスクロールする)。

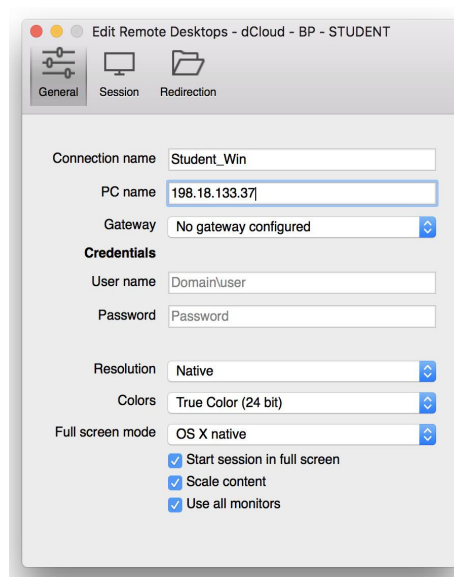


2. dCloud VPN ホストに接続する

必要に応じて、VPN ホストから AnyConnect をダウンロードします。

3. Student_Win RDP に接続する

アクセス クレデンシャルは前のページに記載されています。



シナリオ

Delthak Industries 社は、独自のビジネス モデルを持つ中規模メーカーで、3D プリンタのさまざまなモデルを運用および販売する小規模なチェーン店を展開しています。各店舗には、オンサイト製造用のプリンタがいくつかと、小売用のさまざまなプリンタが設置されています。これらの小規模なロケーションに加えて、米国メリーランド州ベセスダ郊外で大規模な製造施設を運営しています。ベセスダの施設には、同社のセールス チームおよびマーケティング チーム専用のオフィスが併設されています。IT チームは、これらのシステムを長期間慎重に管理し、定期的に再構築しながら、ユーザには、一元管理されたファイル サーバにすべてのデータを保存させています。

Delthak 社の総社員数は約 5,000 人で、米国とヨーロッパの 25 の都市にオフィスがあります。各リモート施設は、一連の VPN を介して本社オフィスと接続され、すべての Web トラフィックは、企業の WSA アプライアンスを経由してルーティングされています。マルウェアに最近感染したことで、Delthak 社の経営者は、従来のウィルス対策 (AV) 製品では適切に保護できないと判断しました。そこで、この問題について現地のシスコ セールス担当者 と協議し、既存の AV ソフトウェアを補完するために、AMP for Endpoints を購入する契約を締結しました。

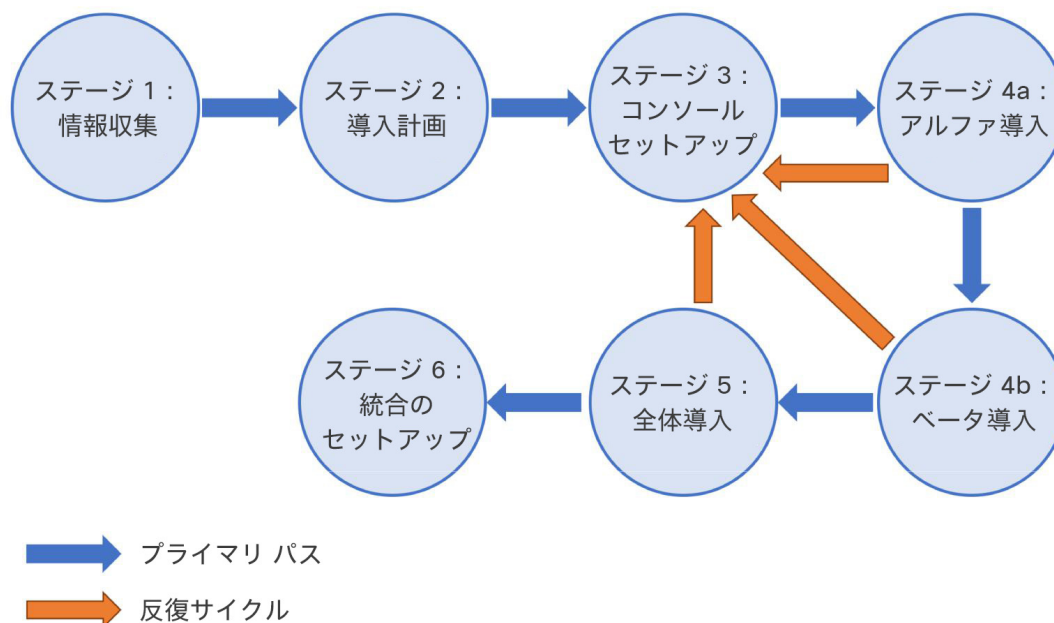
あなたは、Delthak 社のエンドポイント セキュリティの導入をリードしています。あなたの仕事は、AMP for Endpoints の導入戦略を策定して実践することです。その際の目標は、同社のオンライン店舗、POS システム、Windows Server 2016 が稼働する内部ファイル サーバなどの重要なビジネス サービスの中断を最小限に抑えることです。情報の収集とプランニングが完了したら、Delthak 社のマーケティング、セールス、ファイナンス グループに対して、AMP for Endpoints ソフトウェアの導入を開始します。これらの部門のほとんどの従業員は、Windows 7 または Windows 10 のワークステーションやラップトップを使用しています。最高情報責任者 (CIO) との交渉中に、Delthak Industries 社は独自のソフトウェアを開発していないことがわかりました。その代わりに、ベンダーが提供する小売業向けソフトウェアを利用しています。CIO は、社内のファイナンス部門のデータがシステムから漏洩するリスクを懸念しています。このようなデータは機密性の高いものとして分類されており、社外にアップロードされてはならないものです。

また、既存のセキュリティ ソフトウェアを使用して、遅いパッチ管理プロセスに対応しながら、従業員がシステム上で脆弱なアプリケーションを実行できないようにしていることもわかりました。さらに、SHA256 ハッシュ リスト用に、サードパーティの脅威フィードを使用しています。新しいプリンタ ソフトウェアのリリースが速いため、Delthak 社には、古いバージョンのプリンタ ソフトウェアをアプリケーション ブロック リストに追加するポリシーがあります。それにより、プリンタ ファイルが古いソフトウェアによって破損しないようにすることができます。

あなたのサポートにアサインされたシスコのシステム エンジニアから、AMP for Endpoints ユーザ ガイドおよび導入のベスト プラクティスに関するドキュメントのコピーを入手しました。シスコのエンジニアは、これらのドキュメントを利用すれば、複雑な環境に対応する必要はあるものの、大きなリスクを回避するために必要なガイダンスが得られると断言してくれました。また、さらにサポートが必要な場合は、対応してくれます。

導入プロセス

このセクションでは、エンタープライズ環境に AMP for Endpoints を正常に導入するために推奨されるステージについて説明します。以下のフローチャートは、お客様が自社の環境で使用するための、汎用フレームワークとして利用できます。



ステージには、情報収集、導入計画、コンソール セットアップ、アルファ導入、ベータ導入、全体導入、統合のセットアップの各ステージがあります。企業全体に導入する際、情報収集から統合のセットアップまで、これらのステージを段階的に実行することをお勧めします。反復サイクルは、AMP for Endpoints の導入を成功させるプロセスの一環として、円滑な導入、設定の適切なチューニング、パフォーマンス上の潜在的な問題の迅速な解決を実現するために不可欠です。シスコは、それぞれのお客様環境が独自のものであることを認識していますので、このフレームワークは、あくまでも推奨プロセスとして提供するものです。お客様の具体的な使用例に従って調整する必要があります。

AMP for Endpoints 導入ベスト プラクティス ラボでは、上記の各導入ステージを実行し、Delthak Industries 社におけるさまざまなハンズオン演習を通じて、実際の企業への導入をシミュレーションします。このラボ ガイドに記載されている使用例は、対応すべき一連の要件として、すべてのステージで考慮する必要があります。

ステージ 1：情報収集

情報収集は、AMP for Endpoints の導入と設定を円滑に行うための重要な出発点です。このセクションでは、環境およびセキュリティ製品に関するデータやコンプライアンス要件の収集における重要な考慮事項について説明します。

ステージ 1：
情報収集

- オペレーティング システムとバージョン
- エンドポイント数
- 既存のセキュリティ製品
- ソフトウェア導入プロセス
- カスタム アプリケーション
- プロキシ設定
- プライバシー要件

考慮事項：環境データの収集

最初のステップは、既存のセキュリティ ポスチャを把握して文書化することです。文書には、少なくとも以下を記載します。

- AMP for Endpoints がインストールされるエンドポイントの数。
- AMP for Endpoints がインストールされるオペレーティング システム。
- AMP for Endpoints がインストールされる前後に既存のエンドポイントセキュリティ製品が削除されるか。
- AMP for Endpoints を既存のセキュリティ製品と共存させるか。
- ミッションクリティカルなシステムやソフトウェアにはどんなものがあるか。
- 現在のソフトウェア導入プロセスはどのようなものか。
- 環境内に HTTP/S プロキシはあるか。
- 組織のプライバシー要件はどのようなものか。

考慮事項：セキュリティ製品のデータ収集

ほとんどの組織は、既存のエンドポイント セキュリティ製品がすでにインストールされている環境に AMP for Endpoints を導入しています。そのため、AMP for Endpoints に転送される可能性がある対象について、すでに多くの情報が存在しています。一から開始するのではなく、この情報をまとめて現時点での関連性を評価し、AMP for Endpoints のセットアップ プロセスで利用できるようにします。次のリストですべて網羅されているわけではありませんが、最初のポイントとしては最適です。

- 既存のエンドポイント セキュリティ製品には、どのような除外リストが含まれているか。
- すでにアプリケーション ブロック リストまたはアプリケーション ホワイト リストが存在するか。

- 現在のエンドポイント セキュリティ ソフトウェアは、IP アドレスをブロックするために使用されているか。
- 除外リスト、ブロックリスト、ブロックされた IP アドレスは、現在のセキュリティ ポスチャと関連しているか。
- 既存のエンドポイント セキュリティ 製品において、現在どのようなセキュリティ機能が使用されているか。
 - それらの機能は、AMP for Endpoints に存在するか。
 - 既存の設定を AMP for Endpoints Console に移行できるか。

考慮事項：監査およびコンプライアンス

多くの組織は、監査およびコンプライアンス要件の対象となっています。多くの場合、それらの要件によって組織は、アクセスしたユーザや変更を行ったユーザに関するデータ、その変更が行われた日時に関するデータ、およびエンドポイント セキュリティのパフォーマンスに関する履歴データを維持することが求められています。AMP for Endpoints では、詳細なユーザ監査データと最大 30 日分のエンドポイントの履歴データを提供しています。AMP for Endpoints のイベント ストリーミング機能を利用することで、さらに多くの履歴データを保持することも可能です。新しく AMP for Endpoints をインストールした場合にこれらの要件を満たしていることを確認するには、次のような項目を調査することをお勧めします。

- 組織の監査要件は何か。
- 組織が対応すべき政府/自治体のコンプライアンス要件は何か。
 - 例：PCI DSS、GDPR
- 履歴データの保管に関する組織の要件は何か。

ステージ 2 : 導入計画

導入計画フェーズは、導入を成功させるための次の準備ステップです。このステージでは、情報収集セクションで収集したデータを活用して、パブリック クラウドまたはプライベート クラウドの利用有無、設定計画、コンソール セットアップに関して、導入上の意思決定を行います。

ステージ 2 :
導入計画

- 既存のセキュリティ製品とカスタムアプリケーションの除外リスト
- 監査およびコンプライアンス要件
- エンドポイントのグループおよびポリシーの計画
- TETRA/ClamAV を使用するかどうかの判断
- アルファ テスト環境の指定とセットアップ

考慮事項 : パブリック クラウドとプライベート クラウドの比較

AMP for Endpoints を導入する場合、パブリック クラウドとプライベート クラウドの 2 つのオプションがあります。この 2 つのオプションの違いを理解して、組織のニーズに最適なオプションを選択することが重要です。

- パブリック クラウド :
 - パブリック クラウドに AMP for Endpoints を導入するのが、最も一般的です。パブリック クラウドに導入することで、エンドポイントの導入を管理するためのサーバ リソースが不要になり、新たに開発された機能をすぐに利用できます。そのためシスコは、柔軟性が高いこの方法を推奨しています。
 - AMP for Endpoints をパブリック クラウドに導入するための要件 :
 - AMP for Endpoints クラウド サービスにインターネット接続が可能である
 - エンドポイントのオペレーティング システムがサポートされている
 - Windows コネクタ用に、ハード ドライブに 100 MB の空きスペースがある
 - Windows コネクタ + TETRA (ウィルス対策) エンジン用に、ハード ドライブに 1 GB の空きスペースがある
- プライベート クラウド :
 - AMP for Endpoints プライベート クラウドは、自社の環境内でホストされているオンプレミスの仮想アプライアンスです (物理 UCS は計画中)。この導入オプションを選択すると、すべてのエンドポイント テレメトリ データを直接管理できるため、組織のプライバシーを確保できます。ただし、この導入オプションの場合、多くのサーバ要件と課題に対応する必要があります。そのため、厳格なプライバシー要件がない限り、ほとんどの組織には推奨されません。

- AMP for Endpoints プライベート クラウドには、プロキシ モードとエアギャップ モードという 2 つの主要な動作モードがあります。
- AMP for Endpoints プライベート クラウドのほとんどのお客様は、プロキシ モードでアプライアンスを稼働させており、プライベート クラウドを導入する際に推奨される設定です。
- エアギャップ モードは、仮想プライベート クラウド環境では利用できなくなっています（物理 UCS で使用可能になる予定）。このモードは、厳格なプライバシー要件への対応が必要なお客様、または外部ネットワークに接続できないお客様向けのものであります。

考慮事項：AMP for Endpoints の設定計画

AMP for Endpoints では、主にグループによって、複数のエンドポイントを組織化して管理します。グループを使用すれば、組織内のコンピュータを、その機能や場所などの基準に従って管理できます。親グループと子グループを作成し、環境全体をきめ細かく管理することが可能です。そのためには、次の事項を検討し、グループとポリシーのスキーマを慎重に計画することが重要になります。AMP for Endpoints の組織構造を計画する際は、次の点を検討します。

- エンドポイント グループをどのように編成するか。
- ポリシーをどのように体系化するか。
- 除外リストをどのように体系化するか。
- 選択した構造は、今後 1 ~ 2 年のビジネス ニーズを満たしているか。
- TETRA/ClamAV を、AV エンジンとして利用するか。
- AMP Update Server を組織で活用できるか。
- Cognitive Intelligence を利用するか。

考慮事項：ファイアウォールとプロキシの設定

AMP for Endpoints パブリック クラウドでは、適切なエンドポイント コネクタ機能を確認するために、特定のファイアウォール ルールやプロキシを設定する必要があります。パブリック クラウド オプションを使用する組織は、アウトバウンド HTTP/TLS 通信 (TCP/443) を許可する必要があります。このアウトバウンド通信は、特定の IP アドレスとサーバ URL に限定できます。詳細情報については、次の TechNote の記事を参照してください。

- 適切な AMP 運用に必要なサーバ アドレス：
<http://cs.co/amp-server-addresses>

ステージ 3 : コンソール セットアップ

このセクションでは、実際に操作を行います。実践的な演習を通じて、ユーザ アカウントの設定、ポリシーおよびグループの作成と設定、拡散度およびアウトブレイク コントロールの設定、除外リストの作成、AMP Update Server のセットアップを実施します。

ステージ 3 :
コンソール
セットアップ

- ユーザ設定
- ポリシーとグループの作成および設定
- 拡散度およびアウトブレイク コントロールの設定
- 除外リストの作成
- AMP Update Server のセットアップ

演習 : ユーザ設定

適切に設定されていないユーザ アカウントでは、いくつかの AMP for Endpoints 機能を使用できません。使用可能なすべての設定オプションと製品機能に確実にアクセスできるようにするには、ユーザが 2 段階認証、Casebook、タイムゾーンを有効にすることが重要です。ユーザが利用できるその他のオプションには、Google Analytics の停止、電子メールでのお知らせ受信があります。

注 : リモート ファイルの取得、コマンド ラインの表示、拡散度制御機能を使用するには、2 段階認証が必要です。AMP for Endpoints の 2 段階認証はテスト済みで、iOS または Android デバイスの Duo、Google Authenticator、Authy に対応しています。

手順

このラボでは、新規の AMP for Endpoints アカウントが用意されています。アカウントを設定する手順はかなりありますので、ここで頑張ってみましょう。以下の手順を進めるにあたり、すでに VPN をアクティブ化し、dCloud インフラストラクチャに接続していることを前提としています。

1. 自分のマシンからリモート デスクトップを実行し、IP : **198.18.133.37** とクレデンシャル : **Evgeny/C1sco12345** を使用して **Student_Win** に接続します。
2. Google Chrome ブラウザのブックマークを使用して、割り当てられたユーザ アカウント (**studentXXX@sfsnort.com/@mp_Tr41n**) で AMP for Endpoints Console にログインします。

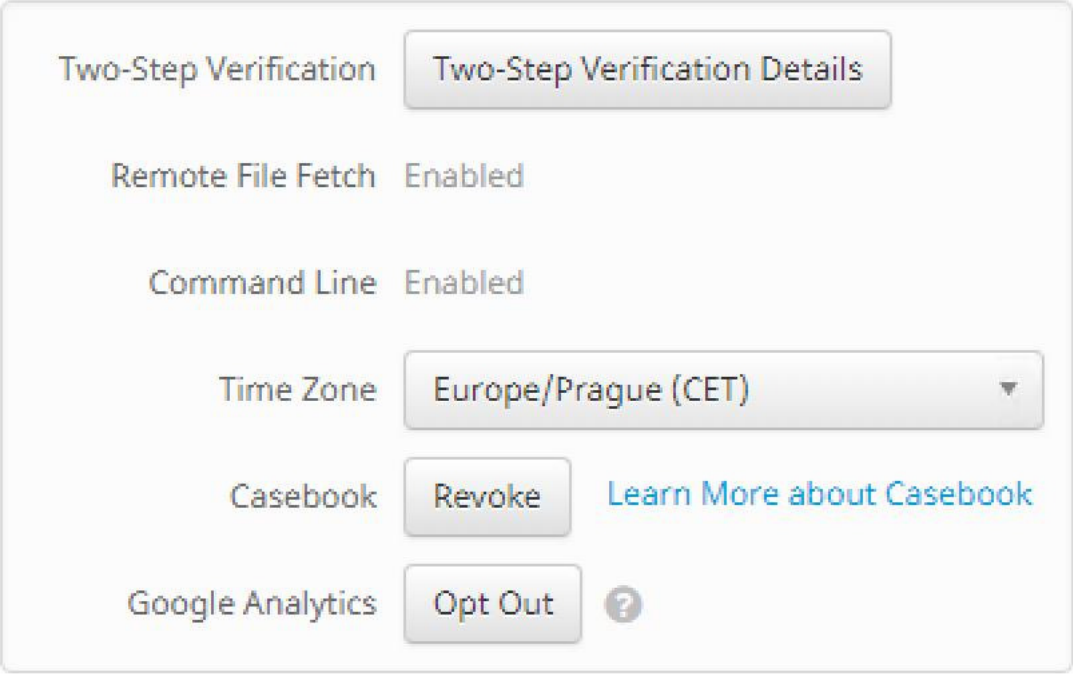
注 : XXX の部分は、監督者に割り当てられた自分の受講者 ID (100 ~ 200) に置き換えます。

3. AMP for Endpoints Console で [アカウント (Accounts)] → [ユーザ (Users)] をクリックし、割り当てられたユーザ名を選択します。

4. [2段階認証 (Two-Step Verification)] オプションの横にある [有効化 (Enable)] をクリックし、注意しながら画面の指示に従います (Google Authenticator の代わりに、Authy または Duo を使用することもできます)。
5. [ユーザ (Users)] ページに戻り、[リモートファイル取得 (Remote File Fetch)] と [コマンドライン (Command Line)] が有効になっていることを確認します。[タイムゾーン (Time Zone)] を設定し、[Casebook] を有効にします。また、[お知らせメール設定 (Announcement Email Preferences)] も設定します。

適切に設定すると、ユーザ ページは次のようになります。

Settings



Two-Step Verification	Two-Step Verification Details
Remote File Fetch	Enabled
Command Line	Enabled
Time Zone	Europe/Prague (CET) ▼
Casebook	Revoke Learn More about Casebook
Google Analytics	Opt Out ?

