

RSA Security Analytics

Intégration de RSA ECAT
pour la Version 10.6

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of EMC trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm.

License Agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability. This software is subject to change without notice and should not be construed as a commitment by EMC.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed in the [thirdpartylicenses.pdf](#) file.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license. EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intégration de RSA ECAT

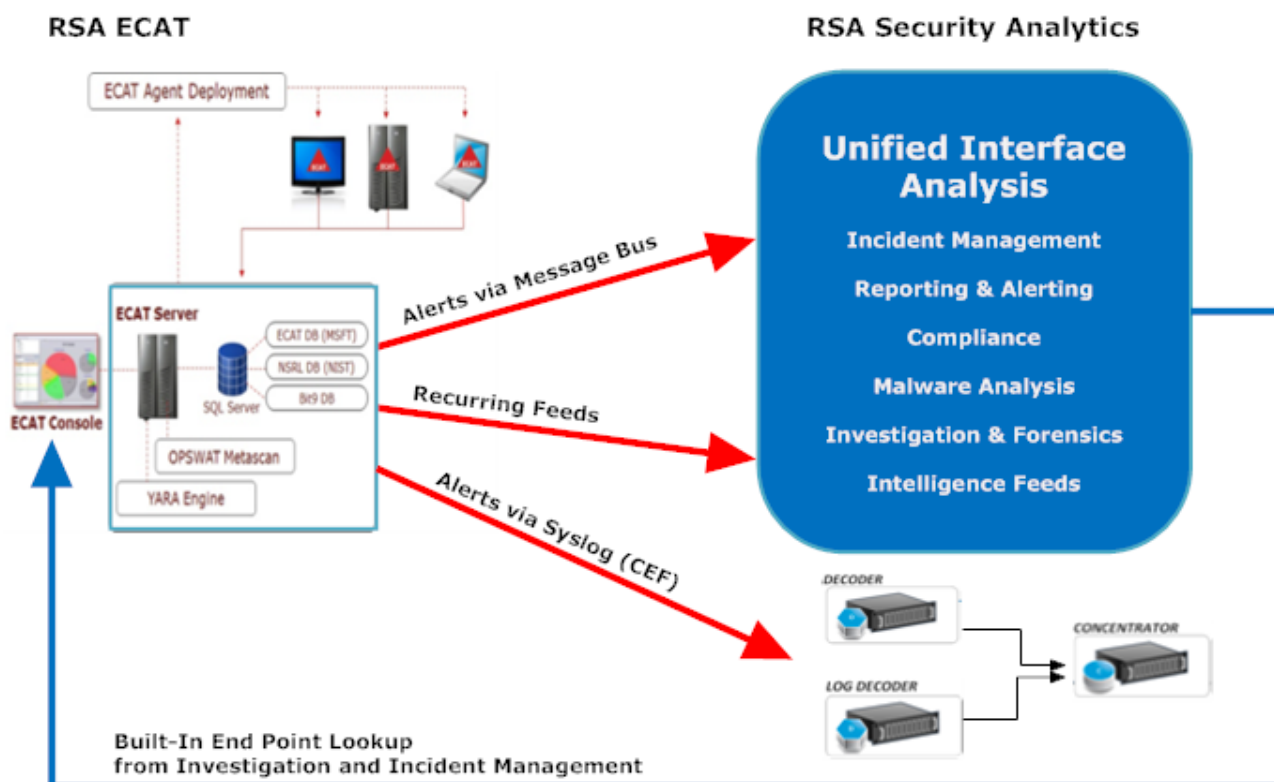
- Intégration de RSA ECAT 4
 - Configurer ECAT pour recevoir des feeds RSA Live 7
 - Configurer des alertes ECAT via les bus de messages 13
 - Configurer des données contextuelles à partir d'ECAT via un feed récurrent 17
 - Configurer des alertes ECAT via Syslog dans un Log Decoder 28



Intégration de RSA ECAT

Les clients RSA qui utilisent à la fois RSA ECAT version 4.0 et ultérieure et RSA Security Analytics version 10.4 et ultérieure, peuvent intégrer ECAT et Security Analytics de plusieurs manières différentes. Ce guide est destiné à Security Analytics version 10.6 et ultérieure.

Options d'intégration



Recherche de point de terminaison intégrée

Avec l'interface utilisateur RSA ECAT installée sur la même machine que le navigateur utilisé par l'analyste pour accéder à Security Analytics, la recherche de point de terminaison intégrée à partir de Security Analytics Investigation et Security Analytics Incident Management fournit un accès par clic droit au serveur de la console ECAT pour les clés méta suivantes : Adresse IP (`ip-src`, `ip-dst`, `ipv6-src`, `ipv6-dst`, `orig_ip`), hôte (`alias-host`,

`domain.dst`), `client` et `file-hash`. Ceux-ci sont décrits dans la section [Lancer la recherche externe d'une clé méta](#) et [Vue Alertes](#) dans Gestion des incidents.

Aucune configuration Security Analytics n'est requise pour la recherche de point de terminaison lorsque vous utilisez l'un des analyseurs intégrés RSA ECAT ou CEF, et que vous n'avez pas personnalisé les clés méta par défaut utilisées lors du chargement des métadonnées dans Investigation. Consultez la section ([Gérer et appliquer des clés méta par défaut dans une procédure d'enquête](#)).

Note: L'exception se produit si vous personnalisez Security Analytics en modifiant le paramètre d'affichage pour les clés méta par défaut dans Investigation, si vous ajoutez les clés méta au fichier `table-map-custom.xml`, ou si vous personnalisez les feeds RSA ECAT. Un certain degré de configuration est nécessaire pour ajouter les clés méta personnalisées au menu contextuel Recherche ECAT dans Administration > vue Système, comme décrit dans [Actions du menu Ajouter un contexte personnalisé](#).

