



RSA | Security Analytics

RSA ECATとの統合ガイド
バージョン 10.6

商標

RSA、RSAロゴ、およびEMCは、EMC Corporationの米国およびその他の国における登録商標または商標です。その他のすべての名称ならびに製品についての商標は、それぞれの所有者の商標または登録商標です。EMCの商標のリストについては、japan.emc.com/legal/emc-corporation-trademarks.htmを参照してください。

使用許諾契約

本ソフトウェアと関連ドキュメントは、EMCが著作権を保有しており、使用許諾契約に従って提供されます。本ソフトウェアと関連ドキュメントの使用と複製は、使用許諾契約の条項に従い、上記の著作権を侵害しない場合のみ許諾されます。本ソフトウェアと関連ドキュメント、およびその複製物を他人に提供することは一切認められません。

本使用許諾契約によって、本ソフトウェアと関連ドキュメントの所有権およびその他の知的財産権が譲渡されることはありません。本ソフトウェアと関連ドキュメントを不正に使用または複製した場合、民事および刑事責任が課せられることがあります。本ソフトウェアは予告なく変更されることがありますので、あらかじめご承知おきください。

サードパーティライセンス

この製品にはRSA以外のサードパーティによって開発されたソフトウェアが含まれます。本製品内のサードパーティ製ソフトウェアに適用される使用許諾契約書の内容については、[thirdpartylicenses.pdf](#)ファイルを参照してください。

暗号技術に関する注意

本製品には、暗号技術が組み込まれています。これらの暗号技術の使用、輸入、輸出は、各国の法律で禁止または制限されています。本製品を使用、輸入、輸出する場合は、各国における使用または輸出入に関する法律に従わなければなりません。

配布

この資料に記載される、いかなるEMCソフトウェアの使用、複製、頒布も、当該ソフトウェアライセンスが必要です。EMC Corporationは、この資料に記載される情報が、発行日時時点で正確であるとみなしています。この情報は予告なく変更されることがあります。

この資料に記載される情報は、「現状有姿」の条件で提供されています。EMC Corporationは、この資料に記載される情報に関する、どのような内容についても表明保証条項を設けず、特に、商品性や特定の目的に対する適応性に対する黙示の保証はいたしません。

目次

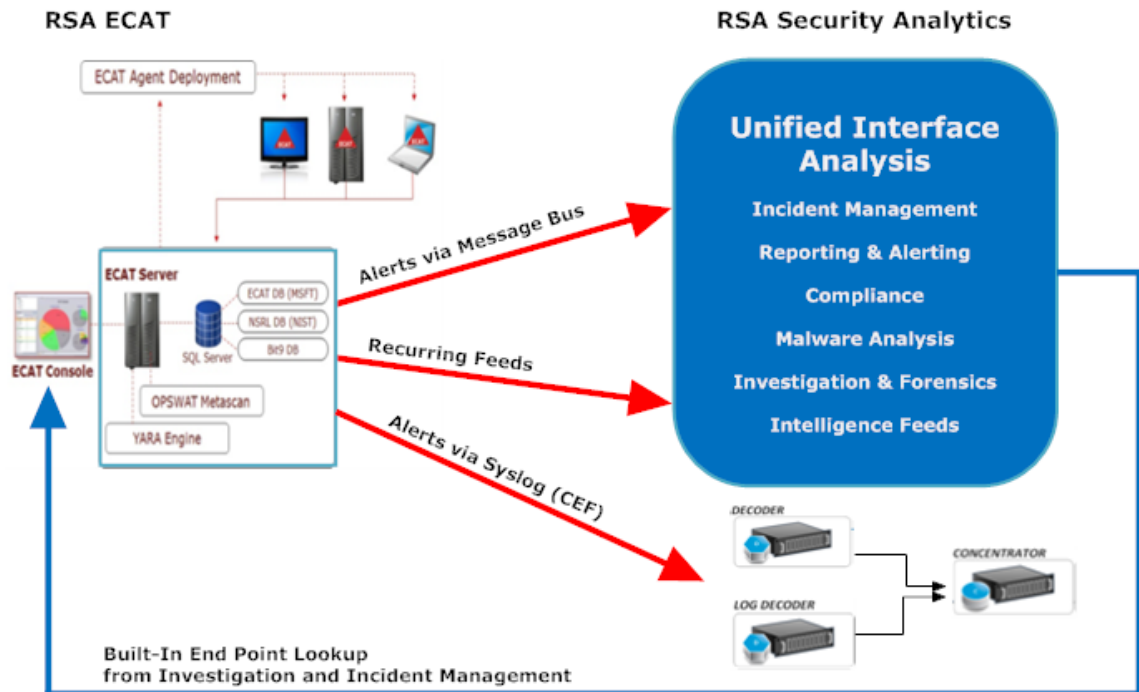
RSA ECATとの統合	5
統合オプション	5
ビルトインのエンドポイント ルックアップ	5
その他の統合オプション	6
ECATアラートとセキュリティ侵害 インジケータ	7
RSA Live Feedを受信するためのECATの構成	8
前提条件	8
Feedの有効化または無効化	8
ECATバージョン4.0の場合	8
ECATバージョン4.1の場合	9
ECAT 4.0以降向けのRSA Live Feed	12
メッセージ バス経由のECATアラートの構成	16
前提条件	16
ECATの外部コンポーネントとしてのIncident Management Brokerの構成	17
ECATバージョン4.0の場合	17
ECATバージョン4.1の場合	17
Security Analytics BrokerでのECATのCA証明書の構成	18
繰り返しFeedを通じたECATからのコンテキスト データの構成	20
前提条件	20
構成	20
Security analyticsのECAT Feedを有効化します。	21
ECATバージョン4.0の場合	21
ECATバージョン4.1の場合	22
ECAT SSL証明書のエクスポート	25
Security Analyticsでの繰り返しカスタムFeedタスクの構成	26
Security Analytics Concentratorサービスの構成	29
結果	31
トラブルシューティング	31
Log DecoderへのSyslog経由のECATアラートの構成	32
前提条件	32

手順	32
Syslog出力をSecurity Analyticsに送信するためのECATの構成	33
ECATバージョン4.0の場合	33
ECATバージョン4.1の場合	35
table-map-custom.xmlでのテーブル マッピングの編集	36
Security Analytics Concentratorサービスの構成	39
例	40
ECATメタ キー	41
結果	42

RSA ECATとの統合

RSA ECAT 4.0以降およびRSA Security Analytics 10.4以降の両方を使用しているRSAユーザーは、ECATとSecurity Analyticsを複数の方法で統合できます。このガイドは、Security Analyticsバージョン10.6以降用です。

統合オプション



ビルトインのエンドポイント ルックアップ

アナリストがブラウザでSecurity Analyticsにアクセスしているコンピュータに、RSA ECAT UI(ユーザー インターフェイス) がインストールされている場合、Security Analytics InvestigationとSecurity Analytics Incident Managementに組み込まれたエンドポイント ルックアップ機能によって、特定のIPアドレスを右クリックすればECATコンソール サーバにアクセスできます。IPアドレス(ip-src, ip-dst, ipv6-src, ipv6-dst, orig_ip)、host(alias-host, domain.dst)、client、file-hash。詳細については、*Investigation*および*Malware Analysis*の「**メタ キーの外部ルックアップの起動**」トピックおよび*Incident Management*の「**[アラート]ビュー**」トピックを参照してください。

ビルトインParserであるRSA ECATまたはCEFのいずれかを使用し、Investigationでメタデータのロードに使用されるデフォルトのメタ キーをカスタマイズしていない場合、エンドポイント ルックアップにSecurity Analyticsの構成は必要ありません。*Investigation*および*Malware Analysis*の「**Investigationでのデフォルト メタ キーの管理と適用**」を参照してください。

注: 例外としては、Investigationのデフォルト メタ キーの表示設定を編集して、Security Analyticsをカスタマイズしたり、メタ キーをtable-map-custom.xmlファイルに追加したり、RSA ECAT Feedをカスタマイズした場合などです。「システム構成」ガイドの「コンテキスト メニューのカスタム アクションの追加」トピックで説明されているように、構成によっては、[Administration] > [システム]ビューから、ECATルックアップのコンテキスト メニューにカスタム メタ キーを追加する必要があります。

その他の統合オプション

WindowsホストにインストールされたRSA ECAT 4.0以降のコンソール サーバを使用し、ECATとSecurity Analyticsを管理者が適切に構成した場合、赤色の矢印で示すように、ECAT解析データに関する4種類の追加の統合が利用可能になります。

利用可能なRSA ECATとSecurity Analyticsとの統合は次のとおりです。

- **Security Analytics Log DecoderへのSyslog(CEF) 経由のECATアラート。**この統合により、LiveインテリジェンスをECATアラートに適用したり、ECATイベントをSecurity Analyticsエコシステム内の他のログやパケット メタデータと関連づけたりすることが可能になります(次を参照: [Log DecoderへのSyslog経由のECATアラートの構成](#))。
- **Security Analytics Incident Managementへのメッセージ バス経由のECATアラート通知。**この統合により、Security Analyticsでの一元化されたインシデント管理およびワークフローへの対応が可能になります(「*Incident Management* 構成ガイド」の「インシデント管理にアラートを表示するためのアラート ソースの構成」トピックを参照)。
- **Security Analytics Liveの繰り返しFeedを通じたECATからのコンテキスト データ** この統合では、たとえば、ホスト オペレーティングシステム、MACアドレス、スコア、ログやパケット データに存在しないその他のデータなどのコンテキスト情報を使用してSecurity Analytics Investigationに表示されるセッションにより豊富な情報を付加することができます(次を参照: [繰り返しFeedを通じたECATからのコンテキスト データの構成](#))。
- **ECAT 4.0以降へのRSA Live Feed。**この統合オプションでは、疑わしいドメインやIPアドレスを含むRSA Liveの複数のFeedを使用して、ECATインスタントIOC(セキュリティ侵害インジケータ)を強化することができます。ECAT内で定義されたインスタントIOCは、RSA LiveのFeedを利用して、インテリジェンスを強化することができます。ECAT 4.0はRSA LiveにFeedを発行しません(次を参照: [RSA Live Feedを受信するためのECATの構成](#))。

ECATアラートとセキュリティ侵害 インジケータ

ECATインスタントIOC(セキュリティ侵害 インジケータ)は、RSA ECATがスキャン対象のホストにおけるマルウェアの存在を判断するために、収集されたECATスキャン データに対して実行するデータベースクエリーです。RSA ECAT 4.0以降には、ユーザーが有効化しアラート対象としてマークできるIOCが同梱されています。RSA ECATは、データベースに収集されて格納される新しいスキャン データに対してIOCクエリーを定期的に行います。IOCクエリーにマッチするデータが検知された場合、これはセキュリティ侵害の可能性を示しており、このイベントをユーザーに報告したり、外部システムにアラートとして送信することができます。

アラートには次のタイプがあります。

- マシン アラート: このアラートは、対象のマシンが疑わしいことを示します。
- モジュール アラート: このアラートは、ファイル、dll、実行ファイルなどのモジュールが疑わしいことを示します。対象のモジュールに関する詳細情報も含まれています。
- IPアラート: このアラートは、疑わしいインターネット アクティビティ(トラフィック)が検知されていることを示します。
- イベントアラート: このアラートは、前述のカテゴリに属さないその他の疑わしいアクティビティがECATで検知されたことを示します。

