Cisco Eメールセキュリティにおける高度なマル ウェア防御(AMP)のベストプラクティスガイド

内容

<u>概要</u>

<u>機能キーの確認</u> 高度なマルウェア防御(AMP)の有効化 高度なマルウェア防御(AMP)グローバル設定のカスタマイズ ファイル分析のしきい値設定 ESAとAMP for Endpointsコンソールの統合 メールボックス自動修復(MAR)の有効化 メールポリシーの高度なマルウェア防御(AMP)の設定 SMAとCisco Threat Response(CTR)の統合 結論

概要

Advanced Malware Protection(AMP)は、マルウェアの検出とブロック、継続的な分析、およびレトロスペクティブアラートを可能にする包括的なソリューションです。Cisco EメールセキュリティでAMPを活用すると、高度なマルウェア防御に対する最もコスト効率の高い簡単なアプローチにより、攻撃前、攻撃中、攻撃後の一連の攻撃に対する優れた保護が可能になります。

このベストプラクティスドキュメントでは、次に示すように、Cisco Eメールセキュリティアプラ イアンス(ESA)のAMPの主な機能について説明します。

- ファイルレピュテーション:ESAを通過する各ファイルのフィンガープリントをキャプチャし、AMPのクラウドベースのインテリジェンスネットワークに送信してレピュテーション判定を行います。これらの結果から、悪意のあるファイルを自動的にブロックし、管理者定義のポリシーを適用できます。
- ファイル分析:ESAを通過する未知のファイルを分析する機能を提供します。安全性の高いサンドボックス環境により、AMPはファイルの動作に関する正確な詳細情報を取得し、そのデータを人間およびマシンの詳細な分析と組み合わせてファイルの脅威レベルを決定できます。この性質はAMPクラウドベースのインテリジェンスネットワークに取り込まれ、AMPクラウドデータセットを動的に更新および拡張して保護を強化するために使用されます。
- Mailbox Auto Remediation(MAR): Microsoft Office 365およびExchange 2013/2016の場合、最初のインスペクション後に悪意のあるファイルが含まれた電子メールの削除を自動化します。これにより、管理者の作業時間が節約され、脅威の影響を抑えることができます。
- Cisco AMP Unity:組織がAMP with AMPサブスクリプションを含むAMP対応デバイスをAMP for Endpointsコンソールに登録できるようにする機能です。このような統合により、AMP for Endpointsコンソールがすでにエンドポイントに提供しているのと同じ方法でCisco Eメール セキュリティを確認して照会し、単一のユーザインターフェイスですべての脅威ベクトルに ファイル伝搬データを関連付けることができます。
- Cisco Threat Response:シスコおよびサードパーティのソースからのセキュリティ関連情報 を1つの直感的な調査および応答コンソールにまとめるオーケストレーションプラットフォー

ムです。これは、イベントログと脅威インテリジェンスの統合フレームワークとして機能す るモジュラ設計によって実現されます。モジュールにより、関係グラフを作成してデータの 迅速な関連付けを可能にします。これにより、セキュリティチームは攻撃の明確なビューを 取得し、効果的な対応を迅速に行うことができます。

機能キーの確認

- ESAで、[System Administration] > [Feature Keys]に移動します
- ファイルレピュテーションおよびファイル分析の機能キーを探し、ステータスがアクティブ であることを確認します

高度なマルウェア防御(AMP)の有効化

- ESAで、[Security Services] > [Advanced Malware Protection File Reputation and Analysis]に移動します
- •[高度なマルウェア保護のグローバル設定]の[有効]ボタンをクリックします。

| Advanced Halware Protection | | |
|-----------------------------|----------------------|--|
| File Reputation: | Enabled | |
| File Analysis: | Enabled | |
| | Edit Global Settings | |

変更を保存します。

高度なマルウェア防御(AMP)グローバル設定のカスタマイズ

- AMPが有効になりました。[グローバル設定の編**集]をクリック**して、グローバル設定をカス タマイズします。
- ファイル拡張子の一覧は随時自動的に更新されるため、常にこの設定を参照し、すべてのファイル拡張子が選択されていることを確認してください。



