フォーマット済みおよび未フォーマットの社会保障番号を検出するカスタム DLP ポリシーの設定

目次

概要

この資料に検出するためにカスタム DLP ポリシーを設定する方法を Cisco E メール セキュリティ アプライアンス（ESA）のフォーマットされた不定様式社会保障番号（SSN）記述されています。

フォーマット済みおよび未フォーマットの社会保障番号を検出するカスタム DLP ポリシーの設定

意図的に DLP スキャン エンジンはフォーマットされていた社会保障番号だけを検出します。 これはさまざまな企業が使用するデータに含まれている 9 ディジット数引き起こされる false positive の高レベルが原因です。 たとえば不定様式社会保障番号のためにスキャンするとき、数をルーティングするバンク ABA は 9 ディジットで、誘発します。 組織によって厳しく必要とされてそのように不定様式社会保障番号のためにスキャンすることを避けることを推奨しません。 組織は不定様式社会保障番号のためにスキャンすることが必要となれば、下記のソリューションで提供されるステップに従うことによってカスタム DLP ポリシーを作成できます。

AsyncOS は RSA か組織によって発達する分類子を使用してあなた自身のポリシーを全く最初から作成するためにオプションを提供します。 このオプションはあらかじめ定義されたポリシー テンプレートがネットワーク環境の固有の要求を満たさないとき高度と検討され、稀なケースでだけ使用する必要があります。

カスタム ポリシーを作成して下さい

1. GUI を使用する場合： **メール ポリシー > DLP Policy Manager**。
2. **追加 DLP ポリシー...**ボタンをクリックして下さい。
3. **ポリシーを**スクリーンの一番下で『Custom』 を選択 し、カスタム ポリシー**の隣で『Add』をクリック して下さい。**
4. DLP ポリシー名を入力して下さい。 次に、例を示します。 *SSN カスタム ポリシー*。

分類子を作成して下さい

カスタム分類子を作成することは DLP エンジンのスキャンされた基準上の大きなフレキシビリティを与えます。 長所にフォーマットされていた SSN および不定様式 SSN 両方のためにスキャンするのにこれを使用します。

1. ドロップダウン コンテンツ一致する分類子から**分類子を**『Create』 を選択 し、**Add ボタンを**クリックして下さい。
2. コンテンツ一致する分類子名前を入力して下さい。 次に、例を示します。 *SSN すべての形式*。
3. ルール セクションの下で、ワードまたは句から**エンティティ**にドロップするを設定して下さい。
4. エンティティを選択して下さい: **フォーマットされている米国社会保障番号**。
5. [Add Rule] をクリックします。
6. 再度**エンティティを**選択して下さい。
7. エンティティを選択して下さい: **不定様式米国社会保障番号**。
8. [Submit] をクリックします。

重大度設定を行って下さい

次の設定はただ助けるガイドラインで、組織必要に基づいていくつかの口径測定または代替コンフィギュレーション設定を必要とするかもしれないどんなに、よい開始点です。

- **重要な重大度設定**
  メッセージに適用される操作: **検疫**
  イネーブル暗号化 (チェックされる)
  暗号化のルール: **メッセージの暗号化を常に使用して下さい**
  暗号化プロファイル (ドロップダウンから設定された暗号化プロファイルを選択して下さい)
  暗号化 された メッセージ サブジェクト: **$subject**
- **高い重大度設定**
  メッセージに適用される操作: **渡して下さい**
  暗号化を有効に して下さい (チェックされる)
  暗号化のルール: **メッセージの暗号化を常に使用して下さい**
  暗号化プロファイル (ドロップダウンから設定された暗号化プロファイルを選択して下さい)
  暗号化 された メッセージ サブジェクト: **$subject**
- **中間重大度設定**
  メッセージに適用される操作: *渡して下さい*
  暗号化を有効に して下さい (チェックされる)
  暗号化のルール: **TLS が失敗した場合その時だけメッセージの暗号化を使用して下さい**

暗号化プロファイル (ドロップダウンから設定された暗号化プロファイルを選択して下さい)
暗号化 された メッセージ サブジェクト: **$subject**

- **低い重大度設定**
  メッセージに適用される操作: **渡して下さい**
  暗号化を有効に して下さい (チェックを外される)

重大度スケールを設定して下さい

再度、次の設定はただ助けるガイドラインで、組織必要に基づいていくつかの口径測定または代替コンフィギュレーション設定を必要とするかもしれないどんなに、よい開始点です。

1. 重大度スケール ダイアグラムの右へ、**スケールを**『Edit』 をクリック して下さい。
2. 無視までの最初のハンドルを = 0 滑らせます。
3. 第 2 ハンドルをまでの LOW = 1 から 9.滑らせます。
4. メディアまでの第 3 ハンドルを = 10 から 50 滑らせます。
5. 最高までの第 4 ハンドルを = 60 から 89 滑らせます。
6. これを正しく設定する場合、自動的に 90 から 100 設定されます重要。
7. 終了したら『Done』 をクリック して下さい。

変更を送信して確定します。

このポリシーの作成を確定するために、**SUBMIT ボタンを**クリックして下さい。 GUI の右上隅の**託変更**ボタンをクリックして下さい。 コミットされていない変更画面に、クリックします**保存します変更を**連れて行かれます。 成功すれば**保留中の** GUI の右上隅の**変更を**見るはずです。

最後の段階

今**メール Policies->Outgoing メール ポリシー**の下で発信メール ポリシーの DLP ポリシーを有効に する必要があります。 あなた自身でカスタム発信ポリシーを作成できる本番の外のテストのために送信側として指定し、このテスト ポリシーの DLP ポリシーを有効に します。

関連情報

- Cisco 電子メール セキュリティ アプライアンス - エンド ユーザ ガイド
- テクニカル サポートとドキュメント – Cisco Systems