実行可能ファイルを含む埋め込みハイパーリンクをどのようにキャプチャおよびブロックできますか。

目次

質問

実行可能ファイルを含む埋め込みハイパーリンクをどのようにキャプチャおよびブロックできますか。

回答

本文および HTML 添付ファイルをスキャンするのにメッセージ フィルターを使用できます。 通常、これらのメールは HTML メールで入ります。 それを検出するスキャン エンジンのために本文含んでいます状態を使用して下さい。 送信メールだけを処理する場合、ただ本文含んでいます」状態を「使用できます。

次のメッセージ フィルタはその長さ ハイパーリンクを実行可能モジュールの端探します。 条件が満たされれば、2 つの操作はアクティブになります。 最初の操作は admin@example.com へメールを送信 することによって口ーカルな システム管理者を知らせることです。

第 2 はメールの廃棄の最終措置です。 メールはドロップするである必要はありませんでしたり代りに検疫することができます。 `drop()` の下記の操作を取除きます; 」「取り替えるの操作とことができます;

検疫は定義する必要があります他ではフィルタ エンジンはフィルタを可能にしません。 デフォルトポリシー検疫を使用できますまたはあなた自身の検疫を作成して下さい (検疫を作成するか、または削除するために手動の検疫を参照して下さい) 。

```
Block_exe_urls: if body-contains("://\\S*\\.exe(\\s|\\b|$)")
{
notify ("admin@example.com");
drop();
}
```

また悪い URL を本文からおよび取り替えられた取除かれた URL とそれら取除いたこのバージョンを使用できます。

```
remove_exe_urls: if body-contains("://\\S*\\.exe(\\s|\\b|$)")
{
edit-body-text("://\\S*\\.exe(\\s|\\b|$)", "URL REMOVED");
}
```

メッセージ フィルターを入力する方法に関する詳細説明に関しては Cisco IronPort アプライアンスに新しいメッセージ フィルターをどのように追加するか検討しなさいかか。

メッセージ フィルターを検討するために E メール セキュリティ アプライアンス セクションによって呼出されるポリシー施行のための Cisco ESA AsyncOS アドバンスド ユーザー ユーザーズ ガイドを参照して下さい。