

# **RSA** Security Analytics

RSA ECATとの統合ガイド バージョン 10.6





Copyright © 2016 EMC Corporation. All rights reserved.

#### 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/emccorporation-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。

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

Syslog出力をSecurity Analyticsに送信するためのECATの構成
ECATバージョン4.0の場合
ECAT <b>バージョン</b> 4.1の場合
table man custom xmlでのテーブル マッピングの編集 36
table-map-custom.xmi CO// ジルマノビングの編末
Security Analytics Concentratorサービスの構成
例
ECATメタ キー
結果

# 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, ipdst, 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実行します。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があることを示しており、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んでいます。
- 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、前述のカテゴリー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

- <u>RSA Live Feedを受信するためのECATの構成</u>
- <u>メッセージ バス経由のECATアラートの構成</u>
- 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
- <u>Log DecoderへのSyslog経由のECATアラートの構成</u>

# 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。
- 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。
- 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。
- [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それぞれ異なり、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。

	SYSLOG Server Syslog is widely used standard for message logging. Multiple Syslog servers may be	
•	added to configuration and alerts will be sent to each enabled Syslog server.	
	RSA Live RSA Live is a threat intelligence delivery system that benefits your security team by reducing the time it takes to identify, assess, and respond to incidents.	(+)
	SMTP Configuration SMTP (email) messages can be configured and will be sent if the option is enabled	(*) <b>(+</b> )
لأشرو	when a computer reaches a certain score.	
$\hat{\square}$	Incident Message Broker ECAT alerts can also be sent to RSA SA Incident Management (IM).	<b>()</b> +
	NadiaGanaga	
ioi	RSA NetWitness v9.7 (previous version of RSA Security Analytics) is a network security monitoring platform that provides visibility and situational awareness about what's	+
	Security Analytics	

4. [RSA Live]ダイアログが表示されます。

	A Live					+	
RSA Live Settings	i		Convertigence (7)				
Osername :			Server Hostname/IP :				
Password :			Port :	443		÷	
Feed Name	Subscribed	Count		Err	or Message		
Malware Domai				0	or message	1	1/1/0001 12:00:
Malware Domai Malware Domai				0	of Message	1	1/1/0001 12:00: 4 1/1/0001 12:00:
Malware Domai Malware Domai Malware IP List				0	or message	1	Last Updated L/1/0001 12:00: 4 L/1/0001 12:00: L/1/0001 12:00:
Malware Domai Malware Domai Malware IP List RSA FirstWatch				0 0 0 0 0 0	o message	1	Last Updated 1/1/0001 12:00: 1/1/0001 12:00: 1/1/0001 12:00: 1/1/0001 12:00:
Malware Domai Malware Domai Malware IP List RSA FirstWatch RSA FirstWatch RSA FirstWatch				0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	of incode		Last Updated 1/1/0001 12:00: 1/1/0001 12:00: 1/1/0001 12:00: 1/1/0001 12:00: 1/1/0001 12:00:
Mahware Domai Mahware Domai Mahware IP List RSA FirstWatch RSA FirstWatch RSA FirstWatch RSA FirstWatch				0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	of message		1350 Updated         1/1/0001 12:00:         1/1/1/0001 12:00:         1/1/1/0001 12:00
Malware Domai Malware Domai Malware IP List RSA FirstWatch RSA FirstWatch RSA FirstWatch RSA FirstWatch RSA FirstWatch				0 0 0 0 0 0 0 0 0	of message		13:t Updated           1/1/0001 12:00:           1/1/0001 12:00:           1/1/10001 12:00:           1/1/0001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/0001 12:00:
Malware Domai Malware Domai Malware ID List RSA FirstWatch RSA FirstWatch RSA FirstWatch RSA FirstWatch RSA FirstWatch RSA FirstWatch				0 0 0 0 0 0 0 0 0 0 0			131 Updated           1/1/0001 12:00:           1/1/0001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:
Malware Domai Malware Domai Malware IP List RSA FirstWatch RSA FirstWatch RSA FirstWatch RSA FirstWatch RSA FirstWatch RSA FirstWatch RSA FirstWatch				0 0 0 0 0 0 0 0 0 0 0 0 0			135t Updated           1/1/0001 12:00:           1/1/0001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:
Malware Domai Malware Domai Malware IP List RSA FirstWatch RSA FirstWatch RSA FirstWatch RSA FirstWatch RSA FirstWatch RSA FirstWatch RSA FirstWatch RSA FirstWatch RSA FirstWatch RSA FirstWatch							135t Updated           1/1/0001 12:00:           1/1/0001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:
Malware Domai Malware Domai Malware IP List RSA FirstWatch RSA FirstWatch							135t Updated           1/1/0001 12:00:           1/1/0001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/10001 12:00:           1/1/0001 12:00:           1/1/0001 12:00:           1/1/0001 12:00:           1/1/0001 12:00:
Malware Domai Malware Domai Malware Domai Malware IP List RSA FirstWatch RSA FirstWatch RSA FirstWatch RSA FirstWatch RSA FirstWatch RSA FirstWatch RSA FirstWatch RSA FraudActio RSA FraudActio Taur Domain Tr 14 items tot							1/1/10001         12:00:           1/1/10001         12:00:           1/1/10001         12:00:           1/1/10001         12:00:           1/1/10001         12:00:           1/1/10001         12:00:           1/1/10001         12:00:           1/1/10001         12:00:           1/1/10001         12:00:           1/1/10001         12:00:           1/1/10001         12:00:           1/1/0001         12:00:           1/1/0001         12:00:

- 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。
  - a. [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。
  - b. [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。
  - c. [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。
  - a. [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	Zeusトラッカーは、世界中のzeus(zbot、 prg、wsnpoem、gorhax、kneberとも呼ば れます)に関係するコマンド&コントロール サーバ(ホスト)のIPアドレスのリストです。 Zeusトラッカーでは、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ドメイントラッカーは、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。Zeusトラッカーでは、 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 な出ロ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のユーザーインタフェースを開き、適切な認証情報を使用してログインします。
- 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のユーザーインタフェースを開き、適切な認証情報を使用してログインします。
- 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。

	×
Security Analytics Connection	+ -
Port: 0 \$	
Test Settings	Cancel Save

- 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 カします。
- 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。

 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ー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 スポートします。

- 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
- 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。
- 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。

- 1. 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。
- 2. 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 ストアにインポートします。
- 3. 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 Se	ecurity Analytics]ダイアログが表示されます。
RSA ECAT	
Ataria Manu 2 Dahibeard Madaines Madaires Plut Plut Certificates	Configure Security Analytics Configure Security Analytics Server Time Zoor [UT-09:00] Alwas Device ServerTime Zoor [UT-09:00] Alwas Util http://23.32.244.336/nevettogation/ - Query Optimization Minimum Query Time Raingrifts usule a used to automatically increase the time and a flock_apprivation for the single automatically increase the time and a flock_apprivation for the single automatically increase the time and a flock_apprivation for the single automatically increase the time and a flock_apprivation for the single automatically increase the time and a flock_apprivation for the single automatically increase the time and a flock_apprivation for the single automatically increase the time and a flock_apprivation for the single automatically into the time and a flock_apprivation for the single automatically into the time and a flock_apprivation for the single automatically into the time and a flock_apprivation for the single automatically into the time and a flock_apprivation for the single automatically into the time and a flock_apprivation for the single automatically into the time and a flock_apprivation for the single automatically into the time and a flock_apprivation flock automatically into the time automatical flock automatically into the single automatically into the time automatical flock automatically into the single automatically into the time automatical flock automatically into the time automatical flock automatically into the single automatically into the time automatical flock automatically into the single automatically into the time automatical flock automatically into the single automatically into the time automatical flock automatically into the single automatically into the time automatical flock automatically into the single automatically into the time automatical flock automatically into the time time automatically into the time automatical flock automatical flock automatically into the time automatical flock automatically into the time automatically into the
InstantiOCs	Do hot Purform Quary Older That The use will be a given provide to the given must be accord to the given must be a
Events	

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。

292art 选 🗾 🧮 曼 🔤 👯 🐼 🏈 🔍 🕅

🖉 RSA ECAT	- Ø ×
Configure Tools Tabs About	
Configure Text Table About  The About  Configure Security Analytics  Configure Security Analytic	222 Port 223 540 5171 Close
Configuration	
RSA ECAT: Version 4.0.0.0	UserName=Administrator, Host=localhost, Instance=, Database=ECAT#PRIMARY, Build=1293025, Version=4.0.0, Schema=22, Number of Servers=1
Arent 🐉 😰 🎇 😻 🖬 👯 🛤 🐓 😒 🐖	* 👍 💬 🔁 5551 PM 📼