これらのアラート タイプはそれぞれSecurity Analyticsに関連づけることができます。

トピック

- [RSA Live Feedを受信するためのECATの構成](#)
- [メッセージ バス経由のECATアラートの構成](#)
- [繰り返しFeedを通じたECATからのコンテキスト データの構成](#)
- [Log DecoderへのSyslog経由のECATアラートの構成](#)

RSA Live Feedを受信するためのECATの構成

RSA ECAT 4.0以降は、RSA LiveからFeedを受信するように構成できます。RSA LiveのFeedの中には、疑わしいドメインやIPアドレスを含むものがあります。ECAT内で定義されているいくつかのIOC(インスタントセキュリティ侵害インジケータ)は、これらのFeedによってインテリジェンスが強化されます。ECATでは、デフォルトですべてのFeedが無効になっています。Feedを有効にすると、ECATコンソールサーバはRSA Live(<https://cms.netwitness.com>)に接続し、FeedデータをECATシステムに定期的にダウンロードします。

注:

- ECATはRSA LiveにFeedを発行しません。Feedデータを受信するのみです。
- ECATバージョン4.0とECATバージョン4.1では、RSA Live Feedを受信するようにECATを構成する手順が異なります。両方のバージョンの手順について説明しています。

前提条件

この統合の要件を次に示します。

- バージョン4.0以降のECAT UIおよびバージョン10.6 Security Analyticsサーバがインストールされている必要があります。
- RSA Liveアカウントが構成されていること。アカウントのユーザー名とパスワードはRSAから入手できます。
- ECATコンソールサーバが<https://cms.netwitness.com>に接続できること。

Feedの有効化または無効化

ECATバージョン4.0の場合

1. ECATのユーザー インタフェースを開き、適切な認証情報を使用してログオンします。
2. ページの上部にあるメニューバーから、[データベース] > [チェックサムのインポート]を選択します。
[Import Checksum]ダイアログが表示されます。
3. [RSA Live]タブを選択し、[Settings]タブを選択します。
4. RSA Liveサーバの詳細と認証情報を入力します。
ホスト値は通常、cms.netwitness.comです。
ポート番号は通常、443です。

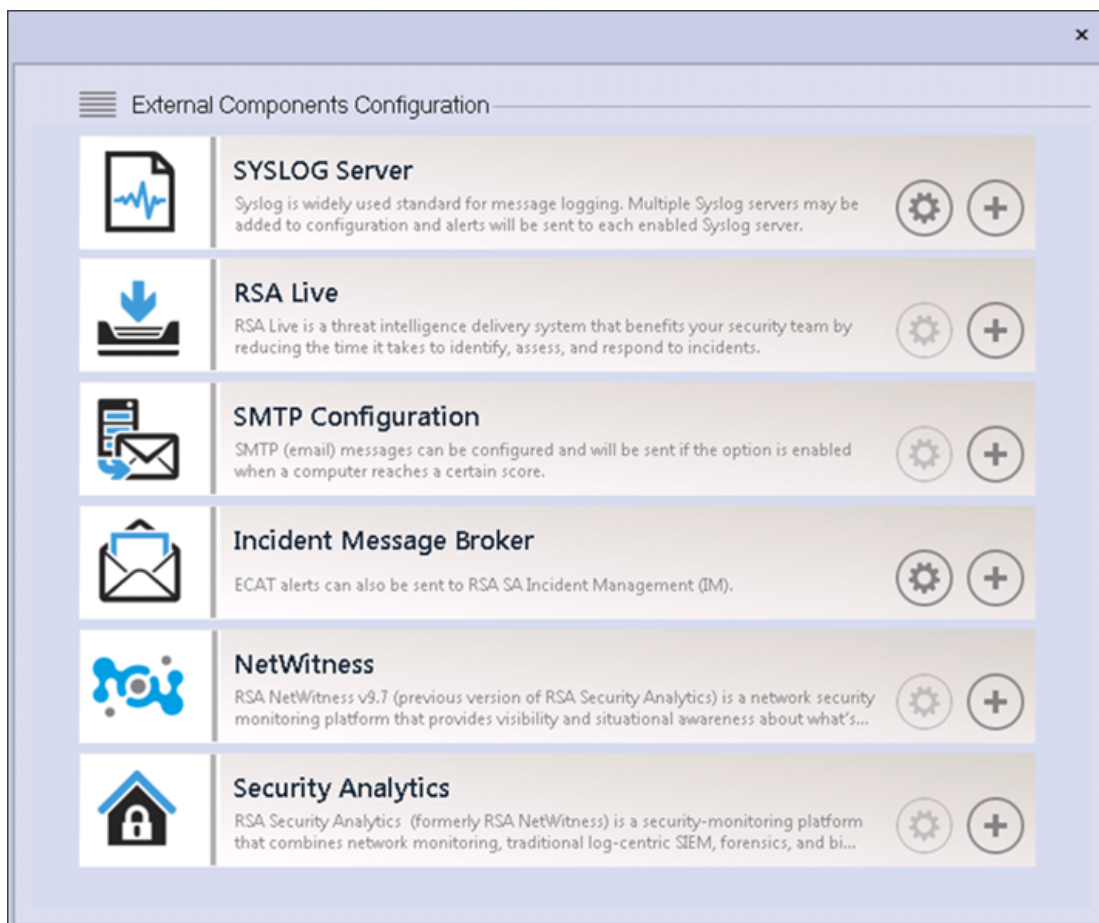
5. 接続を確認するために、[Test Connection]をクリックします。
テストに成功した場合は、「Passed」と表示されます。
6. [Apply]をクリックします。
7. [Subscribed Feeds]タブを選択します。
すべてのFeedのリストが表示されます。
8. RSA LiveからインポートするFeedを選択します。
9. 適切な間隔を入力します。推奨される時間は24時間です。この場合、ECATは、24時間ごとにRSA Liveに接続して、インポートされたデータを更新します。
10. (オプション) Feedを今すぐダウンロードするには、[Refresh Now]をクリックします。
11. [Save]をクリックします。

各種のFeedからインポート済みの既知の有害なドメインおよびIPのステータスを表示するには、[Status]タブを選択し、Feedを選択します。Feedあたりのエントリーの数はいずれも異なり、数百件から数千件の範囲に及びます。

ECATバージョン4.1の場合

1. ECATの認証情報を使用してSQLユーザーを作成します。
 - a. ECATのユーザー インタフェースを開き、適切な認証情報を使用してログオンします。
 - b. [構成] > [ユーザーとロールの管理]をクリックします。
 - c. [セキュリティ]で、パネルを右クリックし、[新しいSQLユーザーの作成]を選択します。
 - d. ログイン名とパスワードを指定します。
2. ページの上部にあるメニュー バーから、[構成] > [監視と外部コンポーネント]を選択します。

3. [外部コンポーネントの構成]ウィンドウが表示されます。[RSA Live]を選択し、[+]をクリックします。



4. [RSA Live] ダイアログが表示されます。

RSA Live

ON

RSA Live Settings

Username : Server Hostname/IP :

Password : Port : 443

RSA Live Subscribed Feeds

Refresh Interval : 24 Hour(s).

Feed Name	Subscribed	Count	Error Message	Last Updated
Malware Domai...	<input type="checkbox"/>	0		1/1/0001 12:00:...
Malware Domai...	<input type="checkbox"/>	0		1/1/0001 12:00:...
Malware IP List	<input type="checkbox"/>	0		1/1/0001 12:00:...
RSA FirstWatch ...	<input type="checkbox"/>	0		1/1/0001 12:00:...
RSA FirstWatch ...	<input type="checkbox"/>	0		1/1/0001 12:00:...
RSA FirstWatch ...	<input type="checkbox"/>	0		1/1/0001 12:00:...
RSA FirstWatch ...	<input type="checkbox"/>	0		1/1/0001 12:00:...
RSA FirstWatch ...	<input type="checkbox"/>	0		1/1/0001 12:00:...
RSA FirstWatch ...	<input type="checkbox"/>	0		1/1/0001 12:00:...
RSA FirstWatch ...	<input type="checkbox"/>	0		1/1/0001 12:00:...
RSA FraudActio...	<input type="checkbox"/>	0		1/1/0001 12:00:...
RSA FraudActio...	<input type="checkbox"/>	0		1/1/0001 12:00:...
14 items total				

Test Settings

5. [RSA Live] の下にある[オン]に、このコンポーネントを識別する名前を入力します。
6. [RSA Liveの設定]で、次の手順を実行します。
- [ユーザー名]と[パスワード]に、このコンポーネントへのアクセスに使用する認証情報を入力します。
 - [サーバホスト名/IP]を指定します。デフォルト値は`cms.netwitness.com`です。必要に応じて、更新します。
 - [ポート]を指定します。デフォルトのポート番号は443です。必要に応じて、更新します。
7. [サブスクライブされたRSA Live Feed]で、次の手順を実行します。
- [更新間隔]に、適切な間隔を入力します。推奨される間隔は24時間です。この場合、ECATは、24時間ごとにRSA Liveに接続して、インポートされたデータを更新しま

す。

- b. RSA LiveからインポートするECATのFeedを選択します。
8. [保存]をクリックします。
RSA LiveコンポーネントがECATに追加され、Feedがアクティブ化されます。
9. 接続を検証するには、新たに追加されたコンポーネントを選択し、[設定のテスト]をクリックします。
すべての設定が正しい場合は、「Passed」と表示されます。

ECAT 4.0以降向けのRSA Live Feed

Feed名	説明
RSA FirstWatch Insider Threat Domains	このFeedには、インサイダー脅威に関係していることが確認されているドメインが含まれます。
RSA FirstWatch Insider Threat IPs	このFeedには、インサイダー脅威に関係していることが確認されているIPが含まれます。
RSA FraudAction IPs	このFeedには、RSA FraudAction FeedからのIPが含まれます。
RSA FraudAction Domains	このFeedには、RSA FraudAction Feedからのドメインが含まれます。
RSA FirstWatch IP Reputation	このFeedには、セキュリティ侵害が確認されているIPが含まれます。
RSA FirstWatch Criminal VPN Entry IPs	このFeedには、犯罪性の高い匿名サービスの既知のVPNエントリーノードを表すIPが含まれます。
RSA FirstWatch Criminal VPN Exit IPs	このFeedには、犯罪性の高い匿名サービスの既知のVPN出口ノードを表すIPが含まれます。

Feed名	説明
RSA FirstWatch APT Threat IPs	このFeedには、APTに関係していることが確認されているIPが含まれます。
RSA FirstWatch Exploit IPs	このFeedには、マルウェアの配信に関係していることが確認されているIPが含まれます。
RSA FirstWatch Command and Control IPs	このFeedには、マルウェアのコマンド&コントロールに関係していることが確認されているIPが含まれます。
RSA FirstWatch APT Threat Domains	このFeedには、APTに関係していることが確認されているドメインが含まれます。
RSA FirstWatch Command and Control Domains	このFeedには、マルウェアのコマンド&コントロールに関係していることが確認されているドメインが含まれます。
RSA FirstWatch Criminal SOCKS node IPs	このFeedには、犯罪性の高い匿名サービスの既知のSOCKSノードを表すIPが含まれます。
IDefense Threat Indicators Domains	情報セキュリティの責任者は、Verisign iDefenseセキュリティインテリジェンスサービスを使用して、24時間365日いつでも、脆弱性、悪意のあるコード、グローバルな脅威に関連する正確で実用的なサイバーインテリジェンスにアクセスできます。Verisign iDefenseによる詳細な解析、インサイト、対応に関する項目は、民間企業や政府機関が、新たに発生する脅威や脆弱性に先行して対応するのに役立ちます。

