目次

概要

この資料はいくつかの E メール セキュリティ アプライアンス (ESA) の発生フィルター、またはウイルス発生フィルターに関するより多くの FAQ を、記述し、回答したものです。

発生フィルターとは何、またはウイルス発生はフィルタリングします (VOF) か。

発生するので、発生フィルター ネットワークをおよびより小さい phishing 詐欺および malware ディストリビューションのような大規模 な ウイルス発生から、非ウイルス攻撃します、保護します。 データが収集されるソフトウェア アップデートが送達されるまで新しい発生を検出することができないほとんどの反malware security software とは違って、発生の Cisco 収集データはリアルタイムの ESA にこれらのメッセージがユーザに達することを防ぐために広がる更新された情報を送信 し、と同時に。

Cisco は着信メッセージは発生の安全または一部だったかどうか確認するルールを開発するのにグローバル トラフィック トラフィック パターンを使用します。 発生の一部であるかもしれないメッセージは Sophos および McAfee によって Cisco からの更新済発生情報に基づくセーフまたは新しいアンチウィルス 定義になるために判別されるまで送達されます検疫されます。

オンライン短い間ただ、Web セキュリティ サービスに不明である phishing および malware Webサイトを指す小規模の、非ウイルス不正侵入で使用されるメッセージは正規の検知 設計、受信者の情報およびカスタム URL を使用します。 発生フィルターはメッセージの内容を分析し、URL リンクを非ウイルス攻撃のこの型を検出するために捜します。 発生フィルターはどちらかアクセスするように試みている Webサイトが悪意のあるかもしれない警告したりまたは Webサイトを完全にブロックするユーザに Web セキュリティ プロキシによって有害性がある Webサイトにトラフィックをリダイレクトするために URL を書き換えることができます。

ESA でアンチウィルス Sophos か McAfee を実行しなくても発

生フィルターを使用できますか。

Cisco はウイルスに対する防御を高めることをウイルス発生フィルターに加えてアンチウィルス Sophos か McAfee が可能にすることを推奨します。 ただし、VOF はアンチウィルス Sophos か McAfee が有効に なるように要求しないで独自に動作できます。

発生フィルターはいつメッセージを検疫しますか。

メッセージはファイルの添付が含まれているとき検疫されます現在の発生ルールおよびしきい値によって設定 される 管理者にメールで会うか、または超過する。 Cisco は有効なフィーチャーキーがある、およびサポート ポータルで現在の発生ルールを送達します各 ESA に。

現在のウイルス発生についての情報は SenderBase で見つけることができます

Ciscoセキュリティ情報収集活動（SIO）Webサイトは現在の非ウイルス脅威のリストを、スパムを含んで提供し、phishing、malware ディストリビューションは試みます。

発生検疫がいっぱいになると何が起こりますか。

検疫がそれに割り当てられる最大領域を超過するときまたはメッセージが最大時間設定を超過すればそれを適度に保存するために、メッセージは検疫から自動的にプルーニングされます。 メッセージは First In First Out（FIFO; 先入れ先出し）基礎で削除されます。 すなわち、以前のメッセージは最初に削除されます。 リリースに検疫を（すなわち、渡せば）設定する検疫からプルーニングする必要があるメッセージを削除できます。 RELEASE メッセージに選択する場合メッセージは検疫から強制だったこと受信者に警告する規定 するテキストとタグ付けされる件名があるために、選ぶことができます。

発生検疫からの続くリリースはアンチウィルス モジュールによって、メッセージ再スキャンし、処置はアンチウィルス ポリシーに従ってとられます。 このポリシーによっては、メッセージは除去されるウイルス添付ファイルによって提供されるか、削除されるか、または提供されるかもしれません。 ウイルスが頻繁に発生検疫からのリリースの後で再スキャンの間に見つけられることが期待されます。 ESA mail_logs かメッセージ トラッキングは参照することができであるとウイルスそれどのように渡されたか注意された検疫で個々のメッセージ見つけられたかどうか確認するために、そして。

システム検疫がいっぱいになる前に、アラートは完全な 95% に達するとき検疫が完全な 75% に達する別のアラートは発信されますとき発信され。 発生検疫に水平な点ウイルス 脅威を一致するすべてのメッセージを削除するか、または発表することを可能にする追加管理機能があります（VTL）。 これは点ウイルスに脅威を当たる検疫の容易な消去をアンチウィルス アップデートが受信された後可能にします。

発生ルールの水平な脅威の意味とは何か。

発生フィルターは 0 と 5.間の脅威 レベルの下で機能します。 水平な脅威はウイルス発生の確率

を評価します。 ウイルス発生のリスクに基づいて、水平な脅威は疑わしいファイルの検疫に影響を及ぼします。 水平な脅威はアンチウィルス ベンダーからのネットワークトラフィック、疑わしい ファイル アクティビティ、入力、および Cisco の脅威 オペレーション センターによって分析を含むがそれに限定されずいくつかのファクタに、基づいています。 さらに、発生フィルター割り当てはネットワークのために脅威 レベルの影響を高めるか、または減少させるために管理者を郵送します。

レベル	リスク	意味
0	なし	メッセージが脅威であることリスクがありません。
1	低	メッセージが脅威であることリスクは低いです。
2	下位/メディア	メッセージが脅威であることリスクはメディアに低いです。 それは a ですか。疑
3	中間	メッセージは確認された発生の一部ですまたは脅威があるコンテンツの大きなリス
4	高	メッセージは大規模発生の一部であるために確認されますまたはコンテンツは非常
5	極度	メッセージか。s コンテンツは膨大なスケールか大規模および非常に危ないである。

ウイルス発生が発生するときどのように警告することができますか。

SenderBase ネットワークがメッセージ プロファイルの特定の種類のための VTL を上げるとき、設定されたアラート eメールアドレスに送信 される 電子メール メッセージによって警告することができます。 VTL が設定された閾値の下で下るとき、別のアラートは発信されます。 こうしてウイルスの進行状況を監視できます。 確認することはアラートが **alertconfig** コマンドを使用して CLI でに発信されることこれらのアラートを、確認します eメールアドレスを受け取ります。

設定するため、または reivew confirugation

- GUI： セキュリティ サービス > 発生フィルターは**編集グローバル な 設定**の下でおよび検討します設定を…
- CLI： **outbreakconfig > 設定される**

前。

新しいウイルス発生は SenderBase によって最初に検出する、VTL は高いです。 VTL が設定された VTL しきい値に会うか、または超過すればアラートを受け取ります。 Sophos アラートはウイルスがように、そしてシグニチャを識別している新しいウイルスがなる利用可能に識別され、キャプチャ される場合続きます。

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