- ファイルレピュテーションの詳細設定を展開する
- File Reputation Serverのデフォルト選択はAMERICA(cloud-sa.amp.cisco.com)です
- ・ドロップダウンメニューをクリックし、最も近いファイルレピュテーションサーバを選択します(特にAPJCおよびヨーロッパのお客様)。

| * Advanced Bettings for File Reputation | File Reputation Server | AMERICAS (cloud-outang clicit core) | 1 |
|---|---|--|------------------|
| | AMP for Endpoints Conside Integration $\langle\Xi\rangle$ | AMERICALISTICAL PROVIDENCE AND A PROVIDA PROVIDENCE AND A PROVIDENCE AND A PROVIDENCE AND A | eresc @ Sweeping |
| | 55, Connunitation for file Reputation. | APUC (closh-sagic amp-data por) Prode equivalent dad Turnel Press (bptonel) Server: Vasname Paughtass Patyst Paughtase Patyst Patyst Patyst Patyst Paughtase Patyst Pat | he _ |
| | Pearliest Interval | The contraction of the second | |
| | Query Timesut | d seconds | |
| | Processing Timesus: | LT MORE | |
| | File Reputation Client 30: | be79abd0-4463-4453-668a-73a3912a0434 | |
| | Pile Ratraspective: | Suppress the vertilet update alorts (8) | |

- ファイル分析の詳細設定を展開する
- File Analysis Server URLのデフォルト選択はAMERICAS(<u>https://panacea.threatgrid.com</u>)です
- ・ドロップダウンメニューをクリックし、最も近いファイルレピュテーションサーバ(特にヨーロッパのお客様)を選択します。

| * Advanced Settings for Rie Analysis | File Analysis Server URL: | 2 AMERICAS (Inter-Strengton Principal com) | 9 |
|--------------------------------------|-----------------------------|--|-----------------------------|
| | File Analysis Chart 32: | Private analysis stread | F-#0577168/801_C100W_000080 |
| Cache Settings | Advanced settings for Cache | | |

ファイル分析のしきい値設定

(オプション)ファイル分析スコアの上限しきい値を設定できます。しきい値設定に基づいてブ ロックされたファイルは、高度なマルウェア防御レポートの[着信マルウェア脅威ファイル (Incoming Malware Threat Files)]セクションに[カスタムしきい値(Custom Threshold)]として表示 されます。

Ditar Custern Value: 50

- AMPグローバル設定ページで、[Threshold Settings]を展開します。
- ・クラウドサービスのデフォルト値は95です。
- •[カスタム値の入力]のラジオボタンを選択し、値を変更します(例:70)。

• [送信]をク**リックし、[変更を**確定]をクリックします

ESAとAMP for Endpointsコンソールの統合

(エンドポイント向けAMPの場合のみ)ユニファイドカスタムファイルブロックリスト(または ファイルAllowlist)は、AMP for Endpointsコンソールを使用して作成でき、ESAを含むセキュリ ティアーキテクチャ全体に格納戦略をシームレスに配布できます。

- •AMPグローバル設定ページで、[ファイルレピュテーションの詳細設定]を展開します
- [Register Appliance with AMP for Endpoints]ボタンをクリックします。

ANP for Endpoints Conside 21 Big Visite 8 Support Appliance with Well for Endpoints.

- [**OK**]をクリックして、AMP for Endpointsコンソールサイトにリダイレクトし、登録を完了します。
- ユーザクレデンシャルを使用してAMP for Endpointsコンソールにログインします
- [Allow authorization the ESA registration:



- AMP for Endpointsコンソールは、ページを自動的にESAにピボットします。
- ・登録ステータスが[SUCCESS]と表示されていることを確認します。

AHP for Endpoints Console Entegration 🛞 VLNESA000181_564D58189584A76C416D-4F8AA6579018 🖲 Deregister 🗸 SUCCESS

• [Submit]をクリックし、[Commit your changes]をクリックします

メールボックス自動修復(MAR)の有効化

O365メールボックスまたはMicrosoft Exchange 2013/2016のメールボックス自動修復(MAR)機能 を使用すると、ファイルレピュテーションの判定がClean/UnknownからMaliciousに変更されたと きにアクションを実行できます。

- •[システム管理] > [アカウント設定]に移動します
- [アカウントプロファ**イル]で[アカウントプロファイルの作成]をクリック**し、Office 365または Microsoft Exchangeのメールボックスを使用してAPI接続プロファイルを作成します。

| Account Profiles 😨 | | | |
|------------------------|---------------------|-------------|--------|
| Create Account Profile | | | |
| Account Profile Name | Profile Type | Description | Delete |
| exchange | Exchange On Premise | | 8 |