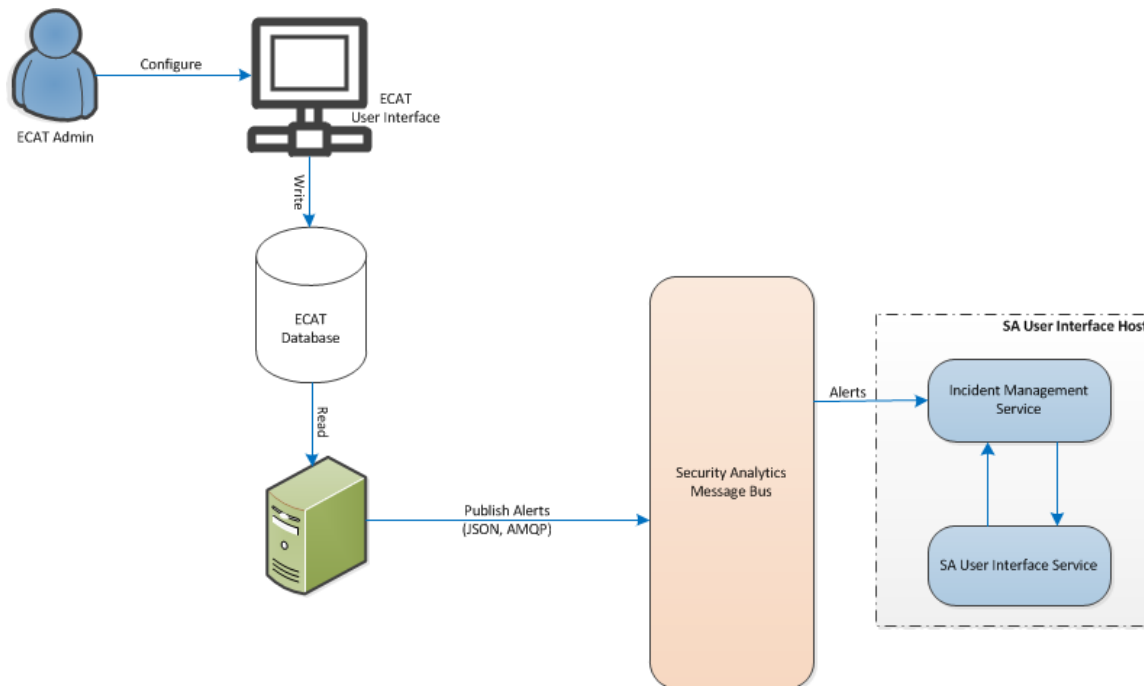
Feed名	説明
Spamhaus DROP List IP Ranges	DROP(Don't Route Or Peer) および EDROPは、盗難され「ハイジャックされた」netblockや、犯罪者やプロフェッショナルなスパマーによって完全に制御されたnetblockが記載された、勧告的な「drop all traffic」リストです。
Zeus Tracker	Zeustラッカーは、世界中のzeus(zbot、prg、wsnpoem、gorhax、kneberとも呼ばれます)に関するコマンド&コントロールサーバ(ホスト) のIPアドレスのリストです。Zeustラッカーでは、2,800を超える悪意のあるzeusコマンド&コントロールサーバを追跡しています。Zeusは、主に、ドライブバイダウンロードとフィッシングという手法によって広まっています。
Zeus Domain Tracker	Zeusドメインラッカーは、zeus(zbot、prg、wsnpoem、gorhax、kneberとも呼ばれます) コマンド&コントロールドメインの名前のリストです。Zeustラッカーでは、2,800を超える悪意のあるzeusコマンド&コントロールサーバを追跡しています。Zeusは、主に、ドライブバイダウンロードとフィッシングという手法によって広まっています。
Malware Domain List	www.malwaredomainlist.com の情報に基づく、マルウェアと頻繁に関係するドメインのリスト。

Feed名	説明
SpyEye Domain Tracker	SpyEyeドメイントラッカーは、spyeye (zbot、prg、wsnpoem、gorhax、kneberとも呼ばれます) 指揮統制ドメインの名前のリストです。SpyEyeトラッカーでは、2,800を超える悪意のあるspyeyeコマンド&コントロールサーバを追跡しています。SpyEyeは、主に、ドライブバイダウンロードとフィッシングという手法によって広まっています。
RSA FirstWatch Criminal Socks User IPs	このFeedには、犯罪性の高い匿名サービスの使用が確認されているIPが含まれます。
Tor Exit Nodes	このFeedには、Torネットワークのアクティブな出口ノードとしてリストされたIPが含まれます。
Tor Nodes	このFeedには、TorネットワークのアクティブノードとしてリストされたIPが含まれます。
Malware Domains	www.malwaredomains.comの情報に基づく、マルウェアと関係するドメインのリスト。
Malware IP List	www.malwaredomainlist.comの情報に基づく、マルウェアと頻繁に関係するIPアドレスのリスト。

メッセージ バス経由のECATアラートの構成

ここでは、Security AnalyticsとECATを統合するのに必要な手順を紹介します。この手順を完了すると、Security AnalyticsのIncident ManagementコンポーネントによってECATアラートが収集され、[インシデント]>[アラート]ビューに表示されるようになります。

次の図に、Security Analyticsのインシデント管理キューへのECATアラートの流れと、[インシデント]>[アラート]ビューでのアラートの表示方法を示します。



前提条件

以下の条件を満たしていることを確認します。

- Incident Managementサービスがインストールされていて、Security Analytics 10.4以降で実行されていること。
- ECAT 4.0以降がインストールされ実行されていること。

ECATの外部コンポーネントとしてのIncident Management Brokerの構成

ECATバージョン4.0の場合

メッセージバス経由でアラートをSecurity Analyticsのユーザーインターフェイスに送信するようにECATを構成するには、次の手順を実行します。

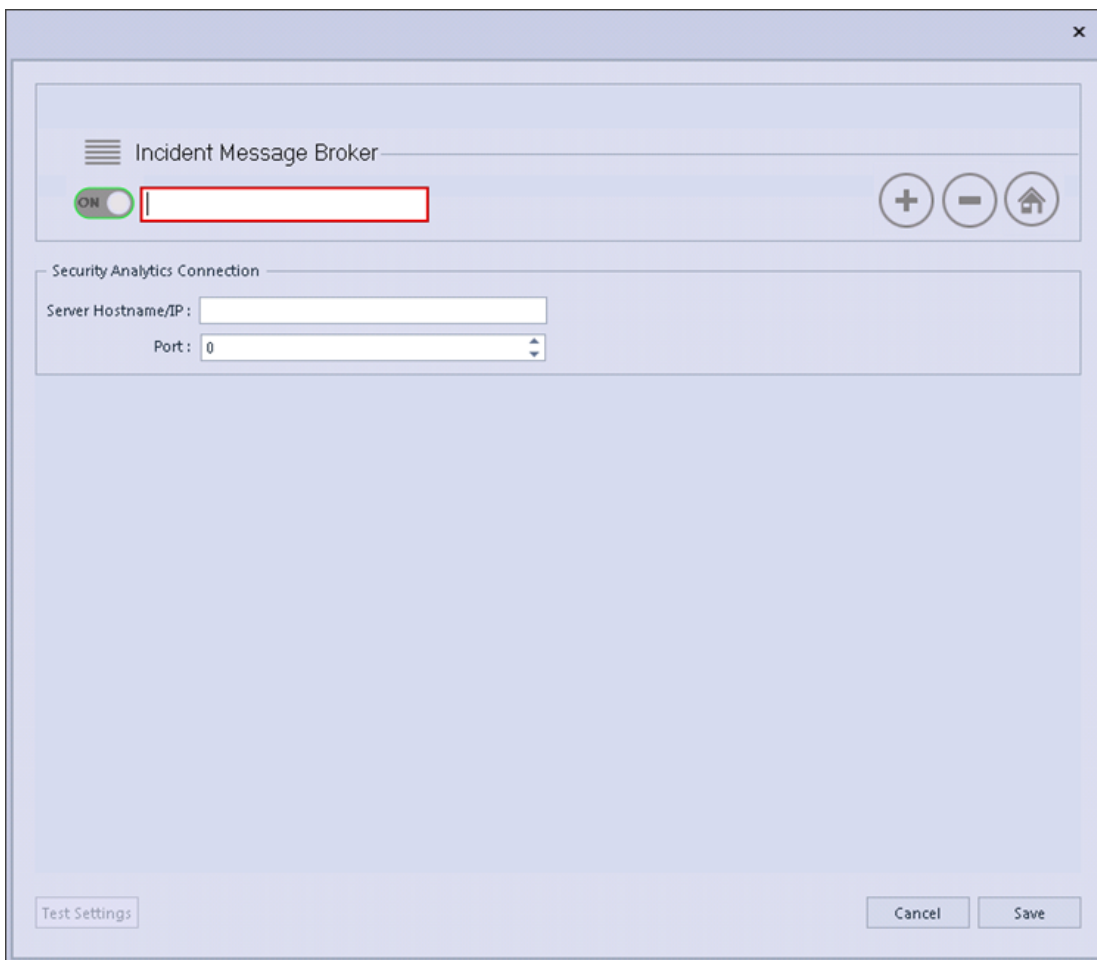
1. ECATのユーザーインターフェイスを開き、適切な認証情報を使用してログインします。
2. メニューバーから[構成]>[監視と外部コンポーネント]を選択します。
[Monitoring and External Components]ダイアログが表示されます。
3. ダイアログ内の任意の場所を右クリックし、[Add Component]を選択します。
[Add Component]ダイアログボックスが表示されます。
4. 次の情報を入力します。
 - [Component Type]のドロップダウンオプションから、IM brokerを選択します。
 - IM brokerを識別するためのUnique Nameを入力します。
 - IM brokerのHost DNS or IP addressを入力します。
 - Port numberを入力します。
5. [保存]>[閉じる]の順にクリックして、すべてのダイアログボックスを閉じます。

ECATバージョン4.1の場合

メッセージバス経由でアラートをSecurity Analyticsのユーザーインターフェイスに送信するようにECATを構成するには、次の手順を実行します。

1. ECATのユーザーインターフェイスを開き、適切な認証情報を使用してログインします。
2. メニューバーから[構成]>[監視と外部コンポーネント]を選択します。
[外部コンポーネントの構成]ダイアログが表示されます。
3. [インシデントメッセージブローカー]で、[+]をクリックして、IM(インシデントメッセージ)ブローカーを追加します。

[インシデント メッセージ ブローカー]ダイアログが表示されます。



4. [インシデント メッセージ ブローカー]の下にある[オン]に、メッセージ ブローカーの名 前を入力します。
5. [Security Analyticsの接続]の下で、次の操作を実行します。
 - a. [サーバホスト名/IP]に、Security AnalyticsサーバのIPアドレスを入力します。
 - b. [ポート]をデフォルト値の[5671]にします。必要に応じて、フィールドを更新します。
6. [保存]をクリックします。