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。

	×
Create a new S	SQL User
Login Name: Password: Confirm Password:	ecatuser

- 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。

			×
External	Components Configuration		
	SYSLOG Server Syslog is widely used standard for message logging. Multiple Syslog servers may be added to configuration and alerts will be sent to each enabled Syslog server.	+	
	RSA Live RSA Live is a threat intelligence delivery system that benefits your security team by reducing the time it takes to identify, assess, and respond to incidents.	+	
	SMTP Configuration SMTP (email) messages can be configured and will be sent if the option is enabled when a computer reaches a certain score.	+	
$\hat{\square}$	Incident Message Broker ECAT alerts can also be sent to RSA SA Incident Management (IM).	+	
tor	NetWitness RSA NetWitness v9.7 (previous version of RSA Security Analytics) is a network security monitoring platform that provides visibility and situational awareness about what's	+	
ᢙ	Security Analytics RSA Security Analytics (formerly RSA NetWitness) is a security-monitoring platform that combines network monitoring, traditional log-centric SIEM, forensics, and bi	+	

3. Security Analyticsで、[+]をクリックします。

[Security	<sup>y</sup> Analytics]タ	イアログが表	示されます。
-----------	--------------------------	--------	--------

Security Analytics	+
Server Hostname/IP: Port: 443	
Configure Security Analytics Servers Time Zone (UTC-11:00) Coordinated Universal Time-11 * Device Identifier URI Query Optimization Query Time Range Min : 0 \$ minutes Max : 30 \$ minutes Do Not Perform Query Older Than 0 \$ days *Set 0 to query all.	Configure ECAT Feeds for SA Enable ECAT Feed Username Password URL Feed Publishing Interval Time Interval: 0  Hrs 30  min

- 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
- 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。

	Define Fee	d	Select Services	Define Columns		Review		
Trigger	Feed Task Type	O Adhor	Recurring					
Starting a	Name *	ECATFEED	e neconnig				5:12:56	
	URL *	https://Ecat	ServerExported:9443/ext/f	eed/machines.csv		Verify 🧉		
Starting at		Authentica	ated User Name sa	Password *	*****		0:12:30	
		Use proxy						
		· · ·						
	Recur Every	2 🗘 Mi	inute (s) 💙					
	— 📀 Date Range							
	- O Advanced O	puons						

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。

Trigger	Define	Feed	56	elect Service	es	Define Columns		Revie	ew		
Starting a	Define Ind	ex								5:14:56	
	Туре		● IP	○ IP Range	O Non I	>					
Starting at	Index Colu	ımn	2 🖌	CIDR						5:14:30	
	Define Val	105									
	Column	1		2 (Index)		3		4			
	Key	alias.hos	t	~		stransaddr	~	gateway			
		WIN2K8-	-60	10.31.20	04.60	10.31.204.60		10.31.204.1			
	1								•		

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 <i>キー</i> 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。

Configu	ure a Custom Fee	ed						
		Define Feed	Select Servic	es Define (	Columns	Review		
Define Ind Type Index Colu Callback K	Define Index Type IP IP Range Non IP Index Column 5 Service Type 1 Truncate Domain Callback Key (5) eth.src							
Column	1	2	3	4	5 (Index)	6	7	
Кеу	alias.host	ip.src 🗸	stransaddr 🗸 🗸	gateway 🗸		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-concentratorcustom.xmlを選択します。
- 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 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。

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

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 <i>キー</i> 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	Feedを利用するには、ECAT 4.1.1.1
対してECAT Feedの統合が機能しません。	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。