- [Submit]をクリックし、[Commit your changes]をクリックします
- (オプション)チェーンプロファイルはプロファイルの集合であり、チェーンされたプロファイルにアクセスするアカウントが展開の異なるテナント間に存在する場合にのみ設定します。
- [ドメインマッピング**の作成]ボタンをクリ**ックして、アカウントプロファイルを受信者ドメイ ンにマッピングします。推奨される設定を次に示します。

| Domain Mapping 🔮 | | |
|---|---------------------|--------|
| Domain Mapping configuration is not available since all profiles are already mapped | | |
| Mailbox Profile/Chained Profile | Recipient Domain(s) | Delete |
| exchange | domein.com | |

• [Submit]をクリックし、[Commit your changes]をクリックします

メールポリシーの高度なマルウェア防御(AMP)の設定

AMPとMARがグローバルに設定されたら、サービスをメールポリシーに対して有効にできます。

- [メールポリシー(Mail Policies)] > [着信メールポリシー(Incoming Mail Policies)]に移動します
- 受信メールポ**リシーの高度なマルウェ**ア保護の設定をカスタマイズするには、カスタマイズ するポリシーの[高度なマルウェ**ア保護]の下の青いリンクをクリック**します。

• このベストプラクティスのドキュメントでは、[ファイルレピュテーションを有効にする]の横 にあるラジオボタンをクリックし、[ファイル分析を有効にする]を選択します。

| Advanced Malware Protection Settings | |
|--|--|
| Policy: | DEFAULT |
| Enable Advanced Malware Protection for This Policy: | Enable File Reputation Enable File Analysis No |

- •AMPの結果をメッセージにするXヘッダーを含めることをお勧めします。
- 次の3つのセクションでは、メッセージエラー、レート制限、またはAMPサービスが使用できない場合に、添付ファイルがスキャン不能と見なされる場合にESAが実行する必要があるアクションを選択できます。推奨されるアクションは、メッセージの件名に警告テキストが付加された状態で現状のまま配信することです。

| Unscannable Actions on Message Errors | | | |
|---|---------------------------------------|--------------------------------|--|
| Action Applied to Message: | Deliver As Is 🔻 | | |
| | Archive Original Message: | No Ves | |
| | Modify Message Subject: | No Prepend Append | |
| | | [WARNING: ATTACHMENT UNSCANNED | |
| | Add Custom Header to Message: | No Yes | |
| | | Header: | |
| | | Value: | |
| | Modify Message Recipient: | No Yes | |
| | | Address: | |
| | Send Message to Alternate Destination | No Yes | |
| | HOSE. | Host: | |
| Unscannable Actions on Rate Limit | | | |
| Action Applied to Message: | Deliver As Is 🔻 | | |
| | Archive Original Message: | No Yes | |
| | Modify Message Subject: | No Prepend Append | |
| | | [WARNING: ATTACHMENT UNSCANNED | |
| | Add Custom Header to Message: | No Yes | |
| | | Header: | |
| | | Value: | |
| | Modify Message Recipient: | No Yes | |
| | | Address: | |
| | Send Message to Alternate Destination | No Yes | |
| | | Host: | |
| Unscannable Actions on AMP Service Not Av | ailable | | |
| Action Applied to Message: | Deliver As Is 🔻 | | |
| | Archive Original Message: | No Yes | |
| | Modify Message Subject: | No Prepend Append | |
| | | [WARNING: ATTACHMENT UNSCANNED | |
| | Add Custom Header to Message: | No Yes | |
| | | Header: | |
| | | Value: | |
| | Modify Message Recipient: | No Yes | |
| | | Address: | |
| | Send Message to Alternate Destination | No Yes | |
| | | Host: | |

次のセクションでは、添付ファイルが悪意があると考えられる場合にメッセージをドロップ

するようにESAを設定します。

| Messages with Halware Attachments: | |
|------------------------------------|-----------------------------|
| Action Applied to Message: | Drop Hessage * |
| Archive Original Message: | 0 No 🖲 Yes |
| Drop Malware Attachments: | # No U Yes |
| Hodity Message Subject: | No * Prepend Append |
| | (WARNING: MALWARE DETICTED) |
| > Advanced | Optional sattings. |

ファイル分析のために添付ファイルが送信された場合は、メッセージを検疫することをお勧めします。

| Hessages with File Analysis Pending: | | |
|--------------------------------------|------------------------------------|--|
| Action Applied to Message: | Quarantine * | |
| Archive Original Message: | © No # Yes | |
| Nodify Message Subject: | © No ® Prepard © Appand | |
| | WAANING: ATTACHMENT(S) HAY CONTAIN | |
| E Advanced | Öptional settings. | |