演習：ポリシー管理

ポリシーの作成と管理は、AMP for Endpoints の中核となる作業です。ポリシーによって、コネクタ機能の設定可能な部分の大半を管理します。そのため、新たに作成されたすべてのポリシーが、現在および将来の組織構造と今後の拡大を考慮して作成されているかを確認することが重要です。この柔軟性を維持するために、組織のニーズに適切に対応する上で必要となるポリシーをいくつか作成することを推奨します。

AMP for Endpoints Console には、管理者が構築するためのベースとなる、さまざまなポリシーがデフォルトで用意されています。これらのポリシーは、エンドポイントのパフォーマンスへの影響を最小限に抑えながら、高いレベルのセキュリティを実現するように設計されています。さまざまなエンドポイントのポリシー設定を決定する際に、シスコはお客様に対して、ポリシー ページの推奨設定をそのまま使用し、組織のセキュリティ ニーズを満たすための変更は、最小限に留めるようにアドバイスしています。

デフォルトでは主に、**監査と保護**の2つのタイプのポリシーが用意されています。

- **監査**ポリシーでは、エンドポイントにあまり干渉せずに AMP for Endpoints Connector を導入できます。デフォルトの監査ポリシーでは、ファイルの検疫やネットワーク接続のブロックは行われません。そのため、初期導入時やトラブルシューティング中にコネクタをチューニングするためのデータを収集する場合に役立ちます。

注：エクスプロイト防止エンジンには、監査ポリシー オプションがありません。そのため、監査ポリシー内で、エンジンを手動で無効にする必要があります。

- **保護**ポリシーは、高度なエンドポイント保護を実現します。これらのポリシーを使用するコネクタは、既知の悪意のあるファイルの検疫や、C2 ネットワーク トラフィックのブロックなどの保護アクションを実行します。

ベスト プラクティス：ポリシー作成に関する AMP for Endpoints のベスト プラクティスでは、基本となる一連のポリシーを作成してからそのポリシーを複製し、同じポリシーのデバッグ バージョンおよびアップデート バージョンを作成します。そうすることで、デバッグ データを収集したり、コネクタをアップデートしたりする際に、一貫性を確保できます。

手順

このハンズオン ラボでは、ワークステーションとサーバの両方をカバーしながら、AMP for Endpoints for Windows Connector を導入することに重点を置いています。そのことを念頭において、Delthak Industries 社のニーズを反映した一連のポリシーを作成していきましょう。

1. AMP for Endpoints Console で、[管理 (Management)] → [ポリシー (Policies)] に移動し、[Windows] タブをクリック後、[監査 (Audit)] ポリシー レコードをクリックして展開設定を切り替え、[編集 (Edit)] をクリックします。
2. [監査 (Audit)] ポリシーの [モードおよびエンジン (Modes and Engines)] タブで、[悪意のあるアクティビティからの保護 (Malicious Activity Protection)] と [システムプロセス保護 (System Process Protection)] エンジンを [監査 (Audit)] に変更し、[エクスプロイト防止 (Exploit Prevention)] エンジンの前にあるチェックボックスをオフにします。

注：エクスプロイト防止エンジンはモニタリング モードを認めていないため、常にブロック/保護します。そのため、監査ポリシーでは完全に無効にすることをお勧めします。

Modes and Engines

Exclusions
19 exclusion sets

Proxy

Outbreak Control

Product Updates

Advanced Settings

Conviction Modes

These settings control how AMP for Endpoints responds to suspicious files and network activity.

Files

Network

Malicious Activity Protection

System Process Protection

Detection Engines

TETRA ⓘ

Exploit Prevention ⓘ

3. [監査 (Audit)] ポリシーの [詳細設定 (Advanced Settings)] → [管理機能 (Administrative Features)] ページに移動し、不正なユーザ (またはマルウェア) が、AMP サービスの開始/停止やアンインストールをできないように、[コネクタ保護パスワード (Connector Protection Password)] を設定します。

Modes and Engines

Exclusions
19 exclusion sets

Proxy

Outbreak Control

Product Updates

Advanced Settings

Administrative Features

Client User Interface

File and Process Scan

Cache

Engines

TETRA

Network

Scheduled Scans

Send User Name in Events ⓘ

Send Filename and Path Info ⓘ

Heartbeat Interval ⓘ

Connector Log Level ⓘ

Tray Log Level ⓘ

Enable Connector Protection ⓘ

Connector Protection Password ⓘ

Automated Crash Dump Uploads ⓘ

Command Line Capture ⓘ

Command Line Logging ⓘ

4. [監査 (Audit)] ポリシーの [詳細設定 (Advanced Settings)] → [クライアントユーザインターフェイス (Client User Interface)] ページに移動し、エンド ユーザにユーザ インターフェイスを表示するかどうかを選択します。

注： シンプルにするために、クライアント インターフェイスは無効にすることを推奨していますが、組織の判断でかまいません。クライアント ユーザ インターフェイスを維持する場合は、デフォルト設定のほとんどをそのまま使用することを推奨します。ただし、[除外リストを非表示にする (Hide Exclusions)] チェックボックスはオンにします。

The screenshot shows the 'Advanced Settings' page for the 'Client User Interface'. The left sidebar contains a navigation menu with the following items: Modes and Engines, Exclusions (19 exclusion sets), Proxy, Outbreak Control, Product Updates, **Advanced Settings** (selected), Administrative Features, Client User Interface (selected), File and Process Scan, Cache, Engines, TETRA, Network, and Scheduled Scans. The main content area displays a list of settings:

- Start Client User Interface ⓘ
- Cloud Notifications ⓘ
- Hide Cataloging Notifications ⓘ
- Hide File Notifications ⓘ
- Hide Network Notifications ⓘ
- Hide System Process Protection Notifications ⓘ
- Hide Exploit Prevention Notifications ⓘ
- Hide Malicious Activity Protection Notifications ⓘ
- Hide Exclusions ⓘ

5. [監査 (Audit)] ポリシーの [詳細設定 (Advanced Settings)] → [ファイルおよびプロセスのスキャン (File and Process Scan)] ページに移動し、[実行時モード (On Execute Mode)] が [パッシブ (Passive)] に設定されていることを確認します。

注：シスコでは、実行時モードの設定をパッシブのままにしておくことを推奨しています。この設定をアクティブ モードに変更すると、パフォーマンスが大幅に低下する可能性があります。

The screenshot shows the 'Advanced Settings' page for a policy. The left sidebar lists various settings categories, with 'File and Process Scan' selected. The main content area shows the following settings:

- Monitor File Copies and Moves ⓘ
- Monitor Process Execution ⓘ
- Verbose History ⓘ
- On Execute Mode: Passive ⓘ
- Maximum Scan File Size: 50 MB ⓘ
- Maximum Archive Scan File Size: 50 MB ⓘ

6. その他のポリシー設定を変更せずに確認し、[保存 (Save)] をクリックします。以下は、この時点での Windows 監査ポリシーを示したものです。

The screenshot shows the Windows Security console for the 'Audit' policy. The title bar reads: 'Audit This policy puts the AMP for Endpoints Connector in a mode that will only detect malicious files but not quarantine them. ... 0 0'. The main content is a table with the following data:

Modes and Engines	Exclusions	Proxy	Groups
Files	Audit Altiris by Symantec	Not Configured	Not Configured
Network	Audit AVAST		
Malicious Activity Protection	Audit Avira		
System Process Protection	Audit Diebold Warsaw		

Outbreak Control	Custom Detections - Simple	Custom Detections - Advanced	Application Control	Network
File Blacklist	Not Configured	Not Configured	Execution Blacklist File Whitelist	blacklist whitelist Not Configured

At the bottom, there are buttons for 'View Changes', 'Download XML', 'Duplicate', 'Edit', and 'Delete'. The 'Modified' date is 2019-02-22 15:00:05 CET and the 'Serial Number' is 47.

7. 次のステップでは、監査ポリシーを複製してデバッグおよびアップデート設定のポリシーを作成します。[ポリシー (Policies)] 設定の [Windows] タブで、[監査 (Audit)] ポリシー レコードをクリックし、展開した設定ビューで [複製 (Duplicate)] ボタンをクリックします (レコード ビューの右下)。これで、[監査のコピー (Copy of Audit)] という名前の複製ポリシーが作成されます。

8. 最初に [編集 (Edit)] (レコード ビューの右下) をクリックして、新しく作成された複製の名前を、[監査-デバッグ (Audit - Debug)] に変えます。次に、[名前 (Name)] ビューでエントリを変更し、最後に、[保存 (Save)] ボタン (ポリシー設定の右下) をクリックします。
9. Windows 監査ポリシーの複製をもう 1 つ作成し、[監査-アップデート (Audit - Update)] に変更します。後で監査設定とデバッグ設定を行います。
10. 上記の手順を、デフォルトの保護ポリシーおよびサーバポリシーについても繰り返し、設定を始めます。主な違いは、[モードおよびエンジン (Modes and Engines)] の設定です。
 - a. 保護ポリシーの [モードおよびエンジン (Modes and Engines)] は、次のようになります。

Modes and Engines

Exclusions
19 exclusion sets

Proxy

Outbreak Control

Product Updates

Advanced Settings

Conviction Modes

These settings control how AMP for Endpoints responds to suspicious files and network activity.

Files

Quarantine Audit

Network

Block Audit Disabled

Malicious Activity Protection

Quarantine Block Audit Disabled

System Process Protection

Protect Audit Disabled

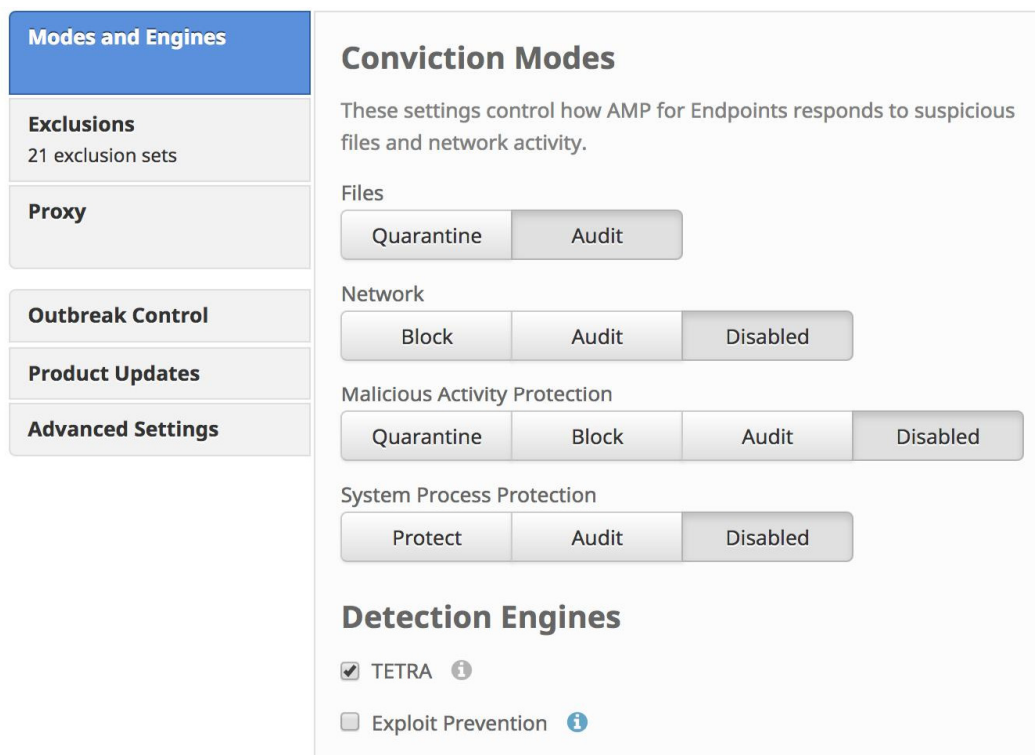
Detection Engines

TETRA ⓘ

Exploit Prevention ⓘ

注：管理機能、クライアント ユーザー インターフェイス、ファイルおよびプロセスのスキャンなどの設定は、監査ポリシーと同じです。

b. サーバポリシーの [モードおよびエンジン (Modes and Engines)] は、次のようになります。



Modes and Engines

- Exclusions**
21 exclusion sets
- Proxy**
- Outbreak Control**
- Product Updates**
- Advanced Settings**

Conviction Modes

These settings control how AMP for Endpoints responds to suspicious files and network activity.

Files
Quarantine Audit

Network
Block Audit Disabled

Malicious Activity Protection
Quarantine Block Audit Disabled

System Process Protection
Protect Audit Disabled

Detection Engines

- TETRA ⓘ
- Exploit Prevention ⓘ

注：ほとんどのサーバ導入では、ネットワーク エンジン (DFC) を完全に無効にする必要があります。さらに、適切なコマンド ライン スイッチを使用してサーバ コネクタをインストールし、デバイス フロー コリレーションのインストールを無効にします。最初の導入では、ファイルは監査モードのままにし、初期チューニングと確認を完了してから、検疫モードに切り替えます。管理機能、クライアント ユーザ インターフェイス、ファイルおよびプロセスのスキャンなどの設定は、監査ポリシーと同じです。

11. デバッグ バージョン ([保護-デバッグ (Protect - Debug)]、[サーバ-デバッグ (Server - Debug)]) およびアップデート バージョン ([保護-アップデート (Protect - Update)]、[サーバ-アップデート (Server - Update)]) のポリシーを作成します。後で監査設定とデバッグ設定を行います。この時点では、[ドメインコントローラ (Domain Controller)] と [トリアージ (Triage)] ポリシーは変更しないでください。

それぞれ設定すると、Windows ポリシー ページは次のようになります。

Policies [View All Changes](#)

Search

All Products Windows Android Mac Linux iOS + New Policy...

Policy Name	Description	Users	Monitors
Audit	This policy puts the AMP for Endpoints Connector in a mode that will only detect malicious files but not quarantine them. ...	4	0
Audit - Debug	This policy puts the AMP for Endpoints Connector in a mode that will only detect malicious files but not quarantin...	1	0
Audit - Update	This policy puts the AMP for Endpoints Connector in a mode that will only detect malicious files but not quaranti...	1	0
Domain Controller	This is a lightweight policy for use on Active Directory Domain Controllers.	1	0
Protect	This is the standard policy for the AMP for Endpoints Connector that will quarantine malicious files and block malicious ...	1	0
Protect - Debug	This is the standard policy for the AMP for Endpoints Connector that will quarantine malicious files and block m...	1	0
Protect - Update	This is the standard policy for the AMP for Endpoints Connector that will quarantine malicious files and block ...	1	0
Server	This is a lightweight policy for high availability computers and servers that require maximum performance and uptime.	2	0
Server - Debug	This is a lightweight policy for high availability computers and servers that require maximum performance and ...	1	0
Server - Update	This is a lightweight policy for high availability computers and servers that require maximum performance and ...	1	0
Triage	This is an aggressive policy that enables the offline engine to scan computers that are suspected or known to be infected...	1	0

演習：グループ

グループは、エンドポイント コネクタとポリシーを関連付けるリンクです。そのため、グループのトップ レベルには、すべてのオペレーティング システムに関連するポリシーを割り当てる必要があります。たとえば、監査親グループには、Windows、Mac、Linux、iOS、Android に対して監査ポリシーが割り当てられます。ただし、コネクタは親グループに直接設定しないでください。企業がエンドポイントを編成するために使用する標準に基づいて、子グループを作成することを強くお勧めします。エンドポイント組織の子グループを活用することで、エンドポイント グループをきめ細かく管理できます。

AMP for Endpoints Console には、5 つの親グループがデフォルトで登録されています。デフォルトの親グループは、テンプレートとして機能します。自社の環境に合わせて、さまざまな親グループや子グループを作成できます。子グループは、親グループのすべてのポリシーを継承します。また、親グループ間で子グループを移動させることもできます。子グループを新しい親グループに移動すると、新しい親グループに関連付けられているすべてのポリシーが継承されます。

Groups

Search		Q
Audit Audit Group for SEVT View Changes	Edit	Delete
Domain Controller Domain Controller Group for SEVT View Changes	Edit	Delete
Protect Protect Group for SEVT View Changes	Edit	Delete
Server Server Group for SEVT View Changes	Edit	Delete
Triage Triage Group for SEVT View Changes	Edit	Delete

作成する親グループは、ポリシーに合わせて同じ名前にする必要があります。たとえば、次のようなポリシーがあるとします。

- 監査
- 監査デバッグ
- 監査アップデート

これらの各ポリシーに対応した親グループを作成する必要があります。

- 監査親グループ
- 監査デバッグ親グループ
- 監査アップデート親グループ

注：グループの名前は、グループ内のデバイスを示すだけのもので、グループのふるまいを示すものではありません。コネクタのふるまいを示すのは、常にポリシー設定です。たとえば、保護ポリシーが関連付けられた、監査という名前のグループがある場合、混乱を避けるために、グループとポリシーの名前は一致させることをお勧めします。

エンドポイントの子グループに編成すると、親グループ間で子グループを移動させるだけで、簡単にきめ細かく管理できます。たとえば、コネクタの新しいバージョンがリリースされた場合、アップデート ポリシーの製品アップデート設定を変更し、関連するアップデート親グループに子グループを 1 つずつ移動するだけです。そのため、グループやポリシーを追加することなく、エンドポイント コネクタをきめ細かく段階的にアップデートできます。

ベスト プラクティス：共通した特性ごとに編成された複数の子グループにコネクタを割り当てます。たとえば組織グループでは、地域、タイムゾーン、オフィス、ビジネスユニット、職務の類似性などで分け、子グループを該当する親グループに関連付けます。すべてのエンドポイント コネクタを 1 つのグループにしたり、コネクタを親グループに直接割り当てたりしないでください。

手順

この演習では、Delthak Industries 社の要件に従って、AMP for Endpoints 環境用の親グループと子グループを作成します。

1. AMP for Endpoints Console で、[管理 (Management)] → [グループ (Groups)] に移動し、[監査 (Audit)] グループの横にある [編集 (Edit)] ボタンをクリックして、名前を [監査親グループ (Audit Parent Group)] に変更します。Windows ポリシーが **監査** (ポリシー作成演習で選択した名前) に割り当てられていることを確認します。[保存 (Save)] をクリックします。

注：この演習では、新たに作成されたグループに、Mac、Linux、Android、iOS ポリシーを割り当てる手順はスキップします (時間の節約と簡略化のため)。ただし、実際の導入プロセスに違いはありません。Windows 以外のオペレーティング システムを含む AMP for Endpoints のインストールでは、関連するポリシーとグループをそれぞれ設定する必要があります。

2. [グループ (Groups)] ページの右側にある [グループの作成 (Create Group)] ボタンを使用して、**監査デバッグ親グループ**と**監査アップデート親グループ**という 2 つの新しいグループを作成します。これらのグループに割り当てられている Windows ポリシーが、それぞれ、[監査-デバッグ (Audit - Debug)] および [監査-アップデート (Audit - Update)] であることを確認します。
3. [保護 (Protect)] グループと [サーバ (Server)] グループに対して同じ手順を繰り返し、合計で 4 つの新しいグループを作成します。各グループの目的を反映して Windows ポリシーが正確に割り当てられていることを確認します。たとえば、[保護デバッグ親グループ (Protect Debug Parent Group)] には、Windows 用の [保護-デバッグ (Protect - Debug)] ポリシーが割り当てられ、[サーバアップデート親グループ (Server Update Parent Group)] には、Windows 用の [サーバ-アップデート (Server - Update)] ポリシーが割り当てられている必要があります。

- 最後に、子グループを作成します。[グループ作成 (Create Group)] ボタンを使用して、[マーケティング (Marketing)]、[セールス (Sales)]、[ファイナンス (Finance)]、[ファイルサーバ (File Servers)] という名前の 4 つの新しいグループを追加します。最初の 3 つのグループは、[監査親グループ (Audit Parent Group)] の子グループとして追加し、最後のグループは、[サーバ親グループ (Server Parent Group)] の子グループとして追加します。

注：新たに子グループを作成する際に、親グループを選択できます。

以下は、上記の手順を完了した後に、[グループ (Groups)] ページの上部がどのように表示されるかを示したものです。新たに作成された親グループのいくつかは、1 つのスクリーンショットに収まっていないことに注意してください。

The screenshot displays the Cisco ISE Groups management interface. On the left, a list of parent groups is shown, including Audit Parent Group, Marketing, Sales, Finance, Protect Parent Group, Triage, Server Parent Group, Domain Controller, Audit Debug Parent Group, Audit Update Parent Group, Protect Debug Parent Group, and Protect Update Parent Group. Each group entry includes a 'View Changes' link and 'Edit'/'Delete' buttons. The Marketing group is selected and highlighted in blue. On the right, a detailed view of the Marketing group is shown, including its last modified date, creator, and a table of policies applied to it.