Security Analytics BrokerでのECATのCA証明書の構成

インシデント管理アラートのSSLを設定するには、次の手順を実行します。

1. ECATのプライマリコンソールサーバで、ローカルコンピュータの個人用証明書ストアから(秘密鍵を選択せずに)ECATのCA証明書を.cer形式(Base-64エンコード X.509)でエク

サポートします。

2. ECATのプライマリコンソール サーバで(ECAT `makecert`実行可能ファイルがあるコンピューターおよび場所から)、ECAT CA証明書を使用して、ECATのクライアント証明書を生成します。(CN名を「ecat」に設定する必要があります)。

```
makecert -pe -n "CN=ecat" -len 2048 -ss my -sr LocalMachine -a sha1 -
sky exchange -eku 1.3.6.1.5.5.7.3.2 -in "EcatCA" -is MY -ir
LocalMachine -sp "Microsoft RSA SChannel Cryptographic Provider" -cy
end -sy 12 client.cer
```

3. ECATのプライマリコンソール サーバで、ステップ2で生成したクライアント証明書の拇印をメモしておきます。次のように、`ConsoleServer.Exe` ファイルの `IMBrokerClientCertificateThumbprint` セクションにクライアント証明書の拇印値を入力します。

```
<add key="IMBrokerClientCertificateThumbprint"
value="?896df0efacf0c976d955d5300ba0073383c83abc"/>
```

注: 値フィールドに拇印の値を入力するときは、疑問符(?)を削除してから値を入力し、ファイルを保存してください。

4. Security Analyticsサーバで、`.cer`形式のECAT CA証明書ファイル(ステップ1)の内容を追加します。


```
/etc/puppet/modules/rabbitmq/files/truststore.pem
```
5. Security Analyticsサーバで、次のいずれかを実行します。
 - 次のコマンドを実行して、Puppetエージェントを実行します:`puppet agent -t`
 - Security Analyticsサーバでエージェントが実行されるまで30分ほど待機してください。
6. ECATプライマリコンソール サーバで、Security Analyticsサーバから、信頼されたルート証明機関ストアに `/var/lib/puppet/ssl/certs/ca.pem` ファイルをインポートします。この手順により、ECATがクライアントとしてIncident Managementサーバの証明書を信頼します。
7. ECATサーバを再起動して、ECATを有効にし、Security Analyticsにアラートが送信されるようにします。

繰り返しFeedを通じたECATからのコンテキスト データの構成

このトピックでは、Security AnalyticsでRSA ECATデータを使用する方法を構成し、ECATからDecoderおよびLog Decoderセッションにコンテキスト データを提供するための手順について説明します。この構成では、コンテキスト メタ値の他、Security Analyticsエコシステムのその他のメタデータとの相関を構築するときに使用できるインスタントIOCアラートが追加されます。

管理者は、Security Analytics Liveの繰り返しFeedを介してECATシステムからのスキャン コンテキスト データを使用するようにSecurity Analyticsを構成できます。この統合により、DecoderまたはLog Decoderからのセッションに対して、Security Analytics Investigationにコンテキスト情報が表示されるようになります。これらの情報には、ホスト オペレーティング システム、MACアドレス、スコアなど、DecoderまたはLog Decoderからのセッションのログまたはパケット データには存在しないデータが含まれます。

注: この機能は、パケットDecoderを使用する環境を対象にしていますが、繰り返しFeedはLog Decoderにも実装できます。

注意: 多数のECATホストがある環境では、繰り返しFeedを使用することで、Security Analyticsの収集デバイス(DecoderおよびLog Decoder)のパフォーマンスが低下する場合があります。

前提条件

- バージョン4.0以降のECATコンソール サーバおよびSecurity Analyticsサーババージョン10.4以降がインストールされている必要があります。
- バージョン10.4以降のRSA DecoderおよびConcentratorがネットワーク内のSecurity Analyticsサーバに接続されている必要があります。

構成

この統合を構成するには、次の手順を実行します。

- ECATユーザー インターフェイスでSecurity AnalyticsのECAT Feedを有効化します。
- ECATコンソール サーバからECAT CA証明書をエクスポートし、Security Analyticsトラストアにインポートします。
- Security Analytics Concentratorサービスを構成して、インデックスを作成するメタ キーを定

義します。

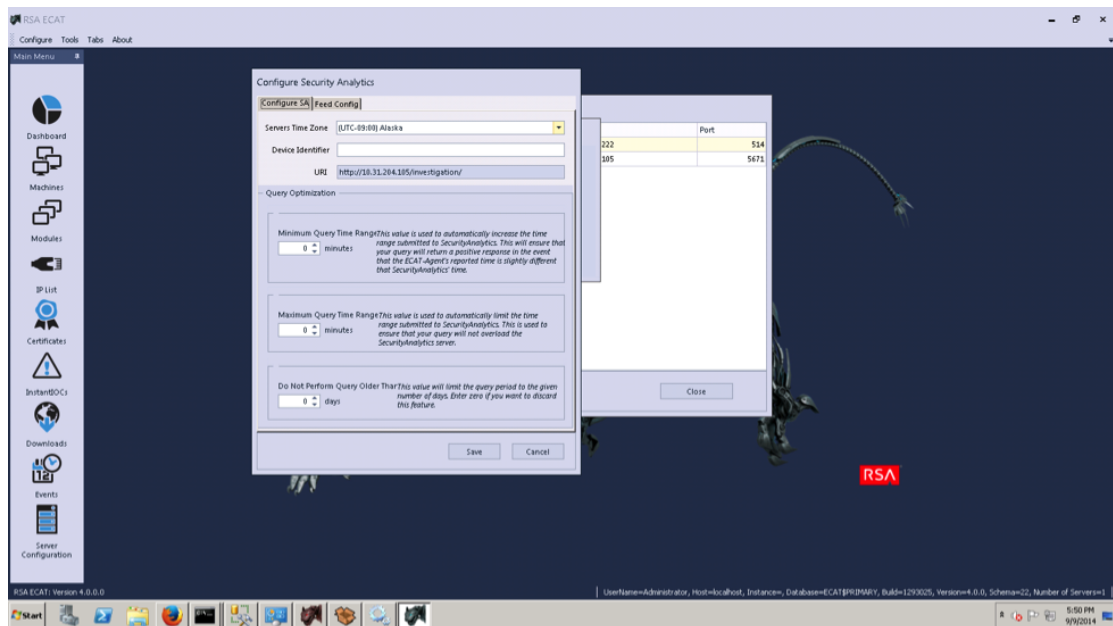
4. Security Analytics Liveで繰り返しFeedを作成します。

Security analyticsのECAT Feedを有効化します。

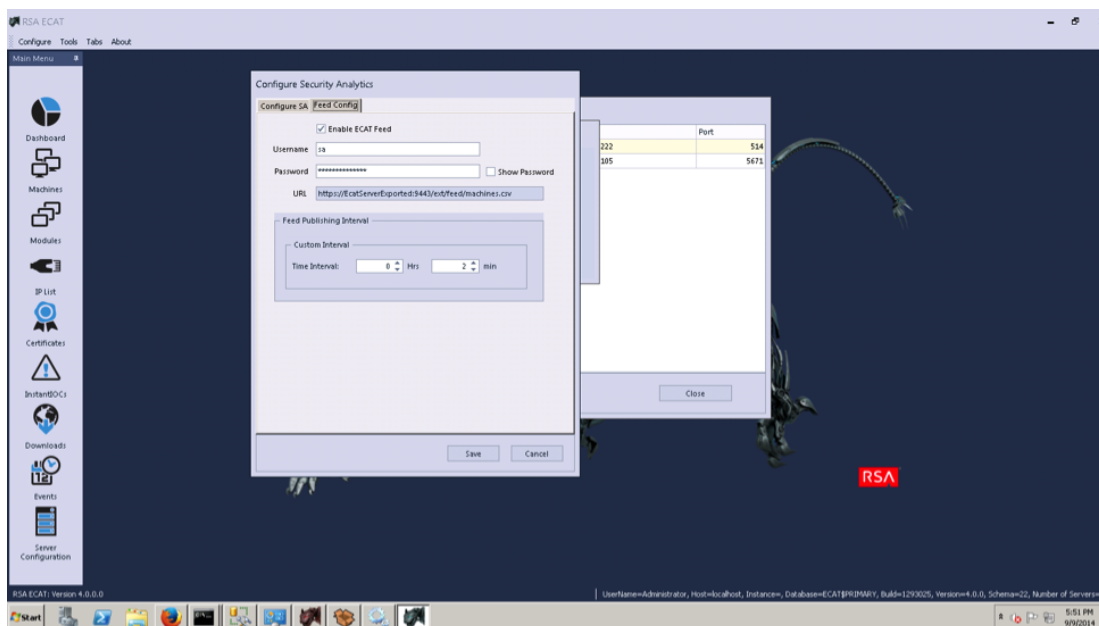
ECATバージョン4.0の場合

1. ECATのユーザー インタフェースを開き、適切な認証情報を使用してログオンします。
2. メニュー バーから[構成]>[外部コンポーネントの監視]を選択します。
[Add Components]ダイアログが表示されます。
3. Security Analyticsコンポーネントを追加します。[Unique Name]と[Host DNS or IP]に値を入力し、[Settings]をクリックします。

[Configure Security Analytics]ダイアログが表示されます。



4. [タイムゾーン]を有効にし、[Feed構成]タブをクリックします。



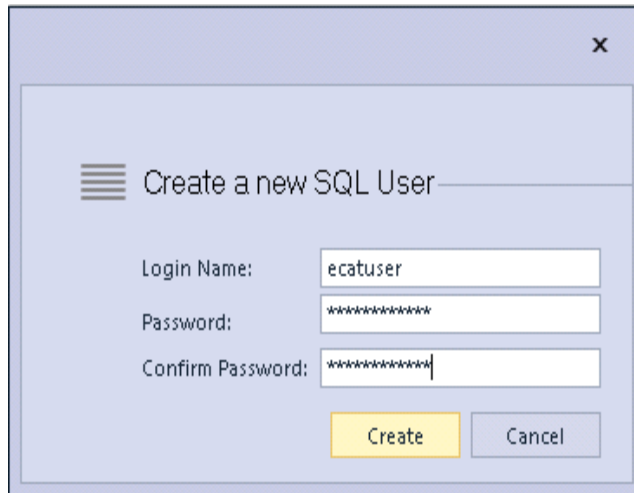
5. [ECAT Feedを有効化]をオンにし、[ユーザー名]と[パスワード]に値を入力します。
[Feed Publishing Interval]を構成します。[保存]をクリックします。
Feedが作成されます。
6. Feedに割り当てられたURL、ユーザー名、パスワードをメモに記録します。この情報は、Security Analyticsで使用されます。
7. Feedが正常に作成されたことを確認するために、ブラウザを開き、URLを入力します。プロンプトが表示されたら、ユーザー名とパスワードを入力します。machines.csvという名前のファイルがダウンロードされるかどうかを確認します。