Intégrations supplémentaires

Avec le serveur de console RSA ECAT version 4.0 ou ultérieure installé sur un hôte Windows et la configuration appropriée de ECAT et Security Analytics par un administrateur, quatre autres intégrations des données d'analyse ECAT sont possibles, comme le décrivent les flèches rouges ci-dessous.

Les intégrations RSA ECAT possibles avec Security Analytics comprennent :

- **Alertes ECAT via Syslog (CEF) dans les Log Decoders Security Analytics.** Cette intégration offre la possibilité d'appliquer Live Intelligence aux alertes ECAT et de corréler des événements ECAT avec d'autres métadonnées de logs ou paquets dans l'écosystème Security Analytics (consultez la section [Configurer des alertes ECAT via Syslog dans un Log Decoder](#)).
- **Alertes ECAT via le bus de messages dans Security Analytics Incident Management.** Cette intégration fournit la fonction de gestion des incidents et de workflow centralisés dans Security Analytics (consultez la section [Configurer les sources d'alertes pour afficher les alertes de gestion des incidents](#)).
- **Données contextuelles ECAT via un feed récurrent Security Analytics Live.** Cette intégration peut enrichir la session affichée dans Security Analytics Investigation avec des informations contextuelles ; comme le système d'exploitation hôte, l'adresse MAC, le score et d'autres données qui peuvent ne pas être présentes dans les données du log ou du paquet (consultez la rubrique [Configurer des données contextuelles à partir d'ECAT via un feed récurrent](#)).
- **Feeds RSA Live dans ECAT version 4.0 et ultérieure.** Cette intégration peut enrichir les indicateurs de compromission ECAT instantanés en utilisant plusieurs feeds dans RSA Live qui contiennent des domaines et des adresses IP suspects. Les indicateurs de compromission instantanés ECAT peuvent bénéficier de ces feeds du point de vue des renseignements. ECAT 4.0 ne publie aucun feed dans RSA Live (consultez la rubrique [Configurer ECAT pour recevoir des feeds de RSA Live](#)).

Alertes et indicateurs de compromission ECAT

Un indicateur de compromission ECAT est une requête de base de données qui exécute RSA ECAT sur des données d'analyse ECAT collectées pour déterminer la présence de logiciels malveillants potentiels sur des hôtes analysés. RSA ECAT version 4.0 et ultérieure est livré avec des indicateurs de compromission que l'utilisateur peut activer et marquer comme pouvant être alertés. RSA ECAT exécute les requêtes des indicateurs de compromission régulièrement sur les nouvelles données d'analyse, qui sont collectées et stockées dans la base de données. Si la requête de

L'indicateur de compromission est satisfaite, cela indique un indicateur potentiel de compromission, et l'événement peut être signalé à un utilisateur ou envoyé à un système externe comme une alerte.

Voici les types possibles d'alerte :

- Alerte de machine : Cette alerte indique que la machine en question est suspecte.
- Alerte de module : Cette alerte indique qu'un module, tel qu'un fichier, une dll ou un exécutable, est suspect. Elle contient des détails sur le module en question.
- Alerte IP : Cette alerte indique qu'il y a eu une activité Internet suspecte (trafic).
- Alerte d'événement : Cette alerte représente toute autre activité suspecte détectée par ECAT qui n'entre pas dans les catégories énoncées ci-dessus.

Chacun de ces types d'alerte peut être associé et envoyé à Security Analytics.



Configurer ECAT pour recevoir des feeds RSA Live

RSA ECAT 4.0 et toute version ultérieure peuvent être configurés pour recevoir des feeds provenant de RSA Live. Plusieurs feeds de RSA Live contiennent des domaines et des adresses IP suspects, et plusieurs indicateurs instantanés de compromission définis dans ECAT peuvent bénéficier de ces feeds du point de vue des renseignements. Aucun de ces feeds n'est activé par défaut dans ECAT. Lorsqu'un feed est activé, le serveur de console ECAT se connecte à RSA Live <https://cms.netwitness.com> et télécharge périodiquement les données des feeds vers le système ECAT.

Note: ECAT ne publie aucune source dans RSA Live. Il s'agit uniquement d'un consommateur de feeds.

Note: La procédure de configuration de RSA ECAT pour recevoir les feeds RSA Live est différente pour ECAT version 4.0 et ECAT version 4.1. Nous avons inclus des instructions pour les deux versions.

Conditions préalables

Cette intégration requiert ce qui suit :

- L'installation de la version 4.0 ou ultérieure de l'interface utilisateur ECAT et de la version 10.6 du serveur Security Analytics.
- Un compte RSA Live, pour lequel vous pouvez obtenir un nom d'utilisateur et un mot de passe à partir de RSA Support.
- Le serveur de console ECAT doit se connecter à <https://cms.netwitness.com>.

Activer ou désactiver les feeds

Pour ECAT version 4.0

1. Ouvrez l'interface utilisateur ECAT et connectez-vous en utilisant les informations d'identification adéquates.
2. Dans la barre de menus située en haut de la page, sélectionnez **Base de données > Importer les checksums**. La boîte de dialogue Importer les checksums s'affiche.
3. Sélectionnez l'onglet **RSA Live**, puis le sous-onglet **Paramètres**.
4. Remplissez les détails du serveur RSA Live et les informations d'identification. La valeur de l'hôte est généralement cms.netwitness.com. Le port est habituellement le **443**.
5. Pour valider la connectivité, cliquez sur **Tester la connexion**. Un message **Réussi** s'affiche si tous les paramètres sont corrects.
6. Cliquez sur **Appliquer**.