(受信メールポリシーのみ)脅威の判定が悪意に対して変化した場合に、エンドユーザに配信されるメッセージに対して実行される修復アクションを構成します。推奨される設定を次に示します。

| Enable Mailbox Auto Remediation (MAR) | |
|--|--|
| Mailbox Auto Remediation Actions apply only if Acc | ount Settings are configured. See System Administration > Account Settings . |
| Action to be taken on message(s) in user's mailbox: | Forward to: |
| | * Oeiete |
| | Forward to: and Delete |

• [Submit]をクリックし、[Commit your changes]をクリックします

SMAとCisco Threat Response(CTR)の統合

SMA Eメールモジュールを統合するには、CTR経由でセキュリティサービス交換(SSE)を使用す る必要があります。SSEを使用すると、SMAをExchangeに登録でき、登録されたデバイスにア クセスするためのCisco Threat Responseの明示的な権限を付与できます。このプロセスでは、 SMAをリンクする準備ができたときに生成されるトークンを介してSSEにリンクします。

- CTRポータル(<u>https://visibility.amp.cisco.com</u>)で、ユーザクレデンシャルを使用してログイン します。
- CTRはモジュールを使用して、ESAを含む他のシスコセキュリティ製品と統合します。[モジ ュール]タブ**をクリック**します。
- [Devices]を選択し、[Manage Devices]をクリックします。

| Threat Response | Investigate | Snapshots | Incidents Beta | Intelligence | Modules |
|--------------------|-------------|-------------|----------------|--------------|---------|
| Settings > Devices | | | | | |
| Settings | Dev | ices | | | |
| Your Account | | | | | |
| Devices | Man | age Devices | Reload Devic | 201 | |
| API Clients | IVIAI | age Devices | I Reioad Devic | | |

- CTRはページをSSEにピボットします。
- +アイコンをクリックして、新しいトークンを生成し、[続行]をクリックします。
 ボックスを閉じる前に、新しいトークンをコピーします。

| Add Devices and Generate Tokens | | |
|---|---|--|
| The following tokens have been generated and will be valid for 1 hour(s): | | |
| Tokens | | |
| 0ac7c30df02c0abfbe4869b8085445c8 | | |
| | | |
| Close Copy to Clipboard Save To Fi | е | |
| | | |

- SMAで、[Management Appliances]タブ> [**Network**] > [**Cloud Service Settings**]に移動します
- [Edit Setting]**をクリック**し、[Threat Response]オプションが[**Enable**]であることを確認**します**。
- Threat Response Server(THREAT)のURLはAMERICAS(api-sse.cisco.com)で、ヨーロッパの お客様の場合は、ドロップダウンメニューをクリックし、
 FUROPE(api eu sse itd cisco.com)を選択します。

| Cloud Service Settings | | | | | | |
|-------------------------|------------------------------------|--------|--|--|--|--|
| Edit Cloud Services | | | | | | |
| Threat Response: | i € Enable | | | | | |
| Threat Response Server: | AMERICAS (api-see.cisco.com) | | | | | |
| Cancel | EUROPE (api eu sie ital circo.com) | Submit | | | | |

- [Submit]をクリックし、[Commit your changes]をクリックします
- Cloud Services Settingにトークンキー(CTRポータルから生成したキー)を貼り付け、 [Register]をクリッ**クします**。

| Registration Token: (3) | Dec7c30dF02x0e3Fbe486918085445c8 | Register |
|-------------------------|----------------------------------|----------|
| | | |

- •登録プロセスが完了するまでに時間がかかります。数分後にこのページに戻り、ステータス を再度確認してください。
- [CTR] > [Modules] > [Device] に戻り、[Reload Device] ボタンをクリックしてSMAがリストに

表示されることを確認します。

| Cisco Threat Response | Investigate Snapshots Incide | nts Beta Intelligen | ice Modules | | | (?) 🔅 | | |
|-----------------------|------------------------------|---------------------|-------------|-------------|----|------------|--|--|
| Settings > Devices | _ | | | | | | | |
| Settings | Devices | | | | | | | |
| Your Account | | | | | | | | |
| Devices | Manage Devices Re | load Devices | | | | | | |
| API Clients | halage vertes | | | | | | | |
| > Modules | Name | Туре | Version | Description | ID | IP Address | | |
| Users | sma1 | SMA | 13.0.0-187 | SMA | 1 | 127.0.0.1 | | |

結論

このドキュメントでは、Eメールセキュリティアプライアンス(ESA)でのCisco Advanced Malware Protection(AMP)のデフォルト設定またはベストプラクティス設定について説明します。 これらの設定のほとんどは、着信および発信の電子メールポリシーの両方で使用でき、設定とフ ィルタリングは両方向で推奨されます。