ECATバージョン4.1の場合

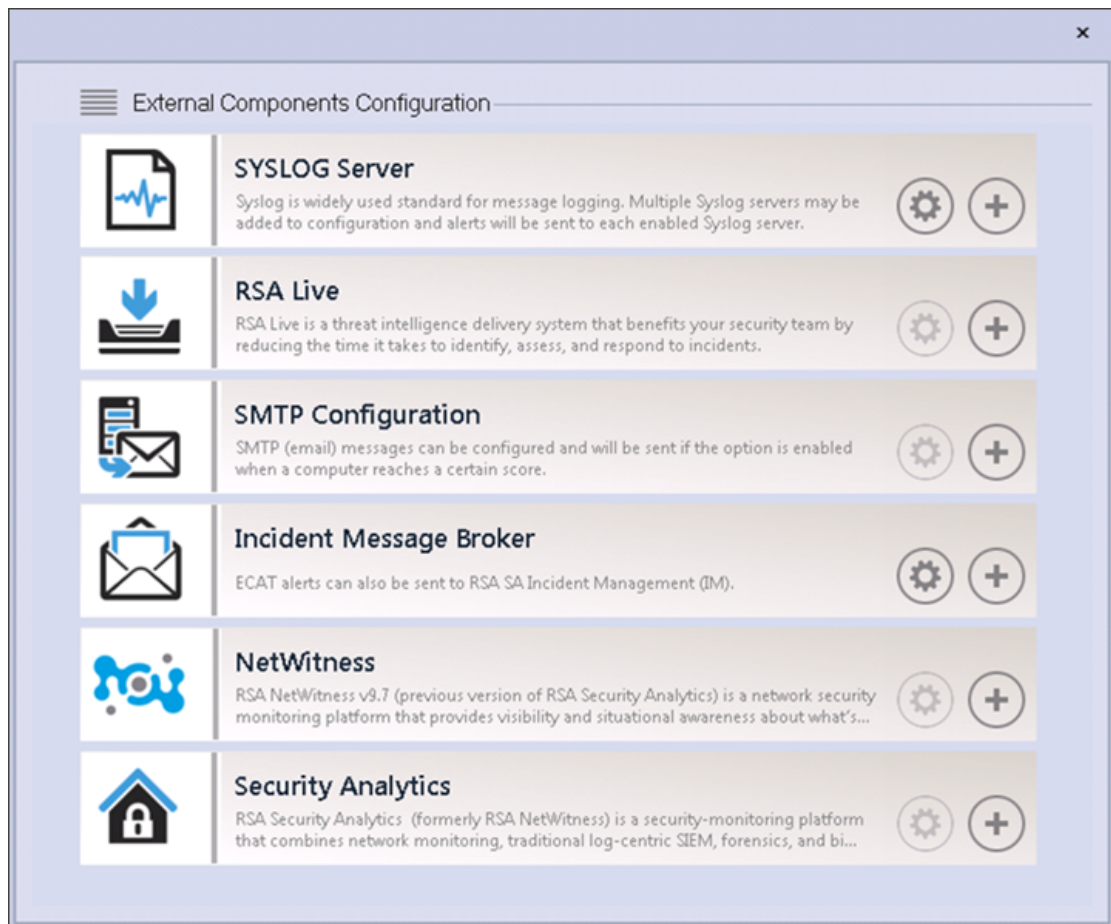
ECATユーザー インタフェースで、次の手順を実行します。

1. ECATでSQLユーザーを作成します。
 - a. ECATのユーザー インタフェースを開き、適切な認証情報を使用してログオンします。

- b. [セキュリティ]の下で、パネルを右クリックし、[SQLユーザーの作成]を選択します。
[新しいSQLユーザーの作成]ダイアログが表示されます。



- c. ログイン名とパスワードを指定します。
2. メニューバーから[構成]>[外部コンポーネントの監視]を選択します。
[外部コンポーネントの構成]ダイアログが表示されます。



3. Security Analyticsで、[+]をクリックします。
[Security Analytics]ダイアログが表示されます。

The screenshot shows the 'Security Analytics' configuration window. At the top, there is a title bar with a hamburger menu icon, the text 'Security Analytics', a green 'ON' toggle switch, and a text input field. To the right are three circular icons: a plus sign, a minus sign, and a home icon. Below the title bar is the 'Security Analytics Connection' section, containing 'Server Hostname/IP' and 'Port' (443) fields. The 'Configure Security Analytics' section includes a 'Servers Time Zone' dropdown menu (set to 'UTC-11:00 Coordinated Universal Time-11'), 'Device Identifier', and 'URI' text fields. The 'Query Optimization' section has 'Query Time Range' with 'Min' (0) and 'Max' (30) minutes, and 'Do Not Perform Query Older Than' (0) days. The 'Configure ECAT Feeds for SA' section features an unchecked 'Enable ECAT Feed' checkbox, 'Username', 'Password' (with an eye icon), and 'URL' text fields. A 'Feed Publishing Interval' section shows 'Time Interval' set to 0 Hrs and 30 min. At the bottom, there are 'Test Settings', 'Cancel', and 'Save' buttons.

4. [Security Analytics]の下にある[オン]に、Security Analyticsコンポーネントを識別する名前を入力します。
5. [Security Analyticsの接続]の下で、次の操作を実行します。
 - a. [サーバホスト名/IP]に、Security Analyticsサーバのホスト名またはIPアドレスを入力します。
 - b. [ポート]をデフォルト値の[443]にします。必要に応じて、フィールドを更新します。
6. [Security Analyticsの構成]の下で、次の操作を実行します。
 - a. [サーバのタイムゾーン]に、コンポーネントのタイムゾーンを入力します。
 - b. [デバイスの識別子]に、Security Analytics ConcentratorのデバイスIDを入力します。

注: [調査] > [ナビゲート] > [<ConcentratorまたはBrokerの名前>] でConcentratorまたはBrokerを検索すると、Security Analyticsのデバイスの識別子が見つかります。デバイスの識別子は、URL内の「investigation」の後の数字です。たとえば、URLがhttps://<IP address>investigation/319/navigate/valuesの場合、デバイスの識別子は319です。

- [保存]をクリックすると、[URI]フィールドが設定されます。
7. [クエリーの最適化]で、次の操作を実行します。
 - a. [最小値]に、最小のクエリー時間範囲を分単位で入力します。この値を使用して、Security Analyticsに送信される時間範囲を自動的に増加させます。これにより、ECATエージェントの報告された時刻がSecurity Analyticの時刻とわずかに異なる場合、クエリーが肯定的な応答を返すようになります。
 - b. [最大値]に、時間範囲の制限を分単位で入力します。この値を使用して、Security Analyticsに送信される時間範囲が自動的に制限されるため、クエリーがSecurity Analyticsサーバを過負荷にすることはありません。
 - c. [古いクエリーを実行しない]に、クエリー期間の制限を日数で入力します。この機能を無効にする場合は、「0」を入力します。
 8. [SAのECAT Feedの構成]で、次の操作を実行します。
 - a. [ECAT Feedを有効化]を選択します。
 - b. SQLユーザー名とパスワード(ステップ1で構成した)を入力し、Feedの場所にアクセスします。
[保存]をクリックすると、[URL]フィールドが設定されます。
 - c. Feedが発行される頻度の時間間隔を入力します。
 9. [保存]をクリックします。
Feedが作成されます。

ECAT SSL証明書のエクスポート

注: Java 8のサポートはSecurity Analytics 10.5に対して追加されたため、この手順は10.5以上にのみ適用されます。それより前のバージョンのSecurity Analyticsを使用している場合は、このガイドで該当するバージョンを参照してください。

ECATコンソールサーバからECAT CA証明書をエクスポートし、それをSecurity Analyticsホストにコピーするには、次の手順を実行します。

1. ECATコンソールにログオンします。
2. MMCを開きます。

3. コンピューター アカウント用の証明書スナップインを追加します。
4. EcatCAという名前の証明書をエクスポートします。
 - a. 秘密鍵なしでエクスポートします。
 - b. DERエンコード バイナリX.509(.CER) 形式でエクスポートします。
 - c. EcatCA.cerという名前を付けます。
5. Security AnalyticsホストにECAT CA証明書をコピーします。

```
scp EcatCA.cer root@<sa-machine>:.
```
6. ECAT CA証明書をSecurity Analyticsトラスト ストアにインポートするには、次のコマンドを実行します。
 - a. 次のコマンドを使用して、Security AnalyticsにインストールされているJavaバージョンを確認します。

```
java -version
```

openjdkバージョンが表示されます。例: `openjdk version "1.8.0_71"`

注: openjdkバージョンは、Security Analyticsのバージョンに応じて異なる場合があります。

 - b. JDKパラメーターを設定するには、javaディレクトリに移動します。以下のコマンドを実行します。

```
JDK=/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.65-0.b17.e16_7.x86_64/jre/
$JDK/bin/keytool -import -v -trustcacerts -alias ecatca -file
~/EcatCA.cer -keystore $JDK/lib/security/cacerts -storepass
changeit
```

証明書更新の確認のプロンプトが表示されたら、「Yes」と入力します。
7. Security Analyticsホスト上で /etc/hostsを編集して、ECATコンソール サーバのIPアドレスをecatserverexportedという名前にマップします。次の行をファイルに追加します。

```
<ip-address-ecat-cs> ecatserverexported
```
8. Security Analyticsホストを再起動するために、次のコマンドを実行します。