Marketing	
No description	
Last Modified	2019-02-26 13:20:48 CET
Created by	Evgeny Mirolyubov
Windows Policy	Audit applied from: Audit Parent Group
Android Policy	Protect applied from: Audit Parent Group
Mac Policy	Audit applied from: Audit Parent Group
Linux Policy	Audit applied from: Audit Parent Group
iOS Policy	Audit applied from: Audit Parent Group
Parent Groups	Audit Parent Group

Computers
No computers have been assigned to this group
No child members

演習：拡散度

AMP for Endpoints の拡散度管理機能は、Threat Grid のファイル分析環境に対するリンクとして組み込まれています。この機能は、拡散度が低い未知の実行可能ファイルに関して、エンドポイントの特定の AMP for Endpoint グループを監視するものです。未知の実行可能ファイルが検出され、特定の拡散度条件に一致した場合に、AMP for Endpoints クラウドサービスは、分析用ファイルのアップロードをエンドポイント コネクタに要求できます。AMP for Endpoints Console にファイルが正常にアップロードされると、さらに静的分析および動的分析を実施するために、Threat Grid Cloud に送信されます。ファイルの脅威スコアが高い場合、AMP Cloud が更新され、ファイルがエンドポイントから削除されます。

注：すべての AMP for Endpoints アカウントは、直近の 24 時間での送信を 100 ファイルに制限するようにデフォルトで設定されています。Threat Grid の「高度なファイル分析」用送信パックを追加購入することで、必要に応じて制限数を増やすことができます。必要な送信数を決定するには、Proof of Value プロセスを実施することが最適です。

手順

Delthak Industries 社の要件に従って、新たに作成されたグループの拡散度を設定していきましょう。

1. AMP for Endpoints Console で、[分析 (Analysis)] → [拡散度 (Prevalence)] に移動し、ページの右側にある [自動分析の設定 (Configure Automatic Analysis)] ボタンをクリックします。
2. 分析用にファイルを送信するグループを選択し、[適用 (Apply)] をクリックします。

ベストプラクティス：すべてのエンドポイントグループに拡散度を設定します。ただし、ソフトウェア開発を担当するグループと、プライバシー要件が厳しいグループは除きます（エンドポイントの追加分析用にファイルは送信されません）。シナリオを参照して、グループを選択します。

3. [現在の自動分析のステータス (Current Automatic Analysis Status)] に、選択したグループの数と、そのグループ内のエンドポイントの数が表示されます。この時点ではエンドポイント コネクタは導入されていないため、数値はまだゼロです。

< Automatic Analysis Configuration

[View All Changes](#)

This enables automatic analysis for Low Prevalence Executables per group.

15 selected

Apply

Warning: Analyzed files are accessible by all users in your organization from the File Analysis page.

Current Automatic Analysis Status

0 low prevalence executables executed in the previous week.
11 selected groups and 4 child groups.
0 computers within the selected groups.

演習：除外リスト

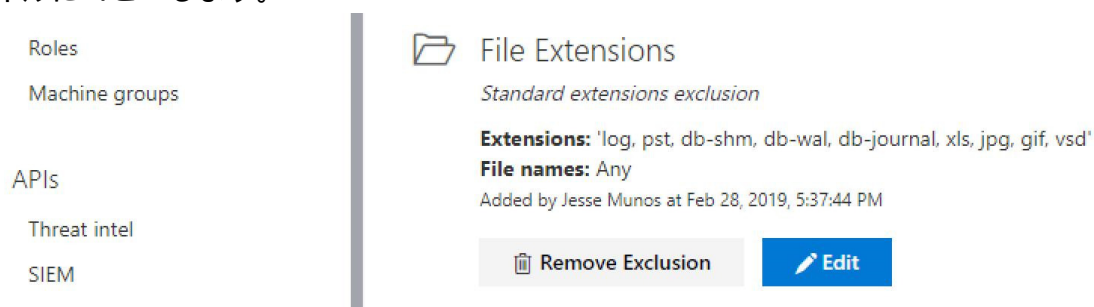
Delthak 社の環境には、しばらくの間、Windows Defender ATP が導入されてきました。そこで、少なくとも各部門のマネージャが使用する Windows 10 エンドポイントについては、Windows Defender ATP を完全に置き換えるのではなく、AMP for Endpoints で補完することになりました。既存の除外リストは、互換性を確保するために、AMP for Endpoints と Windows Defender ATP の両方に追加する必要があります。エンドポイントのパフォーマンスに悪影響が及ばないようにするため、両方の製品で特定の除外リストを作成する必要があります。

注：除外リストを 1 つの製品から別の製品に移植する際は、移植先の環境にも適していることを確認し、セキュリティの対象範囲に不要なギャップが発生しないようにするため、慎重に再評価する必要があります。除外リストの概要については、AMP for Endpoints ユーザ ガイドおよび次のドキュメントを参照してください：<http://cs.co/amp-exclusions>

手順

この演習では、Windows Defender Security Center から既存の除外リストを取得してリストを調整し、AMP for Endpoints にインポートします。さらに、Windows Defender ATP と AMP for Endpoints の双方で、お互いを除外リストに追加する必要があります。

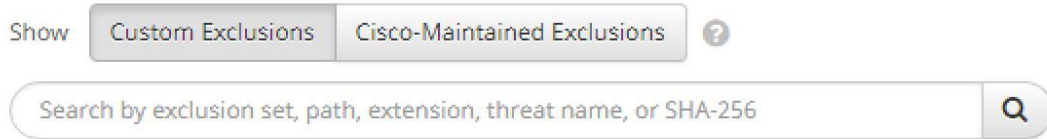
1. Google Chrome ブラウザを開き、[Win Defender ATP] ブックマーク (**SEVT@ATSTME.onmicrosoft.com/C1sco12345**) をクリックし、[設定 (Settings)] → [マシンリスト (Machines list)] に移動すると、現在 Windows Defender ATP がインストールされているエンドポイント システムが表示されます。
2. ここで、[設定 (Settings)] → [フォルダの自動除外 (Automation folder exclusions)] に移動し、既存の除外リストを確認します。その内容をメモに取るか、メモ帳ファイルにコピーします。



注：ここでは、いくつかの拡張子のみを除外します。これは、シンプルにするためです。一般的な除外リストには、はるかに多くの対象が含まれています。2 回検討し、Delthak Industries 社と協議して、これらの除外リストがまだ妥当であることを確認します。

- Google Chrome ブラウザで新規タブ開き、[AMP for Endpoints] ブックマーク (studentXXX@sfsnort.com/@mp_Tr41n) をクリックして、[管理 (Management)] → [除外リスト (Exclusions)] に移動します。除外リストには、[カスタム (Custom)] と [シスコ管理 (Cisco-Maintained)] の2つのカテゴリがあることがわかります。

Exclusions



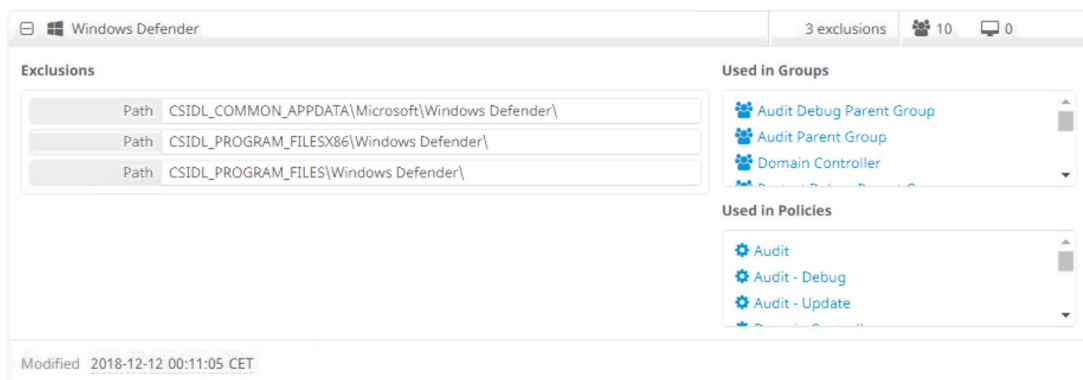
- カスタム除外リスト**は、標準外の特定のケースに対応するために、お客様の組織によって作成されます。カスタム除外リストは、多くの場合初期チューニング後に作成されます。パス、ファイル拡張子、ワイルドカード、脅威、プロセスを除外できます。

ベスト プラクティス：除外リストに関する推奨のベストプラクティスについては、次のドキュメントを確認してください：<http://cs.co/amp-exclusions-bp>

- シスコ管理の除外リスト**は、シスコが作成して管理しているもので、AMP for Endpoints Connector とウィルス対策ソフトウェアやセキュリティ関連のソフトウェアの両方に対応しています。

注：シスコ管理の除外リストは、削除したり変更したりすることはできません。各アプリケーションに関して、除外対象のファイルおよびディレクトリを確認できます。これらの除外リストは、アプリケーションの改善や新しいバージョンに対応して、継続的に更新される可能性もあります。

- [シスコ管理除外リスト (Cisco-Maintained Exclusions)] ボタンをクリックし、範囲を **Windows** に限定してから、**Windows Defender** レコードを見つけてクリックし、3つのパスが除外されていることを確認します。また、この除外リストが適用されているグループとポリシーが、先に作成/変更したすべてのポリシーにリンクされていることも確認します。



5. ここで、**Microsoft Windows Default** レコードを見つけて、リストを確認します。
 - a. Windows Defender ATP に存在していたが、**シスコ管理除外リスト**に存在していない**ファイル拡張子除外リスト**があるかどうかを確認します。
 - b. ある場合は、[新しい除外セット (New Exclusion Set)] ボタンをクリック後、製品に [Windows] を選択し、不足しているファイル拡張子の除外対象を加えて、新しいカスタム除外セットに追加します。この際、複数の除外対象を一度に追加できます。[保存 (Save)] をクリックします。
 - c. カスタム除外セットは、関連するポリシーに適用された場合にのみ有効になります。[管理 (Management)] → [ポリシー (Policies)] に移動し、[監査 (Audit)] ポリシー レコードの横にある [編集 (Edit)] ボタンをクリックします。[監査ポリシー (Audit policy)] ページで [除外リスト (Exclusions)] をクリックし、新しく作成したカスタム除外リストを選択します。[保存 (Save)] をクリックして、監督者に結果を示します。

注： 特定のカスタム除外リストを割り当てる必要があるすべての関連ポリシーについて、上記の手順を繰り返す必要があることに注意してください。この演習では、監査ポリシーにのみ追加し、他はスキップします。

演習：アウトブレイク コントロール

AMP for Endpoints は、お客様の環境内で悪意のあるソフトウェアが拡散するのを管理して軽減するためのさまざまな制御機能を備えています。これらの制御機能には、シンプル カスタム検出 (SHA256 マッチングに基づくファイルの検疫)、拡張カスタム検出 (カスタム Clam AV ルールでのマッチング)、アプリケーション制御 (アプリケーションの実行を制御するためのブロッキングおよびホワイト リスト)、ネットワーク (IP アドレスのブラック リストおよびホワイト リスト)、エンドポイント IOC (お客様がスキャンのためにインポートした OpenIOC 形式のカスタム検出ルール) などが含まれています。

注： アウトブレイク コントロールを 1 つの製品から別の製品に移植する際には、移植先の環境にも適していることを確認し、移植による問題を最小限に抑えるように、慎重に再評価する必要があります。

手順

この演習では、既存のカスタム SHA256 ブラックリストを AMP for Endpoints Console に移植する手順を、順番に説明します。Windows Defender Security Center で、既存の SHA256 ブラックリストを確認できます。

1. Win Defender ATP ポータルで、[設定 (Settings)] → [自動許可/ブロックリスト (Automation allowed/blocked lists)] に移動すると、ブロック リストのエントリが複数表示されます。
2. メモ帳で新しいファイルを作成し、ブロック リストからそのファイルにハッシュをコピーします (1 行につき 1 ハッシュ)。SHA256Block.txt という名前でメモ帳ファイルをデスクトップに保存します。

The following files will be automatically marked as 'Malicious' if in the blocked list or marked as 'Clean' if in the allow list when identified during an Automatic investigation.

✓	List type	Time	File Name	Hash Type	File Hash
	Block	2/28/19, 5:42 PM	Resume.docx	SHA256	1ad74134c02d493c508a02feb9f3f9c54599a3753668be531470604c731138f9
	Block	2/28/19, 5:42 PM	SHA256Block - Notepad		dda2ace9458afb4791c8226386588444b228
	Block	2/28/19, 5:42 PM			a3117b2bc3bd1c24bec22ce765f20251884ca

3. AMP for Endpoints (studentXXX@sfsnort.com/@mp_Tr41n) に戻り、[アウトブレイクコントロール (Outbreak Control)] → [カスタム検出 (Custom Detections)] → [シンプル (Simple)] に移動し、[作成 (Create)] をクリックして、SHA256 ブラックリストにわかりやすい名前をつけて保存します。
4. 新たに作成されたリストの横にある [編集 (Edit)] をクリックし、[SHA-256 セットをアップロード (Upload Set of SHA-256s)] に切り替えて、Windows Defender ATP から取得したハッシュを含む SHA256Block.txt ファイルを参照します。[アップロード (Upload)] をクリックしてページを更新すると、リストにハッシュが表示されます。

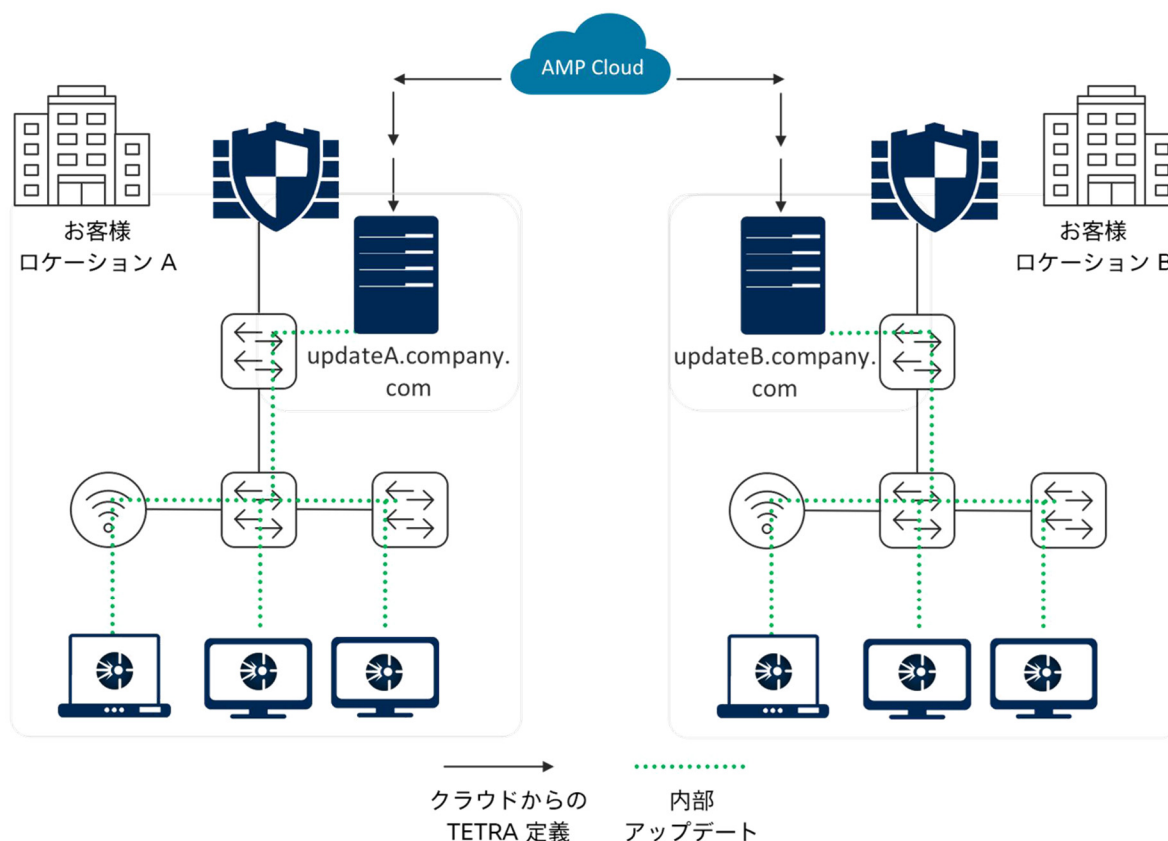
注： AMP for Endpoints Console に SHA256 エントリを 1 つずつ追加することも、一連の SHA256 エントリを含むファイルを一度にアップロードすることもできます。また、ファイル自体をアップロードしてハッシュを計算することもできます。AMP for Endpoints では、正規のクリーン ファイル (AMP Cloud でクリーン ファイルとしてマークされている) のハッシュを、シンプル カスタム検出リストに追加することはできません。正規ファイルが誤って検出されてしまうのを防ぐために、ガードされています。ただし、ファイルが実行されるのを防ぐために、クリーン ファイルをアプリケーション ブロッキング リストに追加することは可能です。

5. シンプル カスタム検出リストは、関連するポリシーに適用した場合にのみ有効になります。[管理 (Management)] → [ポリシー (Policies)] に移動し、[監査 (Audit)] ポリシー レコードの横にある [編集 (Edit)] ボタンをクリックします。[監査 (Audit)] ポリシー ページで [アウトブレイクコントロール (Outbreak Control)] をクリックし、[カスタム検出-シンプル (Custom Detections - Simple)] の横にある、新しく作成されたリストを選択します。[保存 (Save)] をクリックして、次の演習に進みます。

注： 除外リストと同様に、特定のカスタム検出を割り当てる必要があるすべての関連ポリシーにカスタム検出リストを適用する必要があります。そのため、グループとポリシーの関連付けを正確に計画することが非常に重要です。この演習では、監査ポリシーにのみ追加し、他はスキップします。特定のポリシーには、カスタム検出リストを 1 つしか適用できないことに注意してください。

演習 : AMP Update Server

Delthak 社の CIO は、TETRA という AMP for Endpoints AV エンジンを使用して、オフラインでの保護レベルを向上させることを決定しました。Delthak 社ネットワークの帯域幅オーバーヘッドと論理レイアウトを考えると、AMP Update Server を使用して WAN 帯域幅のオーバーヘッドを削減し、コネクタができるだけ迅速に定義ファイルを受信できるようにする必要がありますと判断されました。



ベスト プラクティス : TETRA エンジンが、デスクトップ、仮想環境、サーバで使用される環境では、AMP Update Server を設定することをお勧めします。1 つの組織で、複数の AMP Update Server が各地域のオフィスに定義を提供している場合があります (サーバはポリシーごとに構成されている)。リモートワークステーションとローミングシステムについては、AMP Update Server からではなく、AMP Cloud から直接アップデートをダウンロードすることをお勧めします。

手順

この演習では、用意されている CentOS 仮想マシンに AMP Update Server を設定します。そのためには、AMP for Endpoints Console からサーバソフトウェアと設定をダウンロードし、CentOS システムに導入する必要があります。次に、CentOS 上の Apache Web サーバで AV 定義をホストするように設定します。最後に、AMP Update Server 設定と、関連する AMP for Endpoints Console ポリシーを有効にします。