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。

🕅 RSA ECAT									- d <sup>3</sup> ×
Database Tools	Tabs Configure Abo	ut							
Main Menu 🛛 🕸	🛆 InstantIOCs 🗙								
<u> </u>	Description	Level	🔺 ІІОС Туре	Active	Alerta	Machine Cou	Module Co	Last Execu 🚖	InstantIOC # ×
	Sticky keys login by	0	Machines	$\checkmark$	$\checkmark$	0	0	6/13/2014	Name: CMD_Runs_SC.sql
	Reported infected	0	Modules	$\checkmark$	$\checkmark$	0	0	6/13/2014	
	Reported infected	0	Modules	$\checkmark$	$\checkmark$	0	0	6/13/2014	Description CMD.EXE runs SC.EXE
	Blacklisted	0	Modules	$\checkmark$	$\checkmark$	0	0	6/13/2014	IOC Level: 1 🗘
Dashboard	RSA Live: Bad certifi	0	Modules	$\checkmark$	$\checkmark$	0	0	6/13/2014	Type: Machines 🐨
	RSA Live: Bad mod	0	Modules	$\checkmark$	$\checkmark$	0	0	6/13/2014	
	Blacklisted	0	Modules	$\checkmark$	$\checkmark$	0	0	6/13/2014	Active: V Alertable:
<u> </u>	Reported infected	0	Modules	$\checkmark$	✓	0	0	6/13/2014	Query:
Machines	Reported infected	0	Modules	$\checkmark$	~	0	0	6/13/2014	<u> </u>
5	Suspicious SVCHO	1	Machines	$\checkmark$	✓	0	0	6/13/2014	SELECT DISTINCT
· ۲۰	Java runs CMD.EXE	1	Machines	✓		0	0	6/13/2014	[mp].[FK_Machines] AS [FK_Machines],
_	CMD.EXE runs NET	1	Machines			0	0	6/13/2014	FROM
Modules	CMD.EXE runs REG	1	Machines			0	0	6/13/2014	[dbo].[mocSentinelEvents] AS [se] WITH(NOLOCK)
<b>A</b> 3	CMD.EXE runs SC.EXE	1	Machines			0	0	6/13/2014	INNER JOIN (dbo), [Machines] os [ma] WITH [NOLOCK] ON [[ma], [KK_Machines] = [se]. INNER JOIN (dbo), [Machines] as [ma] WITH [NOLOCK] ON [[ma], [PK_Machines] = [se], [FK_Machines]
	Suspicious services	1	Machines	Image: A state of the state		0	0	6/13/2014	INNER JOIN [dbo].[MachineModulePaths] AS [mp] WITH(NOLOCK) ON [[mp].[PK_MachineModul
10114	FloatingModule &	1	Modules	✓		0	0	6/13/2014	INNER JOIN (dbo),[Hienames] AS [st] WITH(NOLOCK) ON [[st],[PK_Hienames] = [mp],[PK_Hiename INNER JOIN (dbo),[FileNames] AS [tt] WITH(NOLOCK) ON ([tt],[PK_FileNames] = [se],[FK_FileName
IP LIST	Hidden & Beacon	1	Modules	Image: A state of the state		0	0	6/13/2014	WHERE
	SuspectInread & N	1	Modules	✓		0	0	6/13/2014	[se].[BehaviorProcessCreateProcess] = 1 AND
	Suspectinread & H	1	Modules	Image: A state of the state		0	Ű	6/13/2014	
Certificates	Suspectinread & H	. 1	Modules	¥.		U	U	6/13/2014 -	Execute Edit New
^	List of Machines with	ll Curren	tor					LX List of	Modules with Current IOC
					4				
Instantiocs	Machine N Inreat	Level	Score	Admin Star	us Commen	(C 🔺		Filena	ne Inreat Level Score 👻 Module Co Signature Hash Lookup
InstantiOCs									
· • •									
Downloads									
								_	
	0 items total	4						•	Jitems total 🔸 🔸
Events									(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
ECAT: Version 4.0.0.	1153						UserNa	ne=, Host=10	31.204.60, Instance=, Database=ECAT\$DEV40, Build=1291287, Version=4.0.0, Schema=16, Number of Servers=1

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。

	G Server		(+)(=)(\$)
			000
<ul> <li>Syslog Connection –</li> </ul>			
Server Hostname/IP :			
Port :	514	÷	
Transport Protocol :	O TCP		