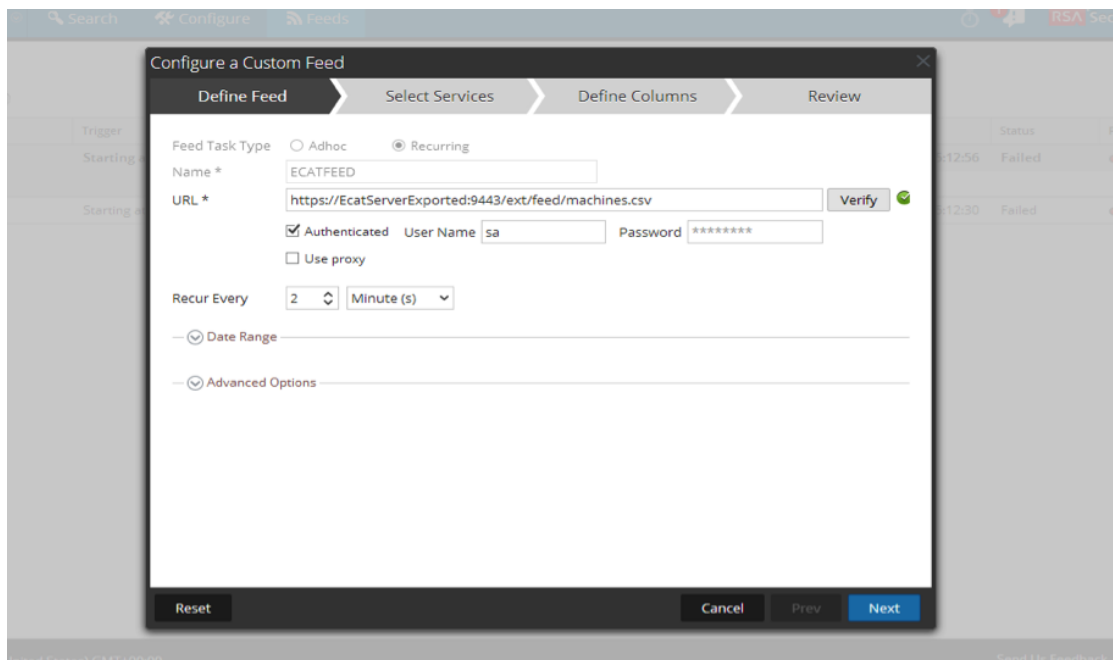
```
stop jettysrv
start jettysrv
```

Security Analyticsでの繰り返しカスタムFeedタスクの構成

Security Analyticsで繰り返しFeedタスクを構成するには、次の手順を実行します。

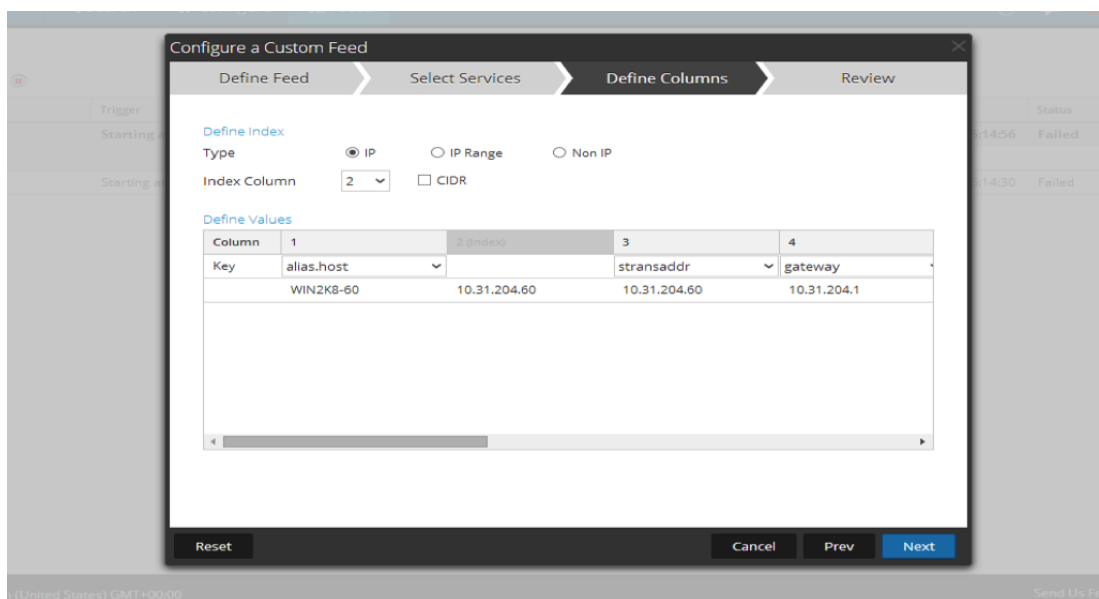
1. Security Analyticsにログオンし、[Live] > [Feed]に移動します。
2. [カスタムFeed] > [次へ]を選択します。

3. 次の操作を実行します。
 - a. [繰り返し]を選択します。
 - b. 名前を入力します。例: EcatFeed。
 - c. ECATがインストールされているWindowsサーバのURLとホスト名を入力します。
 - RSA ECATバージョン4.0の場合は、
`https://<EcatServerHostname>:9443/ext/feed/machines.csv`というURLを使用します。
 - RSA ECATバージョン4.1の場合は、
`https://<EcatServerExported>:9443/api/v2/feed/machines.csv`というURLを使用します。
4. [認証情報]チェックボックスをオンにし、前述の「`{{SA}}`」のECAT Feedの有効化」でメモに記録したユーザー名とパスワードを入力します。
5. [検証]を選択して、Security AnalyticsがWebリソースにアクセスできることを確認します。
6. スケジュールを定義します。[次へ]をクリックします。



7. [サービスの選択]タブで、Feedを使用するDecoderまたはグループを選択します。次へをクリックします。

8. [列の定義]タブで、次の表に従って列名を入力し、Feedを保存します。



次の表に、ECAT Feed用のCSVファイルの列を示します。

列	名前	説明	Security Analyticsでの列名(メタキー名)
1	MachineName	Windowsエージェントのホスト名	alias.host
2	LocalIp	IPv4アドレス	Index
3	RemoteIp	ルーターで検出されるリモートIP	stransaddr
4	GatewayIp	ゲートウェイのIP	gateway
5	MacAddress	MACアドレス	eth.src
6	OperatingSystem	Windowsエージェントで使用されているオペレーティングシステム	OS
7	AgentID	ホストのAgent ID(Agentに割り当てられた一意のID)	client
8	ConnectionUTCTime	エージェントが最後にECATサーバに接続した時刻	ecat.ctime

列	名前	説明	Security Analyticsでの列名(メタキー名)
9	Source Domain	Domain	domain.src
10	ScanUTC time	エージェントが前回スキャンされた時刻	ecat.stime
11	Machine Score	エージェントのスコア	risk.num

注: この表では、推奨されるインデックス設定は、LocalIpです。ただし、DHCPサーバによってECATエージェントPCのLocalIpが割り当てられるが、DHCPリースの有効期限が切れている場合、およびIPが別のPCに再割り当てされる場合は、Feedによって作成されるメタデータが不適切になります。このリスクを回避するには、localIPアドレスの代わりに、マシン名またはMACアドレスをFeedのインデックスとして使用します。たとえば、MACアドレスを使用する場合は、次の図に示されている値を入力できます。

The screenshot shows the 'Configure a Custom Feed' interface with the 'Define Columns' step active. In the 'Define Index' section, the 'Type' is set to 'Non IP' (circled in red), and the 'Index Column' is '5'. The 'Callback Key (5)' is set to 'eth.src' (circled in red). In the 'Define Values' table, the 'Column' 5 is set to 'stransaddr' (circled in red).

Column	1	2	3	4	5	6	7
Key	alias.host	ip.src	stransaddr	gateway	stransaddr	OS	client

Security Analytics Concentratorサービスの構成

1. Security Analyticsにログオンし、[Administration] > [サービス]に移動します。
2. リストからConcentratorを選択して、[表示] > [構成]を選択します。
3. [ファイル]タブを選択し、[編集するファイル]プルダウンメニューから、`index-concentrator-custom.xml`を選択します。
4. 次のECATメタキーをファイルに追加し、[適用]をクリックします。このファイルにはXMLセクションがすでに含まれることに注意してください。例を次に示します。構成と値がFeed定義に含まれる列名に一致することを確認してください。ここで、**description**は、Security Analytics Investigationで表示されるメタキー名です。**level**は「IndexValues」です。**name**は、繰り返しFeedを定義する際にSecurity Analyticsが使用するCSVファイルの列名と

一致します。

たとえば、次のように、メタ キーにインデックスを付けることができます。

```
<key description="Gateway" format="Text" level="IndexValues"
name="gateway" valueMax="250000" defaultAction="Open"/>
<key description="Risk Number" format="Float64" level="IndexValues"
name="risk.num" valueMax="250000" defaultAction="Open"/>
<key description="Strans Addr" format="Text" level="IndexValues"
name="stransaddr" valueMax="250000" defaultAction="Open"/>
<key description="Ecat Scan Time" format="Text" level="IndexValues"
name="ecat.stime" valueMax="250000" defaultAction="Open"/>
<key description="Ecat Connection Time" format="Text"
level="IndexValues" name="ecat.ctime" valueMax="250000"
defaultAction="Open"/>
```

注: デフォルトのファイル(index-concentrator.xml)でインデックスが付けられていないECAT Feed関連のメタ キーは、上の例に示すように、要件に従ってインデックスを付けることができます。

次の図は、すべてのECAT Feed関連のメタ キーのリストです。

列	名前	説明	Security Analyticsでの列名(メタ キー名)
1	MachineName	Windowsエージェントのホスト名	alias.host
2	LocalIp	IPv4アドレス	index
3	RemoteIp	ルーターで検出されるリモートIP	stransaddr
4	GatewayIp	ゲートウェイのIP	gateway
5	MacAddress	MACアドレス	eth.src
6	OperatingSystem	Windowsエージェントで使用されているオペレーティングシステム	OS
7	AgentID	ホストのAgent ID(Agentに割り当てられた一意のID)	client

列	名前	説明	Security Analyticsでの列名(メタキー名)
8	ConnectionUTCtime	エージェントが最後にECATサーバに接続した時刻	ecat.ctime
9	Source Domain	Domain	domain.src
10	ScanUTC time	エージェントが前回スキャンされた時刻	ecat.stime
11	Machine Score	エージェントのスコア	risk.num

5. Concentratorを再起動して、カスタム キーの更新をアクティブ化します。

結果

インデックスが付けられた値(ip.src)が一致したときに、FeedデータをSecurity Analyticsで表示する場合は、該当するメタデータが、Investigation、Reporting、Alertingの各インターフェイスに表示されるようになります。

トラブルシューティング

このセクションでは、繰り返しFeedの使用時に発生する問題の解決方法を提案します。

既知の問題	解決策
ECAT 4.1.0.2とECAT 4.1.1では、Security Analyticsに対してECAT Feedの統合が機能しません。	Feedを利用するには、ECAT 4.1.1.1を使用する必要があります。

Log DecoderへのSyslog経由のECATアラートの構成

このトピックでは、Security AnalyticsでRSA ECATデータを使用する方法を構成し、Syslog経由でECATアラートをLog Decoderセッションに提供するための手順について説明します。これにより、Security Analytics Investigation、Alerts、Reporting Engineで使用するメタデータが生成されます。

ログを収集および集計しているSecurity Analyticsネットワーク環境において、ECATとSecurity Analyticsとを統合し、ECATイベントをCEF(Common Event Format) 形式のSyslogメッセージとしてLog Decoderにプッシュし、Security Analytics Investigation、Alerts、Reporting Engineで使用可能なメタデータを生成できます。このユースケースはSIEM環境の統合です。イベントの一元管理を実現し、ECATイベントと他のLog Decoderデータとの相関分析、ECATイベントに関するSecurity Analyticsレポート作成、ECATイベントに関するSecurity Analyticsアラートの発行などが可能になります。

前提条件

この統合の要件を次に示します。

- バージョン4.0以降のECAT UI
- Security Analyticsサーババージョン10.4以降がインストールされている
- バージョン10.4以降のRSA Log DecoderおよびConcentratorがインストールされている
- ECATサーバからLog Decoderに対してポート514でアクセスできるようファイアウォールが構成されている

手順

この統合を構成するには、次のステップを実行します。

1. 必要なParser(CEFまたはECAT) をLog Decoderに導入します(「Live サービス管理」の「Liveリソースの管理」トピックを参照してください)。

注: Parserは1種類のみ使用します。CEF Parserが導入されている場合は、ECAT Parserより優先されます。Security Analyticsに送られるすべてのCEFメッセージがCEF Parserによって処理されます。両方のParserを有効にすると、パフォーマンスに不要な負荷がかかります。

2. ECAT側で、Syslog出力を構成し、ECATアラートを生成してLog Decoderに送信するよう設定します。
3. (オプション) `table-map-custom.xml`と`index-concentrator-custom.xml`でテーブルマッピングを編集し、Security Analyticsに割り当てるメタデータを必要に応じて追加します。