1. AMP for Endpoints Console で [管理 (Management)] → [ポリシー (Policies)] に移動し、[監査 (Audit)] という名前の Windows ポリシー レコードを展開して、[編集 (Edit)] をクリックします。
2. Windows 監査ポリシー内で [詳細設定 (Advanced Settings)] をクリックして [TETRA] を選択し、[AMP Update Server 設定 (AMP Update Server Configuration)] ボタンをクリックします。そのページの指示に従って、Linux 用のサーバソフトウェア (*update-linux.zip*) とサーバ設定 XML ファイル (*config.xml*) をダウンロードします。
3. デスクトップ上の [AMP Update SERVER SCP] ショートカットを使用して CentOS VM への SCP 接続を開いた後、ローカルの **Downloads** フォルダ (SCP セッションのフォルダではない) を開き、ダウンロードしたサーバソフトウェアと設定ファイルを */root* ディレクトリにドラッグアンドドロップします。
4. [AMP Update Server SSH] ショートカットを使用して CentOS VM に接続し、Apache Web サーバを設定します。このラボでは、最低限の作業用の設定を実施します。
 - a. Apache Web サーバをインストールしてサービスを開始し、ブート時に起動されるようにします。その後、次のコマンドを使用して動作していることを確認します (これらのコマンドをコピーして貼り付けるのではなく、入力します) 。
 - i. **yum install httpd**
 - ii. **systemctl start httpd**
 - iii. **systemctl enable httpd**
 - iv. **systemctl status httpd**

```
[root@centos ~]# systemctl start httpd
[root@centos ~]# systemctl enable httpd
[root@centos ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2019-03-14 09:33:02 EDT; 20h ago
     Docs: man:httpd(8)
           man:apachectl(8)
   Main PID: 5013 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic: 0 B/sec"
   CGroup: /system.slice/httpd.service
           └─5013 /usr/sbin/httpd -DFOREGROUND
             └─5058 /usr/sbin/httpd -DFOREGROUND
               └─5059 /usr/sbin/httpd -DFOREGROUND
                 └─5060 /usr/sbin/httpd -DFOREGROUND
                   └─5061 /usr/sbin/httpd -DFOREGROUND
                     └─5062 /usr/sbin/httpd -DFOREGROUND

Mar 14 09:33:00 centos.dcloud-cisco.com systemd[1]: Starting The Apache HTTP ...
Mar 14 09:33:02 centos.dcloud-cisco.com systemd[1]: Started The Apache HTTP S...
Hint: Some lines were ellipsized, use -l to show in full.
[root@centos ~]#
```


- b. Apache Web サーバがファイアウォールを通過して通信できるように設定し、次のコマンドを使用してファイアウォールをリロードします（これらのコマンドをコピーして貼り付けるのではなく、入力します）。

- i. `firewall-cmd --zone=public --permanent --add-service=http`
- ii. `firewall-cmd --zone=public --permanent --add-service=https`
- iii. `firewall-cmd --reload`

5. Web サーバを設定したら、AMP Update Server ソフトウェアを設定します（これらのコマンドをコピーして貼り付けるのではなく、入力します）。

- a. `/root` ディレクトリに **TETRA** という名前のフォルダを新たに作成し、そのフォルダに、先にダウンロードした AMP Update Server のソフトウェア パッケージ (`update-linux.zip`) を解凍して、スクリプトに実行権限を付与します。

- i. `mkdir /root/TETRA`
- ii. `unzip /root/update-linux.zip -d /root/TETRA`
- iii. `mv /root/config.xml /root/TETRA/config.xml`
- iv. `cd /root/TETRA`
- v. `chmod +x update-linux*`

- b. コマンドを実行して TETRA アップデート ファイルを取得し、ダウンロードが成功したことを確認します。完了するまで数分かかる場合があります。

- i. `sudo ./update-linux-x86-64 fetch --config config.xml --once --mirror /var/www/html/`
- ii. `cd /var/www/html/`
- iii. `ls`

```
INFO: [update-linux-x86-64] 2019/02/26 09:13:07 Microdefinition update complete for AV datab
ase av64bit.
INFO: [update-linux-x86-64] 2019/02/26 09:13:07 New files: 3
INFO: [update-linux-x86-64] 2019/02/26 09:13:07 Modified files: 0
DEBUG: [update-linux-x86-64] 2019/02/26 09:13:07 tetra.go:527: Activating the built-in HTTP
server
INFO: [update-linux-x86-64] 2019/02/26 09:13:07 Time taken: 905.865644ms
DEBUG: [update-linux-x86-64] 2019/02/26 09:13:07 tetra.go:693: Moving /var/www/html/av64bit/
versions.id.downloading into its final destination /var/www/html/av64bit/versions.id
[root@centos TETRA]# ls
config.xml  update-linux-1386  update-linux-x86-64
[root@centos TETRA]# cd /var/www/html/
[root@centos html]# ls
av32bit  av32bit_105867  av64bit  av64bit_75710  report  v1  v2
[root@centos html]#
```

注：実際の導入では、ディレクトリ構造によってコマンドが異なる場合があります。コマンドをコピーして貼り付けるのではなく、CLI で入力します。

- c. サーバのアップデート プロセスを自動化するには、サーバに cron ジョブを追加します。Cron は、Linux オペレーティング システムにおける時間ベースのジョブ スケジューラです。最も使用されるのは、一定の時間、日数、または間隔で定期的にジョブを実行するようにスケジュールする場合です。詳細については、<https://en.wikipedia.org/wiki/Cron> のリンクを参照してください。このアクションを実行するために、新しい SSH 接続を開きます。

i. vi /etc/crontab

- ii. `0 * * * * root /root/TETRA/update-linux-x86-64 fetch --config /root/TETRA/config.xml --once --mirror /var/www/html/`

```
# Example of job definition:
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .----- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# | | | | |
# * * * * * user-name  command to be executed
0 * * * * root /root/TETRA/update-linux-x86-64 fetch --config /root/TETRA/config.xml
--once --mirror /var/www/html/
```

注：ファイルの編集を開始するには、キーボードの「i」を押します。関連する cron エントリの前にある「#」c 記号を削除するだけです。ファイルの編集をやめる場合は、キーボードの「Esc」を押します。ファイルを保存する場合は、内部で「:wq!」と入力し、Enter を押します。

- iii. `sudo systemctl restart crond.service`

- iv. `systemctl status crond.service`

注：Crontab は非常に扱いにくい場合があります。フォーマット要件が異なるツールのバリエーションが複数あることに注意してください。また、指定されている手順は、Web ホスティング ソフトウェアのデフォルト ディレクトリからシグニチャが提供されることを前提としています。

6. 関連するポリシー（監査、保護、サーバ、その他）に移動し、AMP for Endpoint Console でポリシー設定を完了します。

- a. [詳細設定 (Advanced Settings)] → [TETRA] に移動し、[ローカル AMP Update Server (Local AMP Update Server)] の横にあるチェックボックスをオンにし、[AMP Update Server] フィールドに FQDN/IP (CentOS の IP アドレス：198.18.133.56) を指定します。[保存 (Save)] をクリックします。

Content Update Interval ⓘ

Local AMP Update Server ⓘ

AMP Update Server ⓘ

Use HTTPS for TETRA Definition Updates ⓘ

[AMP Update Server Configuration](#)

注：[TETRA の定義のアップデートに HTTPS を使用する (Use HTTPS for TETRA Definition Updates)] チェックボックスは、サーバに適切な証明書が設定され、エンドポイント コネクタが HTTPS を使用するように設定されている場合にのみオンにしてください。このラボでは、このチェックボックスはオフにします。

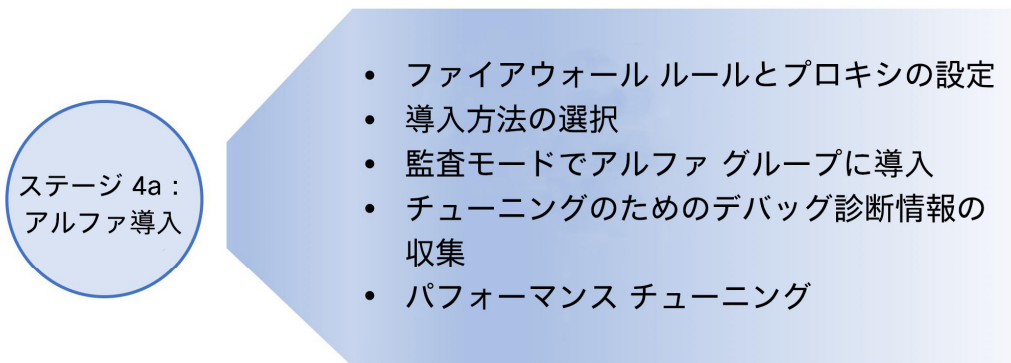
- b. 他のポリシーについてもこれらの手順を繰り返して、TETRA の定義のアップデートに AMP Update Server を使用するようにコネクタを設定します。
7. `/var/www/html/` ディレクトリに移動すると、AMP Update Server によって AMP Cloud から取得されたシグニチャを確認できます (しばらく時間がかかる可能性があるため、後のステージで検証する場合があります)。次の同期サイクル (デフォルトでは 1 時間) まで待てば、サーバからエンドポイント クライアントにシグニチャがダウンロードされ、[管理 (Management)] → [コンピュータ (Computers)] ページに結果が表示されます (AMP Update Server から TETRA 定義を正常に取得できたエンドポイントの場合、ステータスが [ポリシー内 (Within Policy)] になります)。エンドポイント コネクタはまだ導入されていないため、導入プロセスの後のステージでこの手順に戻ることができます。

<input type="checkbox"/>	 win-10-finance.Delthak.local in group Finance	✓ Within Policy	
<input type="checkbox"/>	 win-10-sales.Delthak.local in group Sales	✓ Within Policy	
<input type="checkbox"/>	 WIN-7-FINANCE.Delthak.local in group Finance	⚠ Definitions Outdated	
<input type="checkbox"/>	 WIN-7-SALES.Delthak.local in group Sales	✓ Within Policy	
<input type="checkbox"/>	 Win10-Marketing.Delthak.local in group Marketing	✓ Within Policy	

注：ステージ 4a、4b、5 の最後に、コネクタ導入後のステータスを確認します。定義を取得するにはしばらく時間がかかる場合があるので、ステータスがすぐに [ポリシー内 (Within Policy)] になるとは考えないでください。

ステージ 4a : アルファ導入

大規模なソフトウェア導入の場合と同様に、体系的な方法で確実に導入することをお勧めします。どんな環境に導入する場合でも、段階的に導入することで、問題が発生しても比較的限られたエンドポイントにしか影響を与えずに解決できます。これらの懸念事項は、特にセキュリティ ソフトウェアの場合に当てはまるため、シスコは、段階的なアプローチで AMP for Endpoints を導入することをベスト プラクティスとしています。このラボ ガイドの「導入プロセス」セクションのフローチャートに、各フェーズの概要が記載されています。



演習 : 監査導入 (アルファ グループ)

ステージ 1 ~ 3 では、現在の設定に関する情報を収集し、既知の除外リスト、グループ、ポリシーを使用してコンソールを設定しました。その情報が手元にあり、設定が完了したため、最初のエンドポイント グループへの導入を検討する準備が整いました。

ベスト プラクティス : アルファ導入は、組織の非常に小さなサブセットに対して実施します。組織の規模に応じて、全体のワークステーションの 1 ~ 10% で構成されます。実際の導入環境では、IT スタッフが導入プロセスを開始することを強くお勧めします。IT スタッフは、問題が発生した場合に診断できるスキルがあるため、ヘルプデスクに不要なチケットを発行せずに済みます。デバッグが有効になっている監査ポリシーを使用して、AMP for Endpoints Connector を導入することをお勧めします。監査ポリシーでは、ユーザのエンドポイントに悪影響が及ぶリスクを軽減しながら、デバッグによって、チューニングに使用できる貴重なデータが得られます。

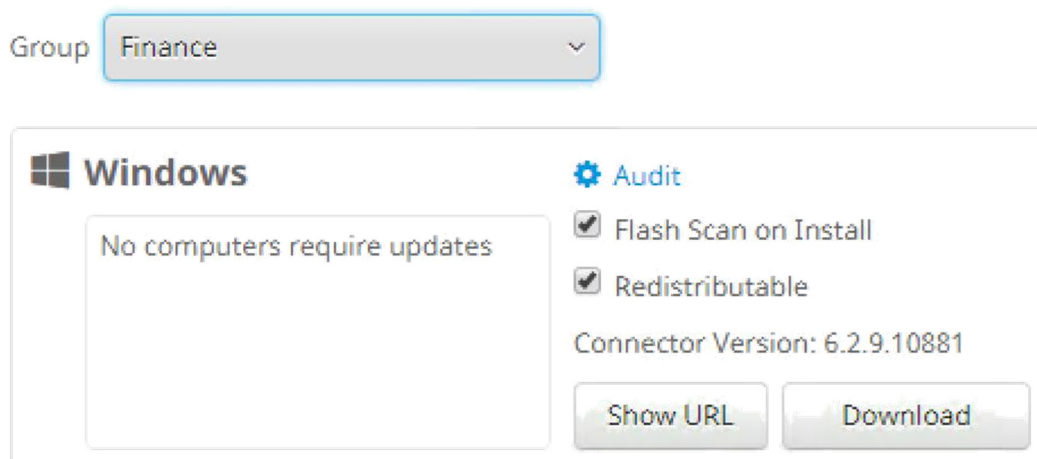
手順

この演習では、Delthak Industries 社の小規模な組織（ファイナンス部門の従業員が数名の組織）に AMP for Endpoints Connector を導入します。その際、必要な診断データを収集して除外リストを更新し、パフォーマンスの問題が発生するリスクに適切に対応できるようにチューニングします。

1. Google Chrome ブラウザを開いて AMP for Endpoints Console にログインし、[管理 (Management)] → [コネクタのダウンロード (Download Connector)] に移動します。[ファイナンス (Finance)] グループを選択後、[ダウンロード (Download)] をクリックして、AMP Connector for Windows を取得します。

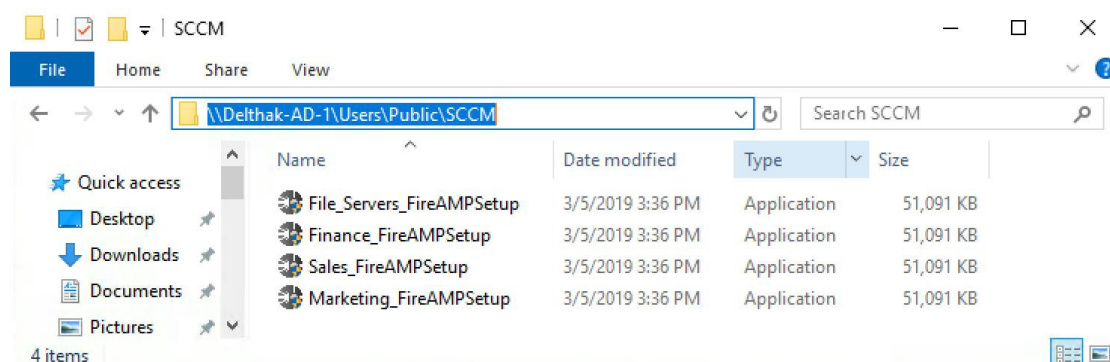
- 先に作成した他の子グループ（セールス、マーケティング、ファイルサーバ）に対して同じ手順を繰り返し、AMP Connector をダウンロードします。

Download Connector



注：デフォルトでは、AMP Connector の最新バージョンがダウンロードされます。古いバージョンは、選択したグループに割り当てられたポリシーの [製品アップデート (Product Update)] 設定で製品バージョンを変更すればダウンロードできます。

- 4 つすべての AMP Connector のインストーラをシステムの次の場所に移動します。
\\Delthak-AD-1\Users\Public\SCCM



- Student_Win** デスクトップの [SCCM] ショートカットを使用して、Microsoft System Center Configuration Manager (SCCM) ソフトウェアがインストールされている、Windows Server 2012R2 システム (**administrator/C1sco12345**) に対する RDP 接続を開きます。Server Manager を閉じ、デスクトップ上の [SCCM コンソール (SCCM Console)] ショートカットをクリックしてツールを起動します (アップデートに関する Configuration Manager のエラー メッセージが表示された場合は閉じます)。
- SCCM コンソールで、[ソフトウェアライブラリ (Software Library)] ワークスペースに移動し、[アプリケーション管理 (Application Management)] フォルダを展開します。[アプリケーション (Application)] を右クリックし、[フォルダ (Folder)] → [フォルダの作成 (Create Folder)] を選択します。わかりやすい名前をつけます (Cisco AMP for Endpoints など)。

6. [アプリケーション (Application)]ビューを展開し、新しく作成されたフォルダを右クリックして、[アプリケーションの作成 (Create Application)]を選択します。
 - a. SCCM では、アプリケーションで .exe がネイティブにサポートされていないため、[アプリケーション情報を手動で指定する (Manually specify the application information)] オプション ボタンを選択し、[次へ (Next)] をクリックして [全般情報 (General Information)] ウィザード ページに進む必要があります
 - b. AMP for Endpoints インストーラの [名前 (Name)] (AMP for Endpoints – Finance) 、 [発行元 (Publisher)] (Cisco) 、 [ソフトウェアバージョン (Software version)] (6.x.x) を指定し、[次へ (Next)] をクリックします。
 - c. [アプリケーションカタログ (Application Catalog)] ページで変更を加えずに [次へ (Next)] をクリックします。
 - d. [導入タイプ (Deployment Types)] ページで [追加 (Add)] をクリックすると、新しいウィザードが開きます。
 - I. [導入タイプの作成 (Create Deployment Type)] ウィザードで、[導入タイプ情報を手動で指定する (Manually specify the deployment type information)] オプション ボタンを選択し、[次へ (Next)] をクリックします ([タイプ (Type)] はそのままにしておきます) 。

- II. この導入タイプの [名前 (Name)] を「Install」とし、[次へ (Next)] をクリックします。
- III. [コンテンツ (Content)] ページで、[コンテンツの場所 (Content location)] の横にある [参照 (Browse)] をクリックし、次の場所を指定します。

\\DELTHAK-AD-1\Users\Public\SCCM

- IV. 同じ [コンテンツ (Content)] ページで、[インストールプログラム (Installation program)] に、ファイナンス部門用のインストーラの名前を指定します。コマンド ライン スイッチも指定し、[次へ (Next)] をクリックします。

Finance_FireAMPSetup.exe /R /S

注：インストール プログラム名は、先に AMP for Endpoints Console からダウンロードしたインストーラの名前と正確に一致させる必要があります。この特定のインストーラは、ファイナンス グループ用です。

Content location: \\DELTHAK-AD-1\Users\Public\SCCM Browse...

Persist content in the client cache

Allow clients to share content with other clients on the same subnet

This option allows clients that use Windows BranchCache to download content from on-premises distribution points. Content downloads from cloud-based distribution points can always be shared by clients that use Windows BranchCache.

Specify the command used to install this content.

Installation program: Finance_FireAMPSetup.exe /R /S Browse...