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。

figure Tools	View About															
Menu 🔻	Dashboard 8	Mathines	4	LinstantiOCs	× ==	locking	🖝 Global IP	🖉 Modules	🙁 Ce	entificates	S Sownload Files	😴 Events	💻 Add/Remove Serv	ers		
	Description	Level 🔺	Type	Active	Alertable	Machine Co	Module Co	Last Executed	Instant00	к						
	Modifies LUA setting	1	Event	2	2	0	0	10/2/2015 12:25	Name	e: Autori	un_Unsigned_In_AppDataL	ocal_Directory.sql				
	Modifies firewall policy	1	Event	2	1	0	0	10/2/2015 12:25	Descriptio	Auton	un unsigned in AppDataLo	cal directory				
withheard	Unsigned creates remot	1	Event	2	2	1	1	10/2/2015 12:25	10C Leve	:t 🚺	C Type: Module	<ul> <li>OS Type: Windo</li> </ul>	wd -			
Shipbard	Unsigned copy itself as	1	Event	×	2	0	0	10/2/2015 12:25	Active	e: 📶	Alertable 💋					
- L	Creates process and cre	1	Event	2	1	0	0	10/2/2015 12:25	Query							
	Unsigned create proces	1	Event	2	×	0	0	10/2/2015 12:25								^
thines	Suspidious REGSVR32.E	1	Machine			0	0	10/2/2015 12:25	SELECT D	Imp].(FK)	(Machines) AS (FK, Machine	ц.				
	CMD.EXE copy file to ne	1	Machine			0	0	10/2/2015 12:25	FROM	(mp).(PK	(MachineModulePaths) AS	FK_MachineModulePat	hal			
ר נ	Suspicious CMD.EXE task	1	Machine	2		0	0	10/2/2015 12:25		[dbo].[M INNER J	fachineModulePaths] AS (m OIN (dbo).[MachinesToEval	p] WETH(NOLOCK) rate] AS [me] WETH(NOL)	OCK) ON [[me].[RK_Mach	ines) = (mp).(FK_Mi	(thines)	
dules	Floating module & Net	1	Module	2	1	0	0	10/2/2015 12:25	WHERE	INNER J	ODV [dbo].[Modules] AS [mo	I MITHINOLOCKI ON ER	vo].[PK_Modules] = [mp]	[FK_Modules]]		
-	Hidden & Beacon	1	Module	Z	×	0	0	10/2/2015 12:25		[mp].(File [mp].(File	leAutoStart] = 1 AND leDirectoryAppDataLocal] =	1 AND				
	Suspect thread & Netw	1	Module		1	0	0	10/2/2015 12:25		[mo].[Mo [mp].[Ma	oduleSignaturePresent] = 0 arkedAsDeleted] = 0	AND				
ist.	Floating code & suspec	1	Module	2		0	0	10/2/2015 12:25								
	Floating code & netwo	1	Module	2		0	0	10/2/2015 12:25								
	Revoked signature	1	Module	2		Ó	0	10/2/2015 12:25								
	Unsigned creates remot	1	Module	×.		0	0	10/2/2015 12:25								
100	Written by blacklisted	1	Module			0	0	10/2/2015 12:25								
$\langle  $	Services in program data	1	Module	×		0	0	10/2/2015 12:25	4							
2	Supplement AutoStart or 330 items total	1	Modula	2		0	n	10/0/0015 10-04	-					Edit	N	New
4003	List of Machines with Cur	rent10C						= * ×	List of Modul	les with C	urrent IOC					
3	Machine N BOC Score	+ Admin	Stat Co	mment					Hide White	elisted						
<b>V</b>									Filename		B	C Score 👻 Risk Score	Machine Count Si	gnature		
wnloads																
u 🕥 🛛																
Ľ۲ (																
vents																
									de laterative et	to the	4				And in case of	

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。

× 1 10, cable map. xml 1 1000 / V V/V C 7 0							
ECATフィールド	Security Analyticsのマッ ピング	Security Analyticsの Transient設定					
agentid	client	×					
CEF Header Hostname Field	alias.host	×					
CEF Header Product	version	0					

以下は、table-map.xml内のメタキーのリストです。

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	0
CEF Header Severity	Severity	0
CEF Header Signature ID	event.type	×
CEF Header Signature Name	event.desc	×
destinationDnsDomain	ddomain	0
deviceDnsDomain	DOMAIN	0
dhost	host.dst	×
dst	ip.dst	×
end	endtime	0
fileHash	checksum	0
fname	filename	×
fsize	filename.size	×
gatewayip	gateway	0
instantIOCLevel	threat.desc	×
instantIOCName	threat.category	0
machineOU	dn	0
machineScore	risk.num	×
md5sum	checksum	0

ECATフィールド	Security Analyticsのマッ ピング	Security Analyticsの Transient設定
OS	OS	0
port	ip.dstport	×
protocol	protocol	0
Raw Message	msg	0
remoteip	stransaddr	0
rt	alias.host	×
sha256sum	checksum	0
shost	host.src	×
smac	eth.src	0
src	ip.src	×
start	starttime	0
suser	user.dst	×
timezone	timezone	0
totalreceived	rbytes	0
totalsent	bytes.src	×
useragent	user.agent	0
userOU	org	0

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	0
moduleSignature	cs.modulesign	0
Target module	cs.targetmodule	0
YARA result	cs.yararesult	0
Source module	cs.sourcemodule	0
OPSWATResult	cs.opswatresult	0
ReputationResult	cs.reputationresult	0

#### 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_yararesult" nwName="cs.yararesult" 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-concentratorcustom.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。
- 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="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.yararesult" valueMax="250000" defaultAction="Open"/>
 <key description="Protocol" format="Text" level="IndexValues" name="protocol"</pre>
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

Security Analyticsの メタ <i>キー</i> 名	意味	ECATメタ <i>キー</i> (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

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 <i>キー</i> 名	意味	ECATメタ <i>キー</i> (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)。