Syslog出力をSecurity Analyticsに送信するためのECATの構成

Log DecoderをSyslog外部コンポーネントとして追加し、ECATアラートを生成してLog Decoderに送信するには、次の手順を実行します。

ECATバージョン4.0の場合

1. ECATのユーザー インタフェースを開き、適切な認証情報を使用してログオンします。
2. メニュー バーから[Configure] > [Monitoring and External Components]を選択します。
3. ダイアログ ボックス内を右クリックして、[Add Component]を選択します。ダイアログ ボックスで、Syslogメッセージを有効にするために必要なフィールドに値を入力します。

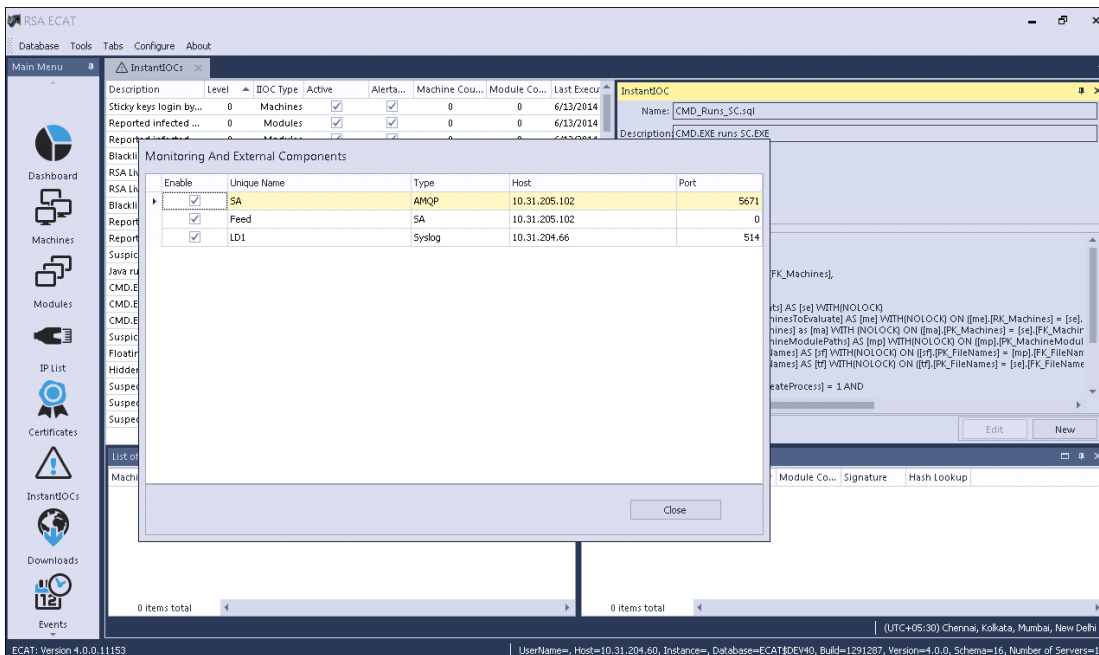
Component Type = Syslog

Unique Name = Log Decoderの記述名

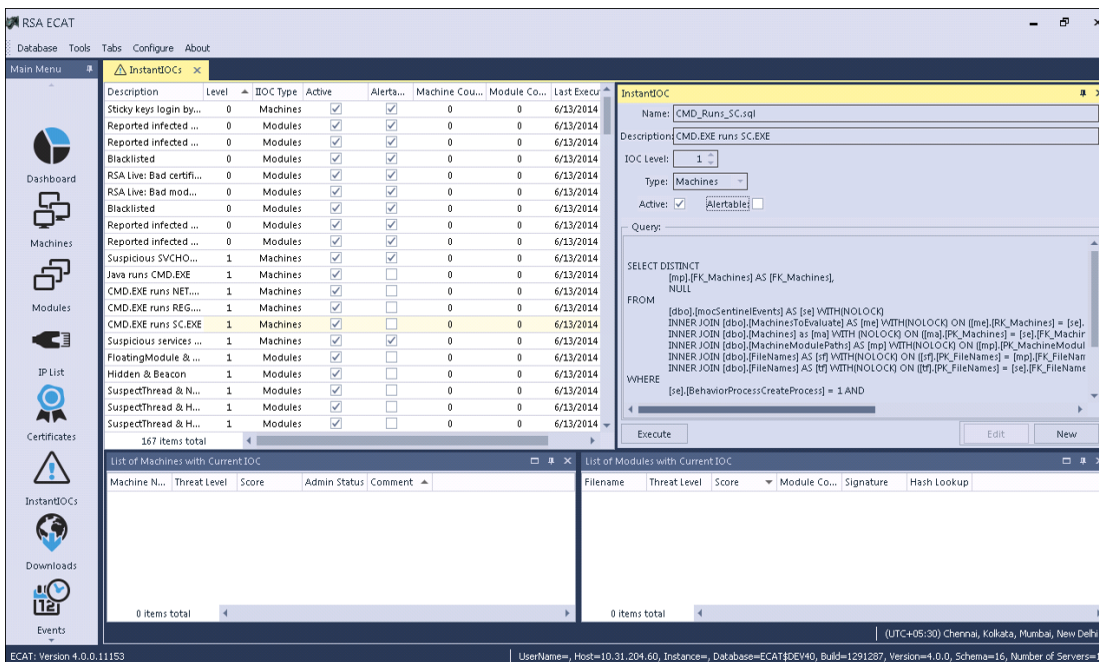
IP = RSA Log DecoderのIPアドレス

Port = 514

4. [Settings]をクリックします。
5. [Configure Syslog] ダイアログ ボックスで、Syslogサーバのトランスポート プロトコルとして[UDP]または[TCP]を選択します。
6. [Save]を2回クリックしてダイアログ ボックスを閉じます。
7. [Enable] チェックボックスをオンにしてコンポーネントを有効にします。
8. [Close]をクリックして終了します。



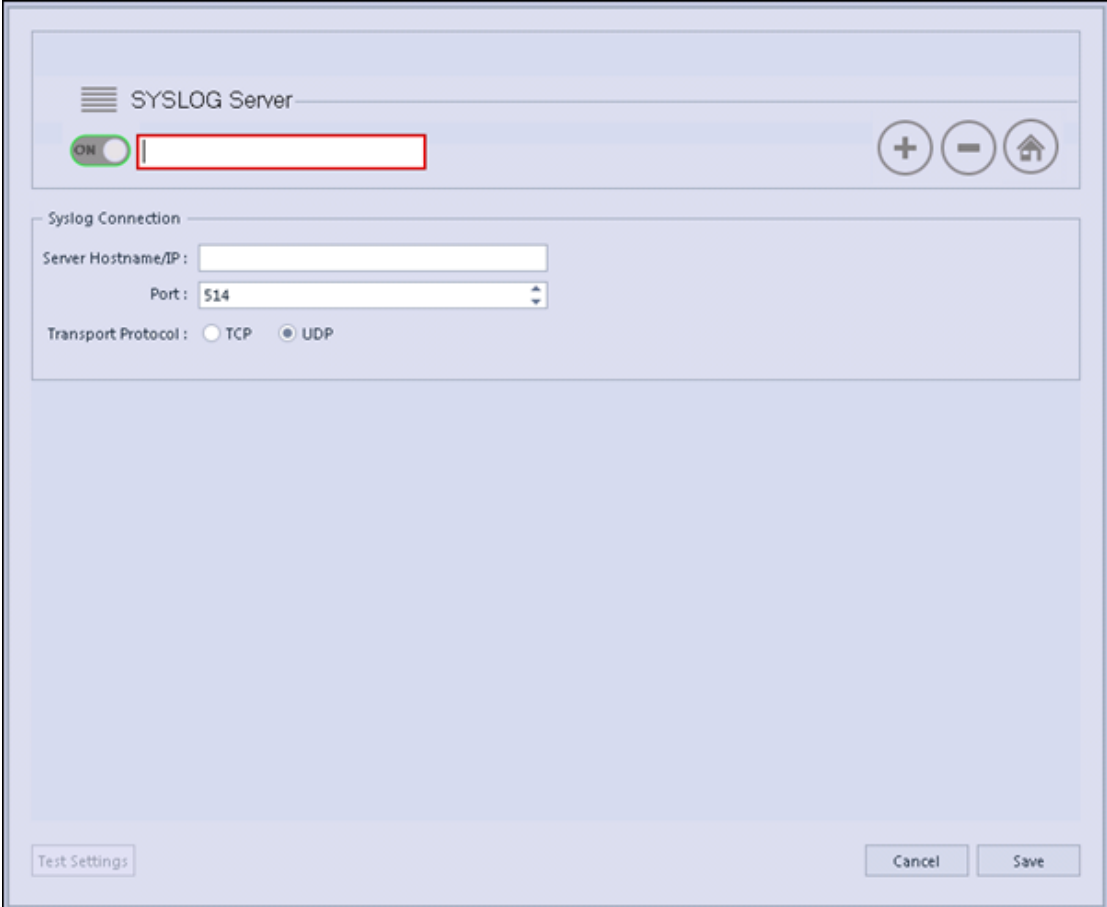
9. [Instant IOCs]をクリックして、アラート対象のIOCを設定します。



インスタントIOCがトリガーされると、SyslogアラートがECATサーバからLog Decoderに送信されます。その後で、Log DecoderアラートがConcentratorで集計されます。これらのイベントはConcentratorにメタデータとして挿入されます。

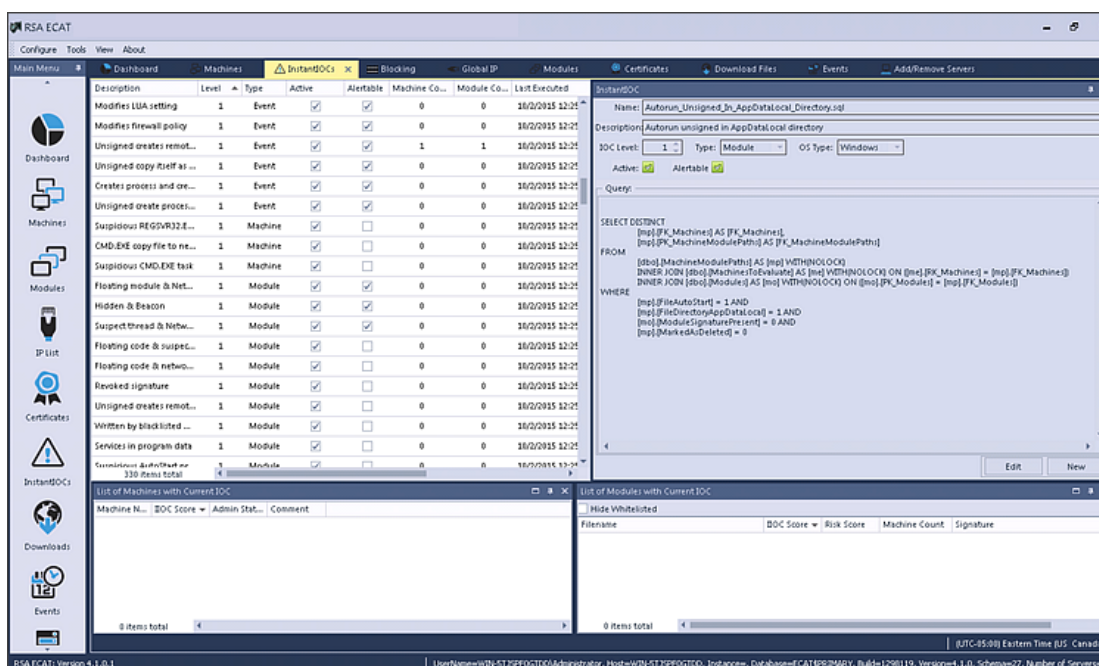
ECATバージョン4.1の場合

1. ECATのユーザー インタフェースを開き、適切な認証情報を使用してログオンします。
2. メニュー バーから[Configure] > [Monitoring and External Components]を選択します。
[External Components Configuration]ダイアログが表示されます。
3. [SYSLOG Server]で、[+]をクリックします。
[SYSLOG Serve]ダイアログが表示されます。