Installation start in:

注：AMP Connector のデフォルトおよびその他のコマンド ライン スイッチについては、次のドキュメントを参照してください：
<http://cs.co/amp-cmd-switches>

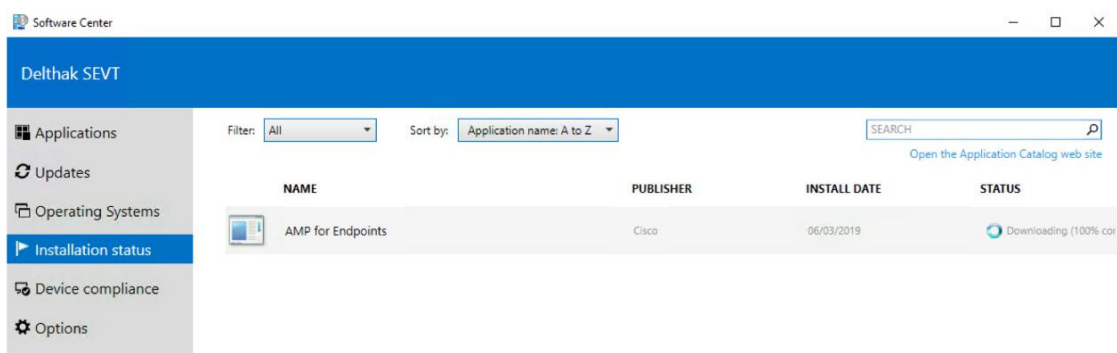
- V. [検出方法 (Detection Method)] ページで、[条件の追加 (Add Clause)] をクリックし、[タイプ (Type)] を [フォルダ (Folder)] に変更します。[パス (Path)] に **%Program Files%** を指定し、[ファイルまたはフォルダ名 (File or folder name)] に **Cisco** を指定します。[OK] をクリックしてから、[Next (次へ)] をクリックします。
- VI. [ユーザエクスペリエンス (User Experience)] ページで、[インストール動作 (Installation Behavior)] として [システム用にインストール (Install for system)] を選択し、[ログオン要件 (Logon requirement)] として [ユーザがログオンしているかどうか (Whether or not a user is logged on)] を選択します。[インストールプログラムの表示 (Installation program visibility)] 設定については、[通常 (Normal)] を選択します。[次へ (Next)] を 4 回クリックした後、[閉じる (Close)] をクリックします。
- e. [アプリケーションの作成 (Create Application)] ウィザードに戻り、[次へ (Next)] を 2 回クリックして、[閉じる (Close)] をクリックします。このプロセスが完了するまで数分かかります。

Icon	Name	Deployment Types	Deployments	Status
	AMP for Endpoints - Finance	1	1	Active

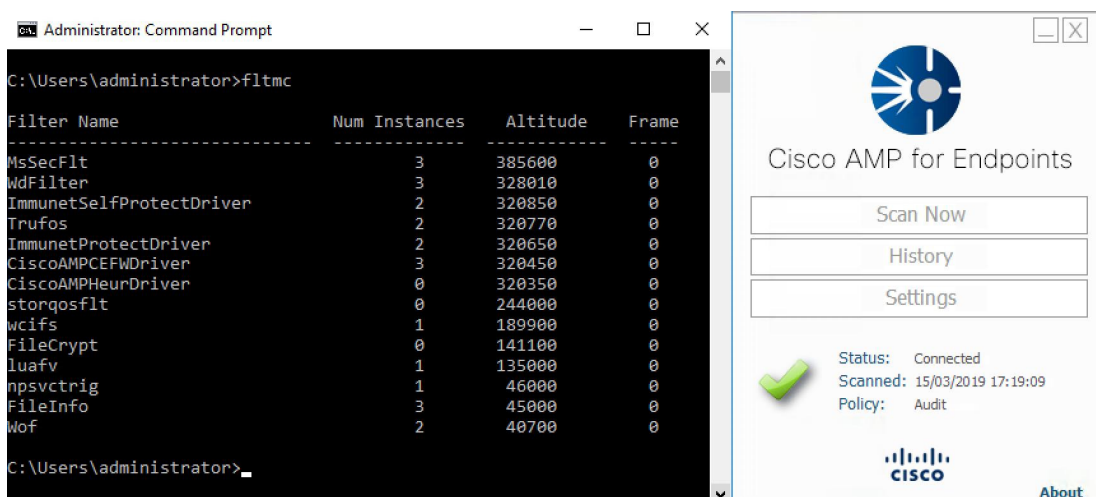
7. 新しいアプリケーションが作成されたら、配信ポイントに配信する必要があります。
[AMP for Endpoints – Finance] を右クリックし、[コンテンツの配信 (Distribute Content)] を選択します。
 - a. [コンテンツの配信先 (Content Destination)] ページが表示されるまで、[次へ (Next)] を 2 回クリックします。
 - b. [追加 (Add)] → [配信ポイント (Distribution Point)] をクリック後、配信ポイントとして [SCCMSERVER.DELTHAK.LOCAL] を選択し、[OK] をクリックします。
 - c. [次へ (Next)] を 2 回クリックして、[閉じる (Close)] をクリックします。
8. 配信ポイントを指定したら、いよいよ導入します。アプリケーション名 (**AMP for Endpoints – Finance**) を右クリックし、[導入 (Deploy)] を選択します。
 - a. [収集 (Collection)] 設定の横にある [参照 (Browse)] をクリックし、[デバイス収集 (Device Collection)] を選択後、**Workstations** フォルダを選択して [ファイナンス (Finance)] の収集を選択します。[OK] をクリックし、[導入設定 (Deployment Settings)] ページが表示されるまで [次へ (Next)] を 2 回クリックします。
 - b. [導入設定 (Deployment Settings)] ページで、[目的 (Purpose)] を [必須 (Required)] に変更する以外は変更せずに、ウィザードが終了するまでクリックします。

注：この演習で示されている導入手順以外で、SCCM を使用してソフトウェアを導入するためには、前提条件がいくつかあります。包括的なガイダンスについては、Microsoft 社のドキュメントを参照してください。

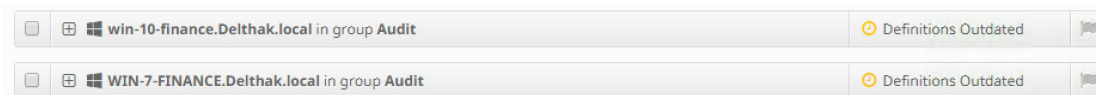
9. しばらくすると、ファイナンス部門のエンドポイントで、AMP for Endpoints Connector のインストール プロセスが開始されます。このプロセスをモニタするには、[Finance Win-7] または [Finance Win-10] ショートカットをクリックし、いずれかのシステムに対する RDP 接続 (**administrator/C1sco12345**) を新たに開きます (ショートカットは、**Student_Win** システムのデスクトップにあります)。RDP 接続を開くと、次に示すように、AMP for Endpoints ソフトウェアのインストール ステータスを確認できます。ステータスはすぐには表示されず、約 5 ~ 10 分かかります。それまで、デスクトップで [Software Center] のショートカットを開いて更新してください。



10. **Finance Win-7** および **Finance Win-10** システムにインストールが完了したら、Windows のタスクバーに新しいアイコンが表示されます。アイコンを右クリックし、[Cisco AMP for Endpoints を開く (OPEN Cisco AMP for Endpoints)] を選択します。
11. インストールが正常に完了し、AMP for Endpoints Connector が AMP Cloud と通信できている場合は、ステータスが [接続済み (Connected)] として表示されます。合わせて、割り当てられたポリシーも表示されます。また、Windows コマンドラインで **fltmc** コマンドを発行するとフィルタ ドライバが表示され、基本的な検証を行うこともできます。ドライバのステータスを表示するもう 1 つの便利なコマンドは、**sc query <ドライバ名>** です。



12. **Student_Win** デスクトップで Google Chrome ブラウザを開き、[AMP for Endpoints] ブックマーク (studentXXX@sfsnort.com/@mp_Tr41n) をクリックして、管理コンソールを開きます。[管理 (Management)] → [コンピュータ (Computers)] に移動します。2 つのエンドポイントが表示されます。レコードを展開して **グループ** と **ポリシー** の割り当てを検証し、その他の設定を確認します。質問がある場合は、監督者に問い合わせてください。



演習：コネクタのチューニング (アルファ グループ)

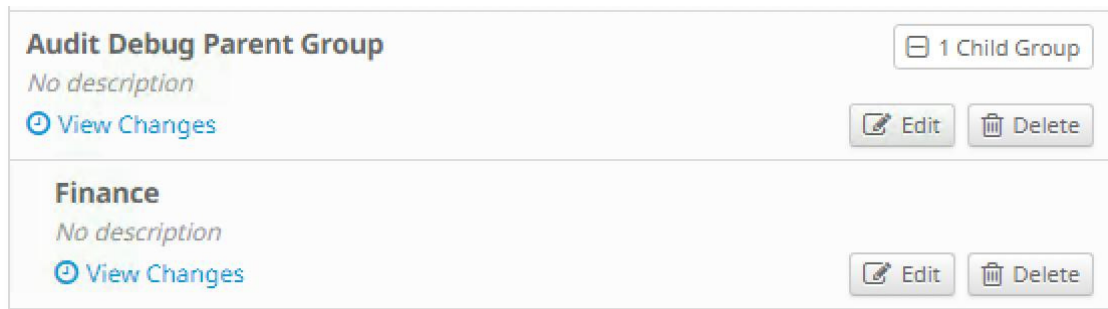
コネクタを導入し、AMP for Endpoints Console に登録したら、一定期間データを収集できるようにします。そうすることで、コネクタは、追加の除外リストを作成するために利用可能なデータを取得できます。実際の導入環境では、エンドポイントから診断パッケージを取得する準備が整う 30 分前 (できれば 1 時間前) には、コネクタを登録してアクティブにする必要があります。

ベスト プラクティス： 必要な除外リストが特定され、実装されていることを確認するために、このプロセスを業務時間内に 2 回以上実行することをお勧めします。

手順

この演習では、ファイナンス グループのエンドポイントに対してデバッグ ログを有効にします。次に、AMP for Endpoints Console の [コンピュータ (Computers)] ページに組み込まれている診断ツールを活用して、診断パッケージを収集します。最後に、Github から利用可能なチューニング ツールを取得して実行し、追加の除外リストが必要かどうかを判断します。

1. Google Chrome ブラウザを開き、AMP for Endpoints Console にログインします (**studentXXX@sfsnort.com/@mp_Tr41n**)。次に [管理 (Management)] → [ポリシー (Policies)] に移動し、[監査-デバッグ (Audit - Debug)] ポリシーをクリック後、[編集 (Edit)] をクリックします。[詳細設定 (Advanced Settings)] → 選択したポリシーの [管理機能 (Administrative Features)] を開き、[コネクタログレベル (Connector Log Level)] と [トレイログレベル (Tray Log Level)] を [デバッグ (Debug)] に変更します。[保存 (Save)] をクリックします。
2. AMP for Endpoints Console で、[管理 (Management)] → [グループ (Groups)] に移動し、**監査親グループ**に属する子グループのリストを展開し、[ファイナンス (Finance)] グループの横にある [編集 (Edit)] をクリックします。[親グループ (Parent Group)] を [監査デバッグ親グループ (Audit Debug Parent Group)] に変更し、[保存 (Save)] をクリックします。



注：ファイナンス グループのエンドポイントが [監査-デバッグ (Audit - Debug)] グループの設定を継承する場合、AMP Cloud から新しいポリシーを取得する必要があります。これは、コネクタのハートビート時に自動的行われます (デフォルトの間隔は 15 分)。AMP Connector 設定 UI (エンドポイント自体の UI) の [ポリシーの同期 (Sync Policy)] ボタンをクリックして、手動でプロセスをトリガーすることもできます。

3. [管理 (Management)] → [コンピュータ (Computers)] ページに移動し、アルファグループ (ファイナンス エンドポイントが 2 台) のエンドポイント レコードを展開します。**Win-10-Finance** エンドポイントの場合は、[診断 (Diagnose)] ボタンをクリックし、[デバッグセッション (Debug session)] で [5 分 (5 minutes)] を選択します。[履歴データ (Historical Data)] と [カーネルログ (Kernel Log)] のチェックボックスはそのままにします。[作成 (Create)] をクリックします。時間の節約のため、**Win-10-Finance** エンドポイントの診断情報のみを収集します。

×
New Connector Diagnostic for win-10-finance.Delthak.local

A new Connector diagnostic was requested for 'win-10-finance.Delthak.local'.

Debug session 5 minutes

Historical Data

Kernel Log

Diagnostic files are limited to 50MB in size and can take up to 24 hours to generate.

Cancel
Create

注： [履歴データ (Historical Data)] をチェックすると、診断が行われた時点でマシンに存在している、使用可能な AMP Connector デバッグ ログがすべて取得されます。[カーネルログ (Kernel Log)] をチェックすると、Cisco TAC に提供する詳細情報を収集可能な、詳細なログが取得されます (標準のファイル チューニングでは効果がない場合)。

4. 診断を要求した直後に、[Finance Win-10] ショートカットを使用して、対象のエンドポイントに対して RDP 接続を開きます。C:\ に移動し、**Financials** という名前のスクリプトをダブルクリックして実行します。
5. [診断 (Diagnostics)] ビューを閉じて [分析 (Analysis)] → [ファイルリポジトリ (File Repository)] に移動し、[タイプ (Type)] フィルタで [コネクタ診断 (Connector Diagnostics)] を選択します。

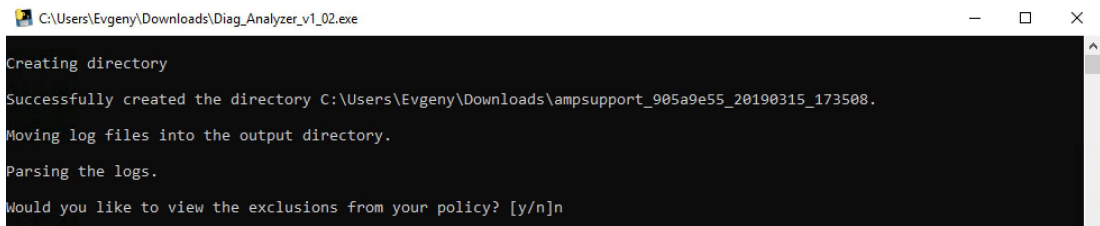
注： 要求後 7 ~ 10 分以内に診断パッケージが表示されます。10 分経ってもパッケージが表示されない場合は、監督者に知らせてください。

6. 診断パッケージが利用可能になったら、[ダウンロード (Download)] を 2 回クリックして、自分の **Student_Win** システムのローカル ドライブにダウンロードします。

Connector diagnostics for WIN-7-FINA... has been Requested		Requested by Evgeny Mirolyubov	2019-03-06 11:05:03 CET
Connector diagnostics for win-10-fina... is Available		Requested by Evgeny Mirolyubov	2019-03-06 11:04:47 CET
Connector Diagnostics Requested	2019-03-06 10:59:17 CET		
Original File Name	ampsupport_ec23d976_20190306_180440.7z		
File Size	3.3 MB		
Computer	win-10-finance.Delthak.local		
View Changes		Download	Remove

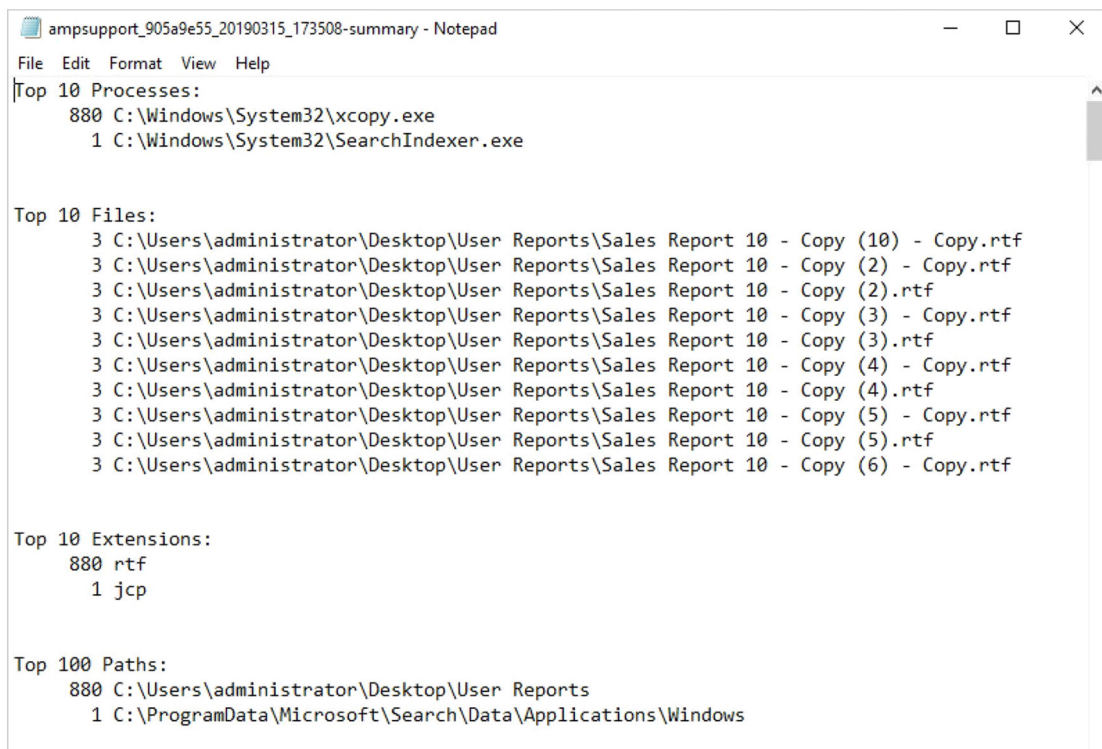
7. Github から Windows Connector Tuning Tool をダウンロードします。 <http://cs.co/amp-tune> にアクセスし (Google Chrome でブックマークを使用)、リポジトリから最新の **Diag_analyzer_v1_02.exe** をダウンロードします (Windows で不審なコンテンツに関するメッセージが表示されてもダウンロードしてかまいません)。 **Downloads** フォルダを開き、**Diag_analyzer_v1_02.exe** ツールと **ampsupport%** 診断パッケージがいずれも同じフォルダ内にあることを確認します。

8. **Diag_analyzer_v1_02.exe** ツールをダブルクリックし、**Win-10-Finance** エンドポイントから新たに収集した診断パッケージに対して実行します。正当なツールであるため、Windows からの警告をスキップし、[実行 (Run Anyway)] をクリックします (インターネットからダウンロードした未知のソフトウェアの場合、通常はこのようなことはしません)。以下のスクリーンショットに示すように、質問には「n」と入力し、ポリシーの除外リストは表示しません。



```
C:\Users\Evgeny\Downloads\Diag_Analyzer_v1_02.exe
Creating directory
Successfully created the directory C:\Users\Evgeny\Downloads\ampsupport_905a9e55_20190315_173508.
Moving log files into the output directory.
Parsing the logs.
Would you like to view the exclusions from your policy? [y/n]n
```

9. ツールを実行すると、Downloads フォルダ (またはツールが実行されたフォルダ) に、**ampsupport%-summary.txt** ファイルが作成されます。出力結果は、Github ページのスクリプト出力例または、次に示す出力例のようになります。



```
ampsupport_905a9e55_20190315_173508-summary - Notepad
File Edit Format View Help
Top 10 Processes:
  880 C:\Windows\System32\xcopy.exe
   1 C:\Windows\System32\SearchIndexer.exe

Top 10 Files:
  3 C:\Users\administrator\Desktop\User Reports\Sales Report 10 - Copy (10) - Copy.rtf
  3 C:\Users\administrator\Desktop\User Reports\Sales Report 10 - Copy (2) - Copy.rtf
  3 C:\Users\administrator\Desktop\User Reports\Sales Report 10 - Copy (2).rtf
  3 C:\Users\administrator\Desktop\User Reports\Sales Report 10 - Copy (3) - Copy.rtf
  3 C:\Users\administrator\Desktop\User Reports\Sales Report 10 - Copy (3).rtf
  3 C:\Users\administrator\Desktop\User Reports\Sales Report 10 - Copy (4) - Copy.rtf
  3 C:\Users\administrator\Desktop\User Reports\Sales Report 10 - Copy (4).rtf
  3 C:\Users\administrator\Desktop\User Reports\Sales Report 10 - Copy (5) - Copy.rtf
  3 C:\Users\administrator\Desktop\User Reports\Sales Report 10 - Copy (5).rtf
  3 C:\Users\administrator\Desktop\User Reports\Sales Report 10 - Copy (6) - Copy.rtf

Top 10 Extensions:
  880 rtf
   1 jcp

Top 100 Paths:
  880 C:\Users\administrator\Desktop\User Reports
   1 C:\ProgramData\Microsoft\Search\Data\Applications\Windows
```

注：Windows Connector Tuning Tool は、Cisco TAC ではサポートしていません。お客様はこのツールを自由に使用できますが、問題が発生した場合は、Github で問題として報告する必要があります。Cisco TAC は、このツールを使用してお客様をサポートすることはありません。チューニングに関するケースがオープンされた場合、TAC は、エンドポイントを直接チューニングしてサポートします。

10. 出力結果を注意深く確認し、実装する必要がある除外対象を判断します。AMP for Endpoints Console に、判断した結果の除外対象を追加します。必要に応じて、導入プロセスの第 3 ステージで実施した除外リスト演習で示されている、除外リストに関するベスト プラクティス ドキュメントを確認することができます。検証のために監督者に結果を提示し、サポートが必要な場合は依頼します。

ベスト プラクティス : AMP for Endpoints Connector を少ないリソースで安定稼働させるために、コネクタのチューニングは、実行可能な範囲内で、できるだけ多くのエンドポイントをサンプルとして、繰り返し実行する必要があります。

演習 : コネクタのアクティベーション (アルファ グループ)

最初のアルファ グループにコネクタを導入してチューニングし、除外リストを追加してパフォーマンス リスクを軽減したら、エンドポイント コネクタを、保護ポリシーが設定されている別の親グループに移動してアクティブにすることができます。このステージでは、パフォーマンスの問題とヘルプ デスクへのチケットの監視を続けます。

ベスト プラクティス : エンドポイントを保護モードに移行する前に、除外リストが正しく設定されていること、および、誤検出を回避するために、カスタム ソフトウェアが、アプリケーション ホワイトリストに追加されていることを確認します。別の問題が発生し、監査モードに戻す必要がある場合は、子グループを、監査デバッグ親グループに戻すだけです。ただし、エンドポイントが保護モードで実行されている間に、診断パッケージを収集することも検討してください。除外リストを複数回チューニングしても問題を解決できない場合は、Cisco TAC サポートにケースをオープンしてください。より詳細な分析が必要な、未知の問題が発生している可能性があります。

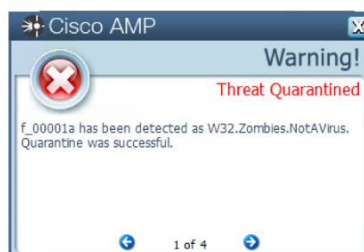
手順

この演習は、コネクタを、監査モード ポリシーから保護モード ポリシーに移動するだけの簡単なものです。すでに説明したように、この 2 つのモードの大きな違いは、保護モードでは既知の悪意のあるファイルを検疫し、C2 トラフィックをブロックしたり、その他の保護アクションを実行したりするのに対して、監査モードでは、アクティビティを記録するだけで、ブロックはしないという点です。

1. Google Chrome ブラウザを開き、AMP for Endpoints Console にログインします (必要な場合)。次に、[管理 (Management)] → [グループ (Groups)] に移動し、[監査デバッグ親グループ (Audit Debug Parent Group)] に属する子グループのリストを展開して、[ファイナンス (Finance)] グループの横にある [編集 (Edit)] をクリックします。[親グループ (Parent Group)] を [保護親グループ (Protect Parent Group)] に変更し、[保存 (Save)] をクリックします。

- [Finance Win-10] ショートカットをクリックして、Finance Win-10 システムに対する RDP 接続を開きます (**administrator/C1sco12345**)。タスクバーの AMP for Endpoints アイコンを右クリックし、[Cisco AMP for Endpoints を開く (Open Cisco AMP for Endpoints)] をクリックします。クライアント ユーザ インターフェイスの [設定 (Settings)] ボタンをクリック後、[ポリシーの同期 (Sync Policy)] をクリックします。
- Finance Win-10** システムに接続したまま Google Chrome ブラウザを開き、[Zombies.pdf] ブックマークをクリックして、何回かこのファイルのダウンロードを試みます。AMP for Endpoints Connector が新しい保護モード ポリシーを正常に取得できていた場合、ダウンロードは失敗します。

注: クライアント ユーザ インターフェイス設定 (詳細設定) で、ファイル通知を表示している場合は、脅威がブロックされたことを示す警告が表示された、小さな UI 要素も確認できます。デフォルトでは、ユーザの邪魔にならないように、これらの通知は非表示になっています。



- (**Student_Win** から) AMP for Endpoints Console に戻ると、複数の脅威検出イベントが表示され、脅威が正常に検疫されたことを確認できます ([ダッシュボード (Dashboard)] → [イベント (Events)])。これは、エンドポイントが、保護グループのポリシーを正常に継承していることを意味します。

win-10-finance.Deithak.local detected f_00001c as W32.Zombies.NotAVirus		Medium	Quarantine: Successful	2019-03-06 10:38:20 CET
File Detection	Detection	W32.Zombies.NotAVirus		
Connector Info	Fingerprint (SHA-256)	00b32c34...989bb002		
Comments	File Name	f_00001c		
	File Path	C:\Users\administrator\AppData\Local\Google\Chrome\User Data\Default\Cache\f_00001c		
	File Size	302.25 KB		
	Parent Fingerprint (SHA-256)	1a9bae25...0c217cd6		
	Parent Filename	chrome.exe		
Report		0	5	Restore File All Computers
		View Upload Status		Add to Whitelist File Trajectory

ステージ 4b : ベータ導入

比較的小規模なアルファ導入とは異なり、初回のベータ導入は、大規模なエンドポイントグループを対象とします。それでも、組織全体に占める割合はごく一部です。ベータ導入ステージは、各統合においてインストール ベースを拡張しながら、数回繰り返します。そうすることで、インストール ベースを確実に完全拡大することができます。ベータ導入は、監査デバッグ設定で開始し、初期のチューニング完了後に保護デバッグ ステージに移行します。チューニングが完了し、エンドポイントの問題が解決されたら、デバッググループから、標準の保護グループに移行できます。

ステージ 4b :
ベータ導入

- アルファグループから保護ポリシーへ
- 新しい診断データ収集
- パフォーマンス チューニング
- 監査モードでベータ グループに導入
- 必要に応じてコンソール セットアップを確認
- 必要に応じてベータ導入を繰り返す

ベスト プラクティス : ミッション クリティカルなシステム (サーバなど) のテスト環境がある場合は、ベータ導入は、テスト環境で行います。ベータ導入の対象となるエンドポイントを選択する場合は、すべての部門またはエンドポイント ロールから少しずつ選択します。そうすることで、対象の環境全体を理解し、各部門からのフィードバックに基づいて、診断やチューニングを円滑に実施できます。ベータ導入ステージは、対象となるすべてのエンドポイント グループ全体で、最大の互換性とパフォーマンスを確保できるように、複数回繰り返す必要があります。

演習 : 監査導入 (ベータ グループ)

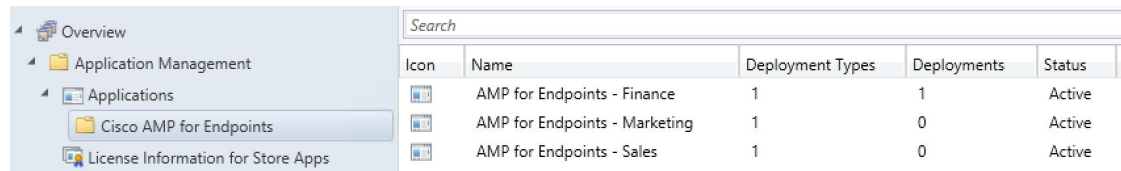
ここから反復的な導入を開始します。アルファ導入ステージと同様に、まず、監査モードで AMP Connector を導入するところから始め、Delthak 社の組織に、より多くのエンドポイントを導入していきます。そうすることで、最初の導入環境が拡張され、役割や職務、ソフトウェア セット、ユーザのふるまいが異なる他の部門をカバーできるようになります。

手順

この演習では、Delthak Industries 社の別のサブセット (セールスおよびマーケティング部門の数名の従業員) に AMP for Endpoints Connector を導入し、必要な診断データを収集して、さらにチューニングを行います。

1. Student_Win システムで、SCCM ショートカットをクリックします (**administrator/C1sco12345**)。SCCM コンソールが閉じている場合は、再度開きます。

2. ソフトウェア ライブラリ ワークスペースに移動し、[アプリケーション管理 (Application Management)] → [アプリケーション (Applications)] → [Cisco AMP for Endpoints] フォルダの順に展開します。1 つのアプリケーションが [AMP for Endpoints – Finance] に追加されているのを確認できます。
3. [AMP for Endpoints – Finance] を右クリックし、[コピー (Copy)] を選択します。
4. コピーが作成されたら、その名前を右クリックして [プロパティ (Properties)] を選択します。
 - a. [全般情報 (General Information)] タブで、[名前 (Name)] を **AMP for Endpoints – Sales** に変更します。
 - b. [導入タイプ (Deployment Types)] タブで、[インストール (Install)] という既存の導入タイプをダブルクリックします。
 - i. [プログラム (Program)] タブに移動し、[インストールプログラム (Installation program)] を **Sales_FireAMPSetup.exe /R /S** に変更して、[OK] を 2 回クリックします。
5. 同じ手順で **マーケティング** 導入用にもう 1 つコピーを作成します。[インストールプログラム (Installation program)] は、**Marketing_FireAMPSetup.exe /R /S** になります。



Icon	Name	Deployment Types	Deployments	Status
	AMP for Endpoints - Finance	1	1	Active
	AMP for Endpoints - Marketing	1	0	Active
	AMP for Endpoints - Sales	1	0	Active

6. 新しいアプリケーションが作成されたら、配信ポイントに配信する必要があります。**AMP for Endpoints – Sales** を右クリックし、[コンテンツの配信 (Distribute Content)] を選択します。
 - a. [コンテンツの配信先 (Content Destination)] ページが表示されるまで、[次へ (Next)] を 2 回クリックします。
 - b. [追加 (Add)] → [配信ポイント (Distribution Point)] をクリック後、配信ポイントとして [SCCMSERVER.DELTHAK.LOCAL] を選択し、[OK] をクリックします。
 - c. [次へ (Next)] を 2 回クリックして、[閉じる (Close)] をクリックします。
7. 配信ポイントを指定したら、いよいよ導入します。アプリケーション名 (**AMP for Endpoints – Sales**) を右クリックし、[導入 (Deploy)] を選択します。
 - a. [収集 (Collection)] 設定の横にある [参照 (Browse)] をクリックし、[デバイス収集 (Device Collection)] を選択後、**Workstations** フォルダを選択して、[セールス (Sales)] の収集を選択します。[OK] をクリックし、[導入設定 (Deployment Settings)] ページが表示されるまで [次へ (Next)] を 2 回クリックします。
 - b. [導入設定 (Deployment Settings)] ページで、[目的 (Purpose)] を [必須 (Required)] に変更する以外は変更せずに、ウィザードが終了するまでクリックします。
8. **AMP for Endpoints – Marketing** についても同じ手順を繰り返し、コンテンツを配信して、ソフトウェアを導入します。

- しばらくすると、セールスおよびファイナンス部門のエンドポイントで AMP for Endpoints Connector のインストール プロセスが開始されます。アルファ グループと同様に、これらのシステムの **Software Center** を利用してプロセスをモニタできます。
- インストールが完了すると、これらのシステム上に AMP for Endpoints のアイコンが表示されます。また、AMP for Endpoints Console の [管理 (Management)] → [コンピュータ (Computers)] に、エンドポイント コネクタが表示されます。

演習：コネクタのチューニング (ベータ グループ)

ベータ グループのチューニング演習は、アルファ グループの場合とほぼ同じです。唯一の違いは、ベータ ステージで導入されたエンドポイントが対象になることです。このステージでは、エンドポイントの役割と対象の組織部門がそれぞれ異なるため、考慮が必要な除外要件が異なる可能性があります。

手順

この演習では、セールスおよびマーケティング部門のエンドポイントに対してデバッグ ログを有効にします。次に、アルファ グループのチューニング フェーズと同様に、診断ツールとチューニング ツールを活用します。

- AMP for Endpoints Console (**studentXXX@sfsnort.com/@mp_Tr41n**) で、[管理 (Management)] → [グループ (Groups)] に移動します。 **監査親グループ** に属するグループのリストを展開し、 **監査デバッグ親グループ** に移動します (**セールスとマーケティング** の 2 グループを移動させます)。これらの子グループに属するエンドポイントは、次のコネクタ ハートビート時に、 **監査-デバッグ** グループの設定を継承します。
- [管理 (Management)] → [コンピュータ (Computers)] ページに移動し、ベータ グループのエンドポイント (セールス エンドポイント 2 台、マーケティング エンドポイント 1 台) のレコードを展開します。 **Win-10-Sales** エンドポイントの場合は、[診断 (Diagnose)] ボタンをクリックし、[デバッグセッション (Debug session)] で [5 分 (5 minutes)] を選択します。[履歴データ (Historical Data)] と [カーネルログ (Kernel Log)] のチェックボックスはそのままにします。[作成 (Create)] をクリックします。
- 診断を要求した直後に、[Sales Win-10] ショートカットを使用して、対象のエンドポイントに対して RDP 接続を開きます。デスクトップの **Sales Orders** フォルダに移動し、そのフォルダからすべてのファイルを削除します。次に **C:\Scripts** に移動し、 **Salaries** という名前のスクリプトをダブルクリックして実行します。

4. [分析 (Analysis)] → [ファイルリポジトリ (File Repository)] に移動し、新たに要求されたパッケージがアップロードされたら、ダウンロードします (このプロセスには 7 ~ 10 分かかる場合があります。これ以上時間がかかる場合は、監督者に知らせてください)。前のチューニング演習と同様に、**Win-10-Sales** エンドポイントから新たにダウンロードした診断パッケージと、**Diag_analyzer_v1_02.exe** ツールを、同じフォルダに配置します。その他の診断パッケージは、すべてそのフォルダから削除します。
5. **Diag_analyzer_v1_02.exe** をダブルクリックしてツールを実行します (既存の除外リストを表示させないでください)。これにより、**ampsupport%-summary** テキスト ファイルが作成され、AMP Connector によって、上位のプロセス、ファイル、拡張子、パスが設定されます。
6. 出力結果を注意深く確認し、実装する必要がある除外対象を判断します。AMP for Endpoints Console に、判断した結果の除外対象を追加します。必要に応じて、導入プロセスの第 3 ステージで実施した除外リスト演習で示されている、除外リストに関するベスト プラクティス ドキュメントを確認することができます。検証のために監督者に結果を提示し、サポートが必要な場合は依頼します。

注：チューニング ツールの出力結果を利用して、最もアクセスが多く、最も頻繁に利用されるファイルとプロセスを特定します。ビジネス環境に対する有効性と外部環境に対する脆弱性を検証し、ファイルやプロセスに脆弱性が存在している場合は、把握していることを確認します。

演習：コネクタのアクティベーション (ベータ グループ)

コネクタを広範なベータ グループに導入してチューニングを実施し、除外リストを追加したら、保護モードに移行することで、エンドポイント コネクタをアクティブにできます。パフォーマンスの問題とヘルプ デスクへのチケットは、引き続き監視します。除外リスト、アプリケーション ホワイトリスト、チューニングに関して、ベータ グループにも、同じ一連のベスト プラクティスが適用されます。

手順

この演習は、ベータ グループのコネクタを、監査モード ポリシーから保護モード ポリシーに移動するだけの簡単なものです。

1. Google Chrome ブラウザを開き、必要に応じて AMP for Endpoints Console にログインします (**studentXXX@sfsnort.com/@mp_Tr41n**)。次に、[管理 (Management)] → [グループ (Groups)] に移動し、[監査デバッグ親グループ (Audit Debug Parent Group)] に属する子グループのリストを展開して、[セールス (Sales)] グループの横にある [編集 (Edit)] をクリックします。[親グループ (Parent Group)] を [保護親グループ (Protect Parent Group)] に変更し、[保存 (Save)] をクリックします。**マーケティング**の子グループについても同じ手順を繰り返します。

2. **Sales Win-10** や **Marketing Win-10** などの新たにアクティブ化されたいくつかのシステムから **Zombies.pdf** (Chrome でブックマークされています) をダウンロードしようとすることで、エンドポイントに保護ポリシーが継承されていることを確認できます。ダウンロードは失敗するはずですが、これらのシステムに接続するための RDP ショートカットは、**Student_Win** デスクトップにあります (**administrator/C1sco12345**) 。

注：1つのグループから別のグループに移動した直後にこの検証を実施する場合は、AMP Connector UI からポリシーを手動で同期する必要があります。

3. 次に、AMP for Endpoints Console の [ダッシュボード (Dashboard)] → [イベント (Events)] ビューで、関連するファイル検疫イベントを確認します。

ステージ 5：全体導入

アルファとベータの導入ステージが両方成功すれば、全体導入が実質的に可能になります。エンドポイントは、保護モードをアクティブにしてインストールします。これは、コネクタをアクティベーションする手順がないことを意味します。このステージでは、ポリシー、グループ、除外リストを適切に設定し、対象の環境に合わせてチューニングする必要があります。設定とパフォーマンスの問題は最小限に抑えられ、管理者は、一般的にどのような状態になるかを想定しているはずで

ステージ 5：
全体導入

- 段階的に全体導入
- 必要に応じて新しい診断データを収集
- 必要に応じてパフォーマンス チューニング
- 環境モニタリング
- 必要に応じてコンソール セットアップを確認

ベスト プラクティス：互換性のあるすべてのエンドポイントに導入できるように、全体導入計画を策定します。導入チームがやりやすいステージに分けて、すべてのエンドポイントに導入します。重要度の低いシステムから始め、徐々に重要度を上げながら、最後に最も重要なシステムに導入します。各導入ステージ間で十分時間を確保し、フィードバック ループを完了させ、必要に応じてチューニングを実施します。

演習：全体導入

この時点で、企業全体に導入する準備が整いました。導入を成功させるためには、除外リストと問題への対応が 90% 以上完了していると確信する必要があります。また、AMP Connector をまだ導入していないシステムに対して、監査モード導入をせずに、保護モードで直接導入することにも自信がなければなりません。このステージでは、通常、新しい組織単位、システムグループ、ユーザ ロールは対象にしません。

手順

全体導入の定義では、通常、アルファ導入フェーズおよびベータ導入フェーズで得たスキルを、互換性のあるすべてのエンドポイントを対象に実践できることを前提としています。このラボの目的のためだけでなく、実験の余地を残すために、最小限のガイダンスでファイルサーバに AMP Connector を導入します。

1. SCCM コンソールで、ファイル サーバ用の新しい AMP for Endpoints アプリケーションを作成します。
2. 適切なコマンドライン スイッチを使用して、インストール プログラムを指定します。

3. SCCM を使用してコンテンツを配信ポイントに配信し、ファイル サーバに導入します。
4. ファイル サーバ上の AMP Connector を確認し、AMP for Endpoints Console を利用してインストールが成功したことを検証します。

考慮事項：コネクタのチューニング

環境内でパフォーマンスと互換性の問題が解消されるまで、コネクタのチューニングを行う必要があります。アルファ導入とベータ導入の両フェーズで除外リストが十分に検討されている場合、このステージでのチューニングは、最小限のものとなります。ただし、現在ほとんどの環境が常に変化しているため、反復可能なプロセスを確立し、問題が発生した場合に迅速に解決できるようにしておくことをお勧めします。そのプロセスには、ヘルプ デスク コールのために企業全体のすべての部門をモニタリングするだけでなく、新たに導入されたエンドポイントの役割に関する診断パッケージを収集することも含まれます。時間の節約のために全体導入ステージではこの演習をスキップしますが、このプロセスが、導入 - 診断 - チューニングという反復可能なループとして機能することを理解できたと思います。

ステージ 6 : 統合

AMP for Endpoints は、セキュリティ ソリューション アーキテクチャの一部として設計されています。そのため、多数の Cisco Security 製品とネイティブに統合されています。さらに、AMP for Endpoints は、Splunk と Q-Radar の両方に対して事前に構築されたプラグインを備えており、大半の SIEM 製品やアラート システムと API で統合することができます。これらの統合によって、クロス プラットフォームでの検出や対応が可能な統合アーキテクチャが形成されます。

ステージ 6 :
統合の
セットアップ

- シスコ製品のネイティブ統合設定
- API クレデンシャルの作成
- サードパーティ製品の統合設定

演習 : Threat Response

革新的なプラットフォームである Cisco Threat Response は、セキュリティに関連する情報をシスコやサードパーティのソースから収集します。収集した情報は、直感的に使用できる単一の調査/対応コンソールに集約されます。Threat Response のモジュールにより、関係を示すグラフが作成され、データの相互関連付けを迅速に行えるため、セキュリティ チームは攻撃を明確に把握するとともに、効果的な対応アクションを迅速に実行できます。また、このラボの最初に有効化した「Casebook」という統合ケース管理ツールによって、日常的なワークフローが効率化されます。

手順

Delthak 社のセキュリティ運用チームは、Threat Response プラットフォームを活用したいと考えています。AMP for Endpoints モジュールを Cisco Threat Response に追加することで、調査担当者は、AMP for Endpoints によって記録された IP アドレス、ドメイン、URL、ファイル ハッシュを検索できるようになります。

1. Google Chrome ブラウザを開いて [Threat Response] ブックマークをクリックし、[Cisco Security アカウントでログインする (Log In with Cisco Security)] ボタンをクリックしてログインし、AMP for Endpoints へのログインに使用したものと同一クレデンシャルを入力します (**studentXXX@sfsnort.com/@mp_Tr41n**) 。

注：このガイドを執筆している時点では、Threat Response は、AMP for Endpoints ユーザ アカウントが管理者特権を持っており、プラットフォームにアクセスして活用できることを前提としています。トークンが期限切れになっていなければ、ログインするためにクレデンシャルを入力する必要もありません。

2. Threat Response にログインしたら、[モジュール (Module)] をクリックします。AMP Global Intel、Private AMP Global Intel、AMP File Reputation、Talos Intelligence など、さまざまなモジュールがデフォルトで有効になっていることがわかります。
3. 同じページで、[新しいモジュールの追加 (Add New Module)] をクリックします。ここで、AMP for Endpoints 用のモジュールを追加します。開いているダイアログウィンドウの指示に従います。[サードパーティ API クライアント ID (3RD PARTY API CLIENT ID)] と [API キー (API KEY)] フィールドに入力したら、[モジュールの作成 (Create Module)] をクリックして確認します。

The image shows a configuration form for creating a new module in Threat Response. The form fields are as follows:

- MODULE TYPE:** AMP for Endpoints - Advanced Malware Protection
- MODULE NAME:** AMP for Endpoints
- URL:** https://api.amp.cisco.com
- 3RD PARTY API CLIENT ID:** 1b2202fb763d0a26c180
- API KEY:** (masked with dots)

Buttons: Cancel, Create Module

* Required

On the right, a guide titled "Connect AMP for Endpoints in 3 Steps" provides instructions:

1. Log in to AMP for Endpoints and navigate to the API Credentials page located under Accounts
2. Click the New API Credential button. Enter Threat Response for Applications name and select a Scope. Selecting Read & Write will allow you to, for example, block a file hash in AMP for Endpoints from within Threat Response. Click the Create button.
3. The API Key Details page will appear. You will need the 3rd Party API Client ID and API Key values within Cisco Threat Response. API Key is irretrievable once you close the tab. Copy it to your clipboard or leave the tab open for the duration of the module configuration process.

注 : [URL] フィールドには、AMP for Endpoints インスタンス (NA、EU、APJC) の場所に
応じた URL を指定します。ここではデフォルトのままにしておきます。

4. 次に、[モジュール (Module)] ページで、新しく作成された AMP for Endpoints モジュールを確認します。このラボで他のモジュールを設定することはありません。ただし、[モジュール (Modules)] ページの [モジュールの設定方法 (How do I configure modules?)] と [API クライアント (API Clients)] ボタンをクリックすれば、他のモジュールの設定方法と Threat Response API に関する手順を確認できます。

5. AMP for Endpoints モジュールの設定を確認するには、前の演習でダウンロードしようとした **Zombies.pdf** ファイルのハッシュを含む簡単な調査を実施します。このファイルが Threat Response のターゲットとしてブロックされているすべてのエンドポイントを確認する必要があります。

00b32c3428362e39e4df2a0c3e0950947c147781fdd3d2ffd0bf5f96989bb002

The screenshot shows the Cisco Threat Response Investigate interface. At the top, there are tabs for 'Threat Response', 'Investigate', 'Snapshots', 'Intelligence', and 'Modules'. Below the tabs, there is a search bar with the hash '00b32c3428362e39e4df2a0c3e0950947c147781fdd3d2ffd0bf5f96989bb002'. Below the search bar, there are buttons for 'Investigate', 'Clear', and 'Reset'. The interface shows 3 Endpoints, 1 Observable, 1 Indicator, 0 Domains, and 1 File Hash. The endpoints list includes WIN-7-SALES, win-10-finance, and Win10-Marketing. The main view displays a network diagram with nodes for file paths and file names, such as 'File Path \\?(\C:\Users\...)' and 'File Name 90a09e4-5a01-...'.

演習 : Threat Grid



Threat Grid は、シスコのマルウェア分析および脅威インテリジェンス プラットフォームで、静的/動的サンプル分析と脅威インテリジェンスの生成/共有によってセキュリティを向上させます。完全に API 主導型の Threat Grid は、現在のセキュリティ インフラストラクチャを強化するように設計されています。そのため、シスコのセキュリティ ポートフォリオの大部分と統合され、サードパーティ製品も増え続けています。

手順

AMP for Endpoints と Threat Grid の統合を設定することで、Cisco Security 統合アカウントで両方のツールにログインできます（このラボでは対象外）。これにより、AMP for Endpoints のファイル分析結果の送信先（拡散度に基づいて送信されるか、手動で送信する）を Threat Grid Cloud ポータルにすることができます。

1. Google Chrome ブラウザに保存されている [Threat Grid] ブックマークをクリック後、[サインイン (Sign in)] をクリックしてログインします (**student/C1sco12345**)。
2. 右上隅のユーザ名をクリックし、[マイアカウント (My Account)] ページに移動します。ここで、[API キー (API Key)] の右側の小さなボタンをクリックして、Threat Grid API キーをコピーします。

API Key

*****  

Disable API Key

True

False

Unselected Copied!

- 次に、AMP for Endpoints Console を開き、[アカウント (Accounts)] → [ビジネス (Business)] に移動して、そのページの右上隅にある [編集 (Edit)] をクリック後、[Cisco Threat Grid API] セクションまで下にスクロールします。Threat Grid からコピーしたキーを [API キー (API Key)] フィールドに貼り付け、[保存 (Save)] をクリックします。

注：この設定をすることで、AMP for Endpoints から送信されたファイル分析結果を、Threat Grid Cloud アカウントで確認できるようになります。これにより、分析結果をさらに詳細に表示し、より深く脅威について研究/調査できます。

- 統合を確認するために、AMP for Endpoints Console から、Threat Grid にファイルを手動でアップロードしてみましょう。AMP for Endpoints Console で、[分析 (Analysis)] → [ファイル分析 (File Analysis)] に移動し、[ファイルの送信 (Submit File)] をクリックします。次に、**Downloads\Software Downloads** フォルダを参照してファイル (resume.docx) を選択し、[アップロード (Upload)] をクリックします。次に、Threat Grid に戻ってダッシュボードを開くと、最近送信されたファイルを [最近のサンプル (Recent Samples)] ビューで確認できます。ファイルは分析中です。

演習 : Cognitive Intelligence

Cognitive Intelligence (旧 Cognitive Threat Analytics) は、他のセキュリティ制御をバイパスしたり、監視されていないチャネル (リムーバブル メディアなど) から侵入したりして、組織の環境内で活発に動作している悪意のあるアクティビティを検出します。Cognitive Intelligence は、クラウドベースのサービスとして、ネットワークの機械学習機能と統計的モデリング機能を使用し、侵害されたエンドポイントと結びついた悪意のある C2 トラフィックを検出します。具体的には、Web トラフィックや NetFlow からユーザやデバイスのふるまいを分析し、コマンドアンドコントロール通信やデータ漏洩、インフラストラクチャで動作する望ましくないアプリケーションを検出します。また、Cognitive Intelligence のバックエンド アルゴリズムによって、バイナリ実行に関連するコマンド ラインの引数を調べたり、ファイルを送信先サーバと関連付けたりすることで、未知の悪意あるファイルの検出率が向上します。そのため、Cognitive Intelligence は、AMP for Endpoints の効果を高めるのに大きく貢献しており、可能な限り活用することがベスト プラクティスと考えられています。

手順

この演習では、AMP for Endpoints から Cognitive Intelligence を有効にし、Cisco Web セキュリティ アプライアンスをテレメトリ ソースとして設定します。

1. AMP for Endpoints Console で、[アカウント (Accounts)] → [ビジネス (Business)] に移動し、[編集 (Edit)] をクリック後、[Cognitive Threat Analytics] セクションまで下にスクロールします。
2. [有効化 (Enable)] をクリックしてから、[設定 (Configure)] をクリックします。最初のテレメトリ ソースを設定できるページにリダイレクトされます。[始める (Let's Get Started)] ボタンをクリック後、[SCP] をクリックし、最後に、適切な [デバイス名 (Device name)] を入力します (何でもかまいませんが、デバイスを特定できるものにします)。次のようなページになります。

DASHBOARD CONFIRMED DETECTED AMP for Endpoints

ADD DEVICE ACCOUNT

Success! Account created for this device. Use the following information to set up log subscription on WSAv-Boston-Branch-x23

SCP Host: SCP Port:

SCP Directory:

Device username:

and enter the SSH key provided by the device:

Once you enter the SSH key, you cannot change it. If you do not have the SSH key, you can enter it at a later time on the DEVICE ACCOUNTS page. Provisioning will not start until the SSH key is entered.

For details on configuring your device, see Configure WSA to Upload Log Files to CTA.

FINISH

注：このラボでは、Web ログ テレメトリ ソースとして Cisco Web セキュリティ アプライアンス (WSA) を設定します。ただし、Cognitive Intelligence は、HTTPS または SCP (McAfee、BlueCoat、Squid、ZScaler など) によって、適切な W3C 形式でログが提供される限り、テレメトリ ソースとしてサードパーティ ツールを活用することもできます。Stealthwatch Enterprise (NetFlow) は、Cognitive に対する最も一般的なテレメトリ ソースの 1 つです。

3. 次の設定ガイドを活用すれば、順を追って、WSA と Cognitive のペアリングを実施/検証できます：<http://cs.co/wsa-cognitive>

一般的なベスト プラクティス

このセクションでは、Cisco AMP for Endpoints を導入して運用する際に考慮すべき、その他の一般的なベスト プラクティスについて説明します。

演習：コネクタのアップデート

ポリシーとグループの作成に関してベスト プラクティスに従った場合、コネクタのアップデートは、スタッフの希望通りのきめ細かさで実行できる簡単なタスクです。対象とするエンドポイントの子グループを、現在の親グループのアップデート バージョンに移動するだけです。

ベスト プラクティス：あるバージョンのエンドポイント コネクタから別のバージョンにアップグレードした後、必ずエンドポイントをリブートします。コネクタのアップデート後にエンドポイントをリブートしないと、多くの場合、コネクタが正常に機能しなくなります。メンテナンスの時間帯に合わせてコネクタのアップデートを計画することをお勧めします。このベスト プラクティスは、将来変わる可能性があります。

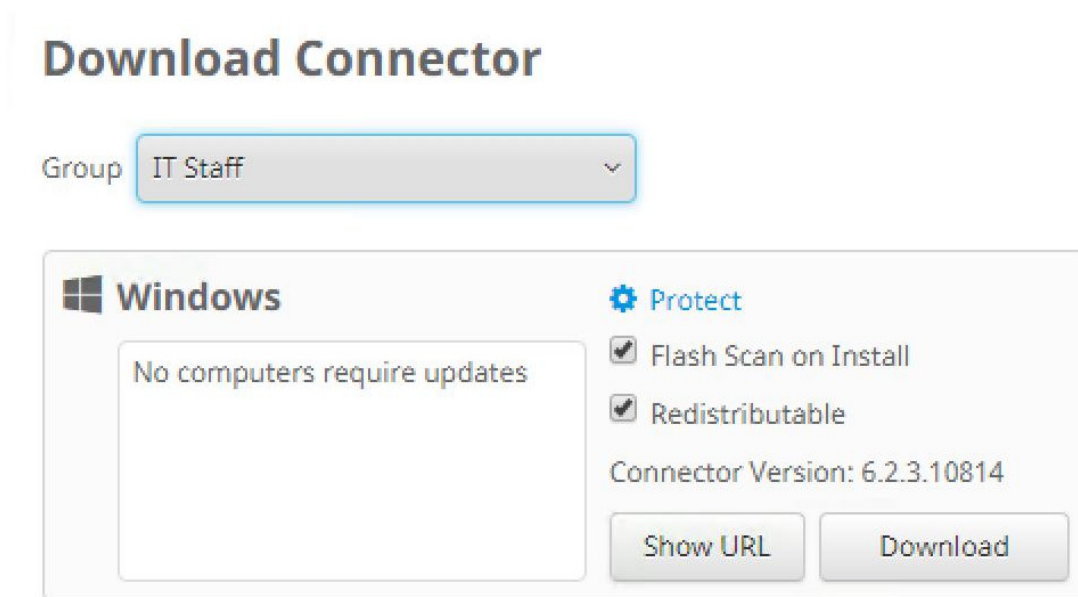
手順

この演習では、まず古いバージョンの AMP Connector を自分の **Student_Win** システムに導入してからアップデートします。この段階では、AMP for Endpoints Console を自分で操作するほうが簡単です。

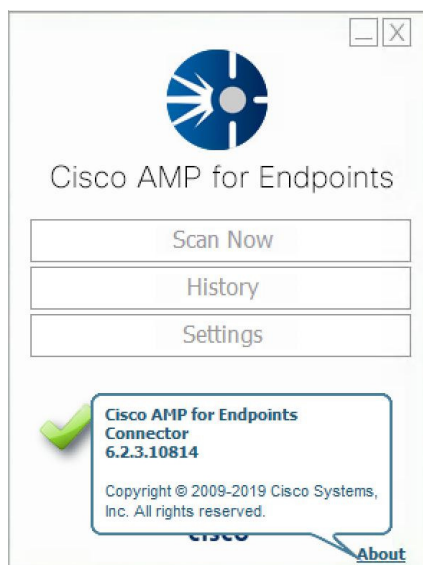
1. AMP for Endpoints Console で、**IT Staff** という名前の子グループを新たに作成し、[親グループ (Parent Group)] として、[保護アップデート親グループ (Protect Update Parent Group)] を選択します。このグループは、[保護-アップデート (Protect - Update)] Windows ポリシーの設定を継承します。[保存 (Save)] をクリックします。
2. Windows の [保護-アップデート (Protect - Update)] ポリシーの [製品アップデート (Product Update)] 設定を変更して、古い製品バージョン (6.2.3.10814 など) を活用します。[保存 (Save)] をクリックします。

注：製品バージョンの設定を変更すると、[管理 (Management)] → [コネクタのダウンロード (Download Connector)] ページから、AMP for Endpoints Connector の古いバージョンをダウンロードできます。

- 新しく作成された **IT Staff** グループ用の Windows AMP Connector をダウンロードします。



- Student_Win** システムに AMP for Endpoints ソフトウェアをインストールし、コンソールに正常に登録されていることを確認します。また、割り当てられたポリシー (**Protect – Update**) と、インストールされているバージョンを確認してください。バージョンは、AMP Connector の UI で [製品について (About)] にマウス ポインタを置くと表示されます。



5. 次に、ポリシー設定を再度変更して、コネクタがアップデートされるようにします。Windows の **Protect – Update** ポリシーの [製品アップデート (Product Update)] 設定を変更します。[製品バージョン (Product Version)] として [6.2.9.10881] (またはそれ以降) を選択します。今から少なくとも数時間先までの有効な [日付範囲 (Date Range)] を選択します。[更新間隔 (Update Interval)] の値は変更しないでください。[リブート (Reboot)] 設定を、[後で強制的にリブート (Force Reboot after...)] に変更し、[リブート延期時間 (Reboot Delay)] として [2分 (2 minutes)] を指定します。これで、エンドポイントがリブートするまでに 2 分間確保され、その間にユーザは作業を保存できます。[保存 (Save)] をクリック後、AMP Connector UI で [ポリシーの同期 (Sync policy)] をクリックすれば、ハートビートまで待たずに最新のポリシーを取得できます。指定した時間に基づいて、アップデート プロセスが開始されます。

Modes and Engines	Product Version	6.2.9.10881	Details
Exclusions 19 exclusion sets	Update Server	upgrades.amp.cisco.com	
Proxy	Date Range	2019-03-07 11:28 2019-03-07 20:47	
Outbreak Control	Update Interval	1 hour	
Product Updates	<input type="checkbox"/> Block Update if Reboot Required		
Advanced Settings	Reboot	Force reboot after...	
	Reboot Delay	2 minutes	

ベスト プラクティス : このラボ ガイドの執筆時点では、コネクタのアップデート後必ずエンドポイントをリブートして、保護が継続されるようにすることをお勧めします。このベスト プラクティスは将来変更され、リブートが不要になる可能性があります。

演習 : トラブルシューティング

AMP for Endpoints は、さまざまなスキャン エンジンおよびセキュリティ エンジンを備えた複雑な製品です。そのため、AMP for Endpoints Connector のトラブルシューティングは、製品の複雑さに精通していない人にとっては、非常に困難な作業となる場合があります。ただし、問題の大部分を解決できる、基本的なトラブルシューティング手順がいくつかあります。

接続テスト

多くの管理者が直面する標準的な問題の 1 つは、ファイアウォールとプロキシのルールセットが完全に実装されていることを検証することです。この問題のトラブルシューティングをサポートするために、AMP for Endpoints には、すべてのエンドポイントに Windows Connector をインストールする一環として、接続テスト用ツールが含まれています。ツールの実行は簡単で、実行結果から、エンドポイントが AMP for Endpoints クラウド インフラストラクチャに正しく接続できているかどうかをすぐに特定できます。

手順

この演習では、接続ツールを使用して、受講者のシステムでクイック接続テストを実施します。

1. **Student_Win** システムに接続し、AMP for Endpoints のローカル ディレクトリ (**C:\Program Files\Cisco\AMP\<バージョン番号>**) を参照します。
2. **ConnectivityTool.exe** を右クリックして [管理者として実行 (Run as administrator)] オプションを選択し、接続ツールを実行します。
3. 生成された **ConnectivityTool.exe.txt** ファイルを開き、一番下までスクロールします。サマリー データを確認すると、接続の問題があるかどうかわかります。接続ツールによって問題が検出された場合は、上にスクロールして、失敗した curl コールを特定すると、その問題がネットワーク内のどこで発生しているかを判断するのに役立ちます。

```
(181142635, +0 ms) Jan 27 03:32:45 [3456]: =====> [pass] Connectivity check completed with no issues
(181142635, +0 ms) Jan 27 03:32:45 [3456]: =====> Cur| code :           No error
(181142635, +0 ms) Jan 27 03:32:45 [3456]: =====> Cur| err  :           No error
(181142635, +0 ms) Jan 27 03:32:45 [3456]: =====> HTTP status:           200
(181142635, +0 ms) Jan 27 03:32:45 [3456]: ***** -END- *****
(181142635, +0 ms) Jan 27 03:32:45 [3456]: ***** SUMMARY *****
(181142635, +0 ms) Jan 27 03:32:45 [3456]: =====> * Completed successfully           6
(181142635, +0 ms) Jan 27 03:32:45 [3456]: =====> * Completed with issues             1
(181142635, +0 ms) Jan 27 03:32:45 [3456]: =====> * Failed checks                       0
(181142635, +0 ms) Jan 27 03:32:45 [3456]: =====> ** TOTAL CHECKS **                 7
(181142635, +0 ms) Jan 27 03:32:45 [3456]: ***** -DONE- *****
```

デバイストラジェクトリ テスト

場合によっては、コネクタが AMP for Endpoints クラウド インフラストラクチャと通信しているかどうか不明なことがあります。「イベント」を長期間レポートしないエンドポイントが存在する場合も多くあります。このような場合、管理者は、エンドポイントが正常に機能しているかどうかを疑問に思います。コネクタがバックエンドにデータをレポートしているかどうかをすばやく簡単に確認する方法の 1 つは、そのエンドポイントの [デバイストラジェクトリ (Device Trajectory)] ビューを開くことです。

手順

この演習では、デバイストラジェクトリを使用して、エンドポイントがクラウドにデータをレポートしているかどうかを確認します。

1. AMP for Endpoints Console (**studentXXX@sfsnort.com/@mp_Tr41n**) で、[管理 (Management)] -> [コンピュータ (Computers)] に移動し、[フィルタ (Filters)] を使用して対象のエンドポイントを特定します。エンドポイントが AMP Cloud と通信している場合、通常、[最後に確認 (Last Seen)] の値は、大きな指標となります。

注：この簡単な演習では、インストールされているエンドポイントのいずれかを選択します。

2. エンドポイント レコードを展開し、[デバイストラジェクトリ (Device Trajectory)] ボタンをクリックします。このシステムのプロセス、ファイル、ネットワーク イベントの履歴が表示されます。
3. エンドポイントが、直近数分間のデバイストラジェクトリ データを保持している場合、そのエンドポイントは正常にレポートし、イベントが検出された際に、イベント データが表示されます。また、**Zombies.pdf** テスト ファイルを該当のエンドポイントにダウンロードし、デバイストラジェクトリに表示されるかどうかを確認することも簡単にチェックできます。

不適切な除外リストのチェック

パフォーマンスの問題は、セキュリティ製品を実行する際に管理者が直面する一般的な問題の1つです。この問題は、通常、除外リストが不十分であることに起因しています。ただし、除外リストの形式が不適切なため、パフォーマンスのオーバーヘッドが大幅に拡大している場合もあります。このような除外リストを特定する方法の1つは、Github の Windows チューニング ツールを使用することです (コネクタ チューニング演習中にダウンロード済み)。このツールは、形式が不適切な除外リストを特定し、それによるパフォーマンス問題を解決するのに役立ちます。

手順

この演習では、Windows チューニング ツールを使用して、不適切な除外リストを確認します。

4. AMP for Endpoints Console の [管理 (Management)] → [コンピュータ (Computers)] ページで、レコードを展開して [診断 (Diagnose)] をクリックし、**Win-7-Sales** エンドポイントから診断サポート パッケージを要求します。
5. 診断パッケージがコンソールにアップロードされるまで待ち (7 ~ 10 分)、[分析 (Analysis)] → [ファイルリポジトリ (File Repository)] ページからダウンロードします。必ず、[タイプ (Type)] で [コネクタの診断 (Connector Diagnostics)] を選択し、**Win-7-Sales** エンドポイントから生成されたパッケージをダウンロードするようにしてください。

6. AMP for Endpoints Console から診断パッケージをダウンロードし、そのフォルダに他の古いパッケージがあれば削除します。同じフォルダに **Diag_analyzer_v1_02.exe** ツールがまだあることを確認します。
7. 最新の診断パッケージに対して **Diag_analyzer_v1_02.exe** ツールを実行します（今回は「y」を選択して、ポリシーからの除外対象を表示します）。新しく生成された **ampsupport%-summary** テキスト ファイルの結果を注意深く確認します。

チューニング ツールの結果と AMP for Endpoints Console の除外リストを評価する場合は、パフォーマンスの観点から除外リストを評価することも重要です。パフォーマンスに関する除外リスト チェックは、次の 2 つの部分から成ります。

1. 除外リストのタイプ（ワイルドカード、パス、プロセス、ファイル拡張子、脅威）は適切か。
2. 除外リストは適切な形式になっているか。
 - a. 脅威の除外：
 - i. W32.B76344BA43-95.SBX.TG
 - ii. W32.Auto:dfd99f89d2.in05.Talos
 - b. ファイルの拡張子：
 - i. .log
 - ii. .txt
 - iii. .db
 - c. ワイルドカードによる除外：
 - i. C:\Program Files\MyApplication*.log
 - ii. C:\Users*\MyApplication\
 - iii. C:\ProgramData*\MyApplication*.log

先頭がワイルドカードで始まる除外リストがある場合、ツールは次のような警告を生成します。

```
[WARNING] - Exclusions that start with * can lead to performance issues.
These should be converted to the Multi-drive exclusion type.
Please refer to CSCvm37634:
https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvm37634/?refering_site=dumpcr
.*\Program\ Files\ \(\x86\)\\SysTrack\\LsiAgent\\Condense\\. *\\. *\\.hld
.*\Program\ Files\ \(\x86\)\\SysTrack\\LsiAgent\\Condense\\. *\\. *\\. *\\.tmp
.*\System\ Volume\ Information\\tracking\.log
.*\Users\\. *\\AppData\\Local\\Temp\\. *\\-.*\\.tmp
.*\Users\\. *\\AppData\\Local\\Temp\\warsaw_.*
.*\Windows\\Security\\database\\. *\\.chk
.*\Windows\\Security\\database\\. *\\.edb
.*\Windows\\Security\\database\\. *\\.jrs
.*\Windows\\Security\\database\\. *\\.log
.*\Windows\\Security\\database\\. *\\.sdb
.*\Windows\\SoftwareDistribution\\Datastore\\Logs\\. *\\.log
.*\Windows\\SoftwareDistribution\\Datastore\\Logs\\edb.*\\.log
.*\Windows\\System32\\drivers\\. *\\-.*\\.tmp
.*\Windows\\Temp\\AltirisScript.*\\.cmd
.*\Windows\\Temp\\content\\.zip\\.tmp\\. *\\.diff
.*\Windows\\Temp\\content\\.zip\\.tmp\\cur\\.scr
.*\Windows\\Temp\\content\\.zip\\.tmp\\SymDeltaDecompressOptions\\.xml
.*\Windows\\Temp\\musdmys_.*
.*\Windows\\Temp\\TMP.*\\.tmp
.*\Windows\\Temp\\warsaw_.*
```


注：ワイルドカードで始まる除外リストは、パフォーマンスの問題を引き起こす可能性があります。そのような除外リストは形式を変え、CSIDL パスまたはドライブ文字を使用して先頭のワイルドカードを削除する必要があります。

どのような方法が使用されても、多くの場合、シンプルなチューニングではトラブルシューティングできない問題が発生します。そのような場合、問題が発生している間にエンドポイントからデバッグ診断データを取得し、Cisco TAC に送信するのが最適なアプローチです。そうすることで、発生した問題を特定して解決するまでの時間が大幅に短縮されます。

考慮事項：仮想デスクトップ インフラストラクチャ

AMP for Endpoints は、VDI ベンダーに依存しません。AMP for Endpoints は、仮想ホスト オペレーティング システムに依存せず、仮想環境で機能します。

AMP for Endpoints は、永続的 VM と非永続的 VM の両方に対応しています。

- 永続的な VM は、他のデスクトップやラップトップと同様に扱われます。永続的な VDI 環境では、導入ゴールド イメージを正しく作成することに注力する必要があります。
- 非永続 VM では、導入前に詳細設定とチューニングが必要です。

注：どちらの構成でも、AMP for Endpoints の ID 永続化機能にアクセスできる必要があります。この機能を有効にするには、Cisco TAC にケースをオープンし、機能の有効化を要求します。ID 永続化の概要：<http://cs.co/amp-id-persist>

ID 永続化により、AMP for Endpoints は、エンドポイント UUID をコンソール内の既存のコンピュータ レコードに適切にマッピングできるようになります。ID 永続化は、AMP for Endpoints ダッシュボードでコネクタ レコードが重複して作成されないようにするために使用されます。この機能は、履歴レコードの継続性を確保することで、エンドポイント コネクタ レコードの一貫性を維持するのにも役立ちます。さらに、1つのエンドポイントが複数のコネクタ ライセンスを使用することを防ぎます。コンソールに重複したレコードが表示される場合は、TAC ケースをオープンして解決を依頼します。TAC は、重複の原因を特定し、重複するレコードのクリーンアップをサポートします。

ベスト プラクティス：ID 永続化を使用する際に、すべてのポリシーで統一して使用すると、設定が統一されていない場合に、コネクタ レコードが重複して作成される可能性があります。ID 永続化を使用する際に推奨される設定は、[ビジネス全体でホスト名ごとに永続化 (By Hostname across Business)] です。

まとめ

このハンズオントレーニングの目的は、エンタープライズ環境で AMP for Endpoints ソフトウェアをインストールして設定するためのベスト プラクティスと導入方法をデモンストレーションすることでした。この目的は、情報収集、導入計画、コンソール セットアップ、アルファおよびベータ導入、全体導入、統合のセットアップなど、実際の環境での導入プロセスのほとんどすべての段階をシミュレーションした一連のハンズオン演習を通じて追求されました。また、反復サイクルが、インストールを成功させるための一部であることが実証されました。したがってシスコは、円滑な導入エクスペリエンスを実現するために、反復サイクルを活用することを強く推奨します。

ラボ演習では、インストールを成功させるためにお客様とパートナーが認識しておくべき多くの考慮事項があることも示されています。そのため、このトレーニングが、導入プロセスに着手して進めていくために必要な、基本的なガイドとなることを願っています。

付録 AMP for Endpoints の概要

この付録では、Cisco AMP for Endpoints ソリューションの概要、保護機能、導入使用例について記載します。

ソリューション概要

Cisco AMP for Endpoints は、クラウドマネージ型のエンドポイント セキュリティ ソリューションです。エントリ ポイントで攻撃を阻止する機能、エンドポイントに侵入した脅威を検出する機能、他の予防的セキュリティ レイヤを回避する高度な脅威に対応する機能が組み合わされています。エンドポイント システムのディスク上で発生するファイルおよびプロセスのアクティビティを継続的にモニタリングし、過去にさかのぼって分析します。これにより、マルウェアを遡及的に特定し、フォレンジック、脅威検出、インシデント対応機能を実行できます。

AMP for Endpoints は、サイバー チームによる日常業務を支援するために、強力なインシデント対応ワークフローを提供します。ダッシュボードの [受信トレイ (Inbox)] タブでは、環境内で注意が必要なエンドポイントをすばやく特定して、修復作業を開始できます。受信トレイは、チケット管理システムを完全に代替するものではありませんが、インシデントを簡単に管理できるように、ツールの機能がさらに強化されています。

The screenshot displays the Cisco AMP for Endpoints interface. At the top, there are status indicators: 25 Require Attention, 1 In Progress, and 2 Resolved. Below this is a navigation bar with buttons for 'Begin Work', 'Mark Resolved', and 'Move to Group...'. A 'Sort' dropdown is set to 'Severity'. The main content area shows a device profile for 'Demo_Qakbot_1' in the 'Triage' group, with 38 events. The profile includes fields for Hostname, Operating System (Windows 7, SP 1.0), Connector Version (5.1.11.10455), Install Date (2019-02-13 14:36:52 UTC), Connector GUID (76918664-24f5-4757-97f0-dc9ffe64560e), Group (Triage), Policy (Audit Policy), Internal IP (190.238.4.149), External IP (210.181.20.7), and Last Seen (2017-09-18 08:26:30 UTC). A pop-up window for 'W32.Qakbot.loc' shows a list of events with severity levels (Critical, High) and timestamps. A 'Vulnerabilities' section indicates 'No known software vulnerabilities observed'. At the bottom, there are buttons for 'Scan...', 'Move to Group...', 'Diagnose...', 'Begin Work', and 'Mark Resolved'.

デバイス トラジェクトリは、エンドポイントでのプロセスおよびファイルの実行履歴を表示する視覚的な機能です。これにより、環境内でのファイルのふるまいについて、優れたインサイトが得られます。たとえば、ファイルの実行方法や実行時期、ネットワーク接続の有無、接続している場合に他のファイルを導入したかどうかなどに関するものです。AMP for Endpoints は、Talos によって生成されたグローバル脅威インテリジェンス (正当、悪意がある、不明) に基づいて、ファイルに廃棄フラグを割り当てます。図の黄色の部分、注意が必要な、感染の侵害ポイントを示します。脅威がどのように導入されたかを説明するのに役立ちます。

Demo_Qakbot_1 in group Triage 38 compromise events (spanning 1 day)

Filters Search Device Trajectory



ファイルトラジェクトリには、ファイルに関する情報が表示されます。これにより、AMP for Endpoints 環境全体でファイルが確認された場所を把握できます。AMP for Endpoints を、Cisco E メールセキュリティ、Webセキュリティ、ネットワークセキュリティ (Firepower) デバイスとネイティブに統合することで、ファイルトラジェクトリは、これらのインスペクションポイントのいずれかを通過して転送中のファイルを、単一の統合ビューで表示することができます。そのため、1つのユーザインターフェイスから別のインターフェイスに移動するタイムラグがなくなり、セキュリティチームの効率が向上して、最も時間が必要なときに、時間を節約できます。

File Details

Known As		Attributes	
SHA-256	0a8eb4fd...fc9f7ece	Size	123 KB / 125,952 bytes
SHA-1	1593492457b1ec4e0aa6f7ce619927fa27df2eba	Type	PE Executable
MDS	d204193ae858f18f901ef2b004a01cd6	File Properties	
Detected As		Program	Microsoft® Windows® Operating System
Current Disposition Clean		Version	6.1.7601.23471
Known names		File Version	6.1.7601.23471
audiodg.exe		Copyright	© Microsoft Corporation. All rights reserved.

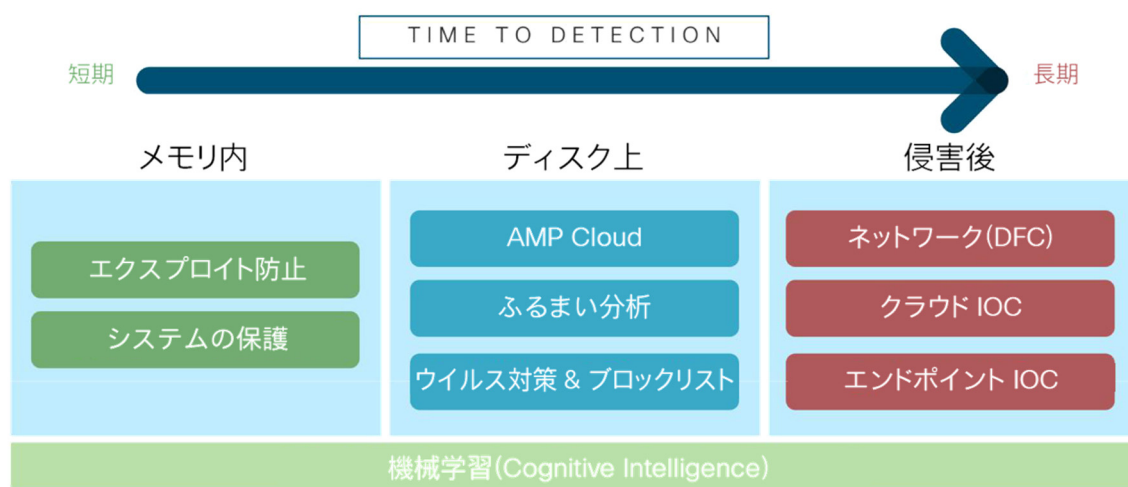
Network Profile

Trajectory

AMP for Endpoints は、Windows (デスクトップおよびサーバ)、Linux (RedHat および CentOS)、MacOS、Android、iOS など、さまざまなオペレーティングシステムをサポートしています (iOS 用の公式製品名は Clarity。Cisco Security Connector の一部)。

保護ラティス

Cisco AMP for Endpoints の保護機能は、さまざまなテクノロジーで構成されており、それらのテクノロジーが連携することで、エンドポイントで悪意のあるコードを防止、検出、修復することができます。次の図は、AMP for Endpoints Connector for Windows のセキュリティスタックについて説明したものです。



メモリ内の防御エンジンには、主に次のものがあります。

- **エクスプロイト防止**：保護されたプロセスのソフトウェア脆弱性を標的とした、難読化されたマルウェア、エクスプロイト、ポストエクスプロイト ツールで一般的に使用されるメモリ攻撃からエンドポイントを保護します。
- **システム保護 (システム プロセス保護エンジン)**：他の不正プロセスによるメモリインジェクション攻撃によって、重要な Windows システム プロセスが改ざんされたり、侵害されたりしないように保護します。

ディスク上の検出テクノロジーには、主に次のものがあります。

- **AMP Cloud**：グローバル脅威インテリジェンスを使用して、マルウェアをブロックします。脅威インテリジェンスは、Cisco Talos、Threat Grid、Cognitive Intelligence (機械学習) の調査によって、新たな脅威に対する知識が継続的に蓄積されています。
- **ふるまい分析 (Malicious Activity Protection エンジン)**：ランサムウェアに関連したふるまいなど、実行中のファイルまたはプロセスに関連する異常なふるまいをランタイムで検出してブロックします。
- **ウイルス対策とブロックリスト (TETRA for Windows およびカスタム検出)**：従来のシグニチャベースのウイルス対策エンジンとしてエンドポイントに存在し、ディスク上のマルウェアを検出する機能を備えています。カスタム検出は、カスタム シグニチャを定義し、業界標準形式のブラックリストを適用することで、セキュリティアナリストが強力な制御機能を使用できるようにすることを目的としています。

感染後の検出テクノロジーには、主に次のものがあります。

- **ネットワーク (DFC; デバイス フロー コリレーション)** : エンドポイント上のプロセス/ファイルの送受信ネットワーク通信を検査し、ポリシー (IP レピュテーションおよびカスタム IP ブロック リスト) に従って、アクションを制限できます。
- **クラウド IOC** : パターン認識により、エンドポイントで検出された不審なアクティビティを公開します。関連するアラートは、より詳細な調査と対応を促すトリガーとして機能します。
- **エンドポイント IOC** : 企業全体のエンドポイントをスキャンして侵害後の痕跡を得るための、強力な脅威検出機能です。スキャン用ファイルは、カスタムまたはシスコが作成したオープン IOC XML ファイルからインポートできます。

Cognitive Intelligence は、シスコの機械学習研究チームの取り組み (12 年以上の研究実績、80 人以上の機械学習データサイエンティスト/エンジニア、60 以上の取得済みおよび出願中特許、関連する 200 以上の出版物) により、AMP for Endpoints の効果をさらに向上させます。さらに、ネットワーク (Web ログ、Netflow) テレメトリの分析に基づいて、ファイルレスおよびエージェントレスで検出する機能も備えています。その分析結果は、特定の組織に最適化された、豊富なコンテキストに基づく、脅威に関する知識となります。また、複数の監視対象データセット (ネットワーク、エンドポイント、攻撃者モデル) にわたる脅威のふるまいとアクティビティの相関関係についてバックエンドのインテリジェンスも活用し、セキュリティの有効性レベルを向上させます。それに加え、他の専用モデルが AMP および Threat Grid 製品の内部に組み込まれて動作することで、機械学習ベースの静的ファイル分析が実現されます。

これらのセキュリティ機能は、広範囲に及ぶ高度なマルウェアを防御するための、全体的アプローチの基盤となります。シスコは、これらすべてのエンジンを相互に組み合わせて使用し、ソリューションの価値を最大限に活用することを推奨していますが、お客様は、ポリシーによって、どのエンジンを有効にするか無効にするかを選択できます。これらのテクノロジーは個別にリストされていますが、保護ラティスとして連携することで、可視性を向上させ、攻撃サイクル全体にわたって制御を強化できます。

オンラインおよびオフラインのエンジン

ほとんどのエンタープライズ環境にとって重要な考慮事項は、クラウド接続を常に確立して、継続的に保護するための要件です。AMP for Endpoints エンジンは、AMP Cloud 接続の有無にかかわらず、エンドポイントを保護します（エンジンによって異なります）。次の表は、エンジンを2つのグループに分類したものです。オンライン（脅威を検出して防御するために、AMP Cloud 接続を必要とするエンジン）とオフライン（セキュリティ関連の機能を実行して保護する際に、AMP Cloud 接続が不要なエンジン）の2グループです。

オンライン	オフライン
AMP Cloud	エクスプロイト防止
クラウド IOC	システム プロセス保護
エンドポイント IOC	Malicious Activity Protection
Threat Grid	ウイルス対策シグニチャ*
シンプル カスタム検出	拡張カスタム検出*

* 拡張カスタム検出/ウイルス対策シグニチャの初期導入には、AMP Cloud 接続が必要

使用例

Cisco AMP for Endpoints は、他のエンドポイント セキュリティ ソリューションと合わせてインストールすることも、スタンドアロン ツールとして活用することもできます。他の製品と合わせて導入する場合は、2つの製品を併用できることを確認し、パフォーマンスと互換性の問題が発生しないように、ベースライン設定とチューニングを正確に行うことを推奨します。

このハンズオン トレーニングの付録では、AMP for Endpoints の概要について説明していますが、<https://console.amp.cisco.com/docs> で入手できる公式の製品ドキュメントに代わるものではありません。