4. Syslogメッセージを有効にするために必要なフィールドに値を入力します。
On = Log Decoderの記述名
Server Hostname/IP = RSA Log Decoderのホスト名またはIPアドレス
Port = 514
Transport Protocol=Syslogサーバの転送プロトコルとして[UDP]または[TCP]を選択します。
5. **Save**をクリックします。

6. [Instant IOCs]をクリックして、アラート対象のIOCを設定します。



インスタントIOCがトリガーされると、SyslogアラートがECATサーバからLog Decoderに送信されます。その後で、Log DecoderアラートがConcentratorで集計されます。これらのイベントはConcentratorにメタデータとして挿入されます。

table-map-custom.xmlでのテーブルマッピングの編集

RSAが提供するデフォルトのtable-map.xmlファイルでは、メタキーはTransientに設定されています。メタキーをInvestigationで表示するには、キーがNoneに設定されている必要があります。マッピングに変更を加えるには、Log Decoderでtable-map-custom.xmlという名前でのファイルのコピーを作成して、メタキーをNoneに設定する必要があります。

以下は、table-map.xml内のメタキーのリストです。

ECATフィールド	Security Analyticsのマップ	Security AnalyticsのTransient設定
agentid	client	×
CEF Header Hostname Field	alias.host	×
CEF Header Product Version	version	○

ECATフィールド	Security Analyticsのマッピング	Security AnalyticsのTransient設定
CEF Header Product Name	product	○
CEF Header Severity	Severity	○
CEF Header Signature ID	event.type	×
CEF Header Signature Name	event.desc	×
destinationDnsDomain	ddomain	○
deviceDnsDomain	DOMAIN	○
dhost	host.dst	×
dst	ip.dst	×
end	endtime	○
fileHash	checksum	○
fname	filename	×
fsize	filename.size	×
gatewayip	gateway	○
instantIOCLLevel	threat.desc	×
instantIOCName	threat.category	○
machineOU	dn	○
machineScore	risk.num	×
md5sum	checksum	○

ECATフィールド	Security Analyticsのマッピング	Security AnalyticsのTransient設定
os	OS	○
port	ip.dstport	×
protocol	protocol	○
Raw Message	msg	○
remoteip	stransaddr	○
rt	alias.host	×
sha256sum	checksum	○
shost	host.src	×
smac	eth.src	○
src	ip.src	×
start	starttime	○
suser	user.dst	×
timezone	timezone	○
totalreceived	rbytes	○
totalsent	bytes.src	×
useragent	user.agent	○
userOU	org	○

以下の7個のキーはtable-map.xmlに含まれていません。これらのキーをSecurity Analyticsで使用するには、キーをtable-map-custom.xmlに追加して、フラグをNoneに設定する必要があります。

ECATフィールド	Security Analyticsのマッピング	Security AnalyticsのTransient設定
moduleScore	cs.modulescore	○
moduleSignature	cs.modulesign	○
Target module	cs.targetmodule	○
YARA result	cs.yarareult	○
Source module	cs.sourcemodule	○
OPSWATResult	cs.opswatresult	○
ReputationResult	cs.reputationresult	○

必要な場合は、以下のエントリーをtable-map-custom.xmlに追加します。

```
<mapping envisionName="cs_reputationresult" nwName="cs.reputationresult"
flags="None" envisionDisplayName="ReputationResult"/>
<mapping envisionName="cs_modulescore" nwName="cs.modulescore" format="Int32"
flags="None" envisionDisplayName="ModuleScore"/>
<mapping envisionName="cs_modulesign" nwName="cs.modulesign" flags="None"
envisionDisplayName="ModuleSignature"/>
<mapping envisionName="cs_opswatresult" nwName="cs.opswatresult" flags="None"
envisionDisplayName="OpswatResult"/>
<mapping envisionName="cs_sourcemodule" nwName="cs.sourcemodule" flags="None"
envisionDisplayName="SourceModule"/>
<mapping envisionName="cs_targetmodule" nwName="cs.targetmodule" flags="None"
envisionDisplayName="TargetModule"/>
<mapping envisionName="cs_yarareult" nwName="cs.yarareult" flags="None"
envisionDisplayName="YaraResult"/>
```

注：Log Decoderを再起動するか、ログParserを再ロードすることによって、変更を有効にします。

Security Analytics Concentratorサービスの構成

1. Security Analyticsにログオンし、[Administration] > [サービス]に移動します。
2. リストからConcentratorを選択して、[表示] > [構成]を選択します。
3. [ファイル]タブを選択し、[編集するファイル]プルダウンメニューから、index-concentrator-custom.xmlを選択します。

4. ECATメタ キーをファイルに追加して、[適用]をクリックします。このファイルにはXMLセクションがすでに含まれることに注意してください。
5. Concentratorを再起動します。
6. Reporting Engineのデータ ソースとしてConcentratorを追加するには、[Administration] > [サービス]ビューで、[Reporting Engine] > [表示] > [構成] > [ソース]を選択します。ECATのメタがReporting Engineに提供されるため、適切なメタ キーを選択して、レポートを実行できます。

例

注: 以下に示す行は、例です。使用環境に合わせて値を調整してください。各項目の意味は次のとおりです。

descriptionは、Security Analytics Investigationで表示されるメタ キー名です。

levelは「IndexValues」です。

nameは、下の表に示されるECATメタ キー名です。

```
<language>
<key description="Product" format="Text" level="IndexValues" name="product"
valueMax="250000" defaultAction="Open"/>
  <key description="Severity" format="Text" level="IndexValues" name="severity"
valueMax="250000" defaultAction="Open"/>
  <key description="Destination Dns Domain" format="Text" level="IndexValues"
name="ddomain" valueMax="250000" defaultAction="Open"/>
  <key description="Domain" format="Text" level="IndexValues" name="domain"
valueMax="250000" defaultAction="Open"/>
  <key description="Destination Host" format="Text" level="IndexValues"
name="host.dst" valueMax="250000" defaultAction="Open"/>
  <key description="End Time" format="TimeT" level="IndexValues" name="endtime"
valueMax="250000" defaultAction="Open"/>
  <key description="Checksum" format="Text" level="IndexValues" name="checksum"
valueMax="250000" defaultAction="Open"/>
  <key description="Filename Size" format="Int64" level="IndexValues"
name="filename.size" valueMax="250000" defaultAction="Open"/>
  <key description="Gateway" format="Text" level="IndexValues" name="gateway"
valueMax="250000" defaultAction="Open"/>
  <key description="Distinguished Name" format="Text" level="IndexValues" name="dn"
valueMax="250000" defaultAction="Open"/>
  <key description="Risk Number" format="Float64" level="IndexValues"
name="risk.num" valueMax="250000" defaultAction="Open"/>
  <key description="ReputationResult" format="Text" level="IndexValues"
name="cs.reputationresults" valueMax="250000" defaultAction="Open"/>
  <key description="Module Score" format="Text" level="IndexValues"
name="cs.modulescore" valueMax="250000" defaultAction="Open"/>
  <key description="Module Sign" format="Text" level="IndexValues"
name="cs.modulesign" valueMax="250000" defaultAction="Open"/>
  <key description="opswat result" format="Text" level="IndexValues"
name="cs.opswatresult" valueMax="250000" defaultAction="Open"/>
  <key description="source module" format="Text" level="IndexValues"
```



```

name="cs.sourcemodule" valueMax="250000" defaultAction="Open"/>
  <key description="Target Module" format="Text" level="IndexValues"
name="cs.targetmodule" valueMax="250000" defaultAction="Open"/>
  <key description="yara result" format="Text" level="IndexValues"
name="cs.yarareult" valueMax="250000" defaultAction="Open"/>
  <key description="Protocol" format="Text" level="IndexValues" name="protocol"
valueMax="250000" defaultAction="Open"/>
  <key description="Event Time" format="TimeT" level="IndexValues"
name="event.time" valueMax="250000" defaultAction="Open"/>
  <key description="Source Host" format="Text" level="IndexValues" name="host.src"
valueMax="250000" defaultAction="Open"/>
  <key description="Start Time" format="TimeT" level="IndexValues" name="starttime"
valueMax="250000" defaultAction="Open"/>
  <key description="Timezone" format="Text" level="IndexValues" name="timezone"
valueMax="250000" defaultAction="Open"/>
  <key description="Received Bytes" format="UInt64" level="IndexValues"
name="rbytes" valueMax="250000" defaultAction="Open"/>
  <key description="Agent User" format="Text" level="IndexValues" name="user.agent"
valueMax="250000" defaultAction="Open"/>
  <key description="Source Bytes" format="UInt64" level="IndexValues"
name="bytes.src" valueMax="250000" defaultAction="Open"/>
  <key description="Strans Address" format="Text" level="IndexValues"
name="stransaddr" valueMax="250000" defaultAction="Open"/>
</language>

```

ECATメタキー

以下は、サンプル インデックス ファイルで使用されるECATメタキー名と説明です。

Security Analyticsの メタキー名	意味	ECATメタキー (名前)
MachineName	Windowsエージェントのホスト名	alias.host
LocalIp	IPv4アドレス	index
RemoteIp	ルーターで検出されるリモートIP	stransaddr
GatewayIp	ゲートウェイIP	gateway
MacAddress	MACアドレス	eth.src
OperatingSystem	Windowsエージェントで使用されているオペレーティングシステム	OS

Security Analyticsの メタキー名	意味	ECATメタキー (名前)
AgentID	ホストのAgent ID(Agentに割り当てられた一意のID)	client
ConnectionUTCtime	エージェントが前回ECATサーバに接続した時刻	ecat.ctime
Source Domain	Domain	domain.src
ScanUTC time	エージェントが前回スキャンされた時刻	ecat.stime
Machine Score	エージェントがどの程度疑わしいかを示すスコア	risk.num

結果

アナリストは次の操作を実行できます。

- ECATイベントをエンリッチメント ソースとして構成することにより、ECATイベントに基づいて Security Analyticsアラートを作成する。
- ECATメタを使用してESAルールを作成する(「*ESA*を使用したアラート」の「**ルールライブラリへのルールの追加**」トピックを参照)。
- ECATメタを使用してECATイベントに関するレポートを作成する(「**レポート作成**」の「**レポート ルールの使用**」トピックを参照)。
- ECATアラートをIncident Managementで表示する(「*Incident Management*」の「**[アラート] ビュー**」トピックを参照)。
- 標準のSAメタキーとともにECATメタキーをInvestigationで表示する(「*Investigation*および *Malware Analysis*」の「**調査の実施**」トピックを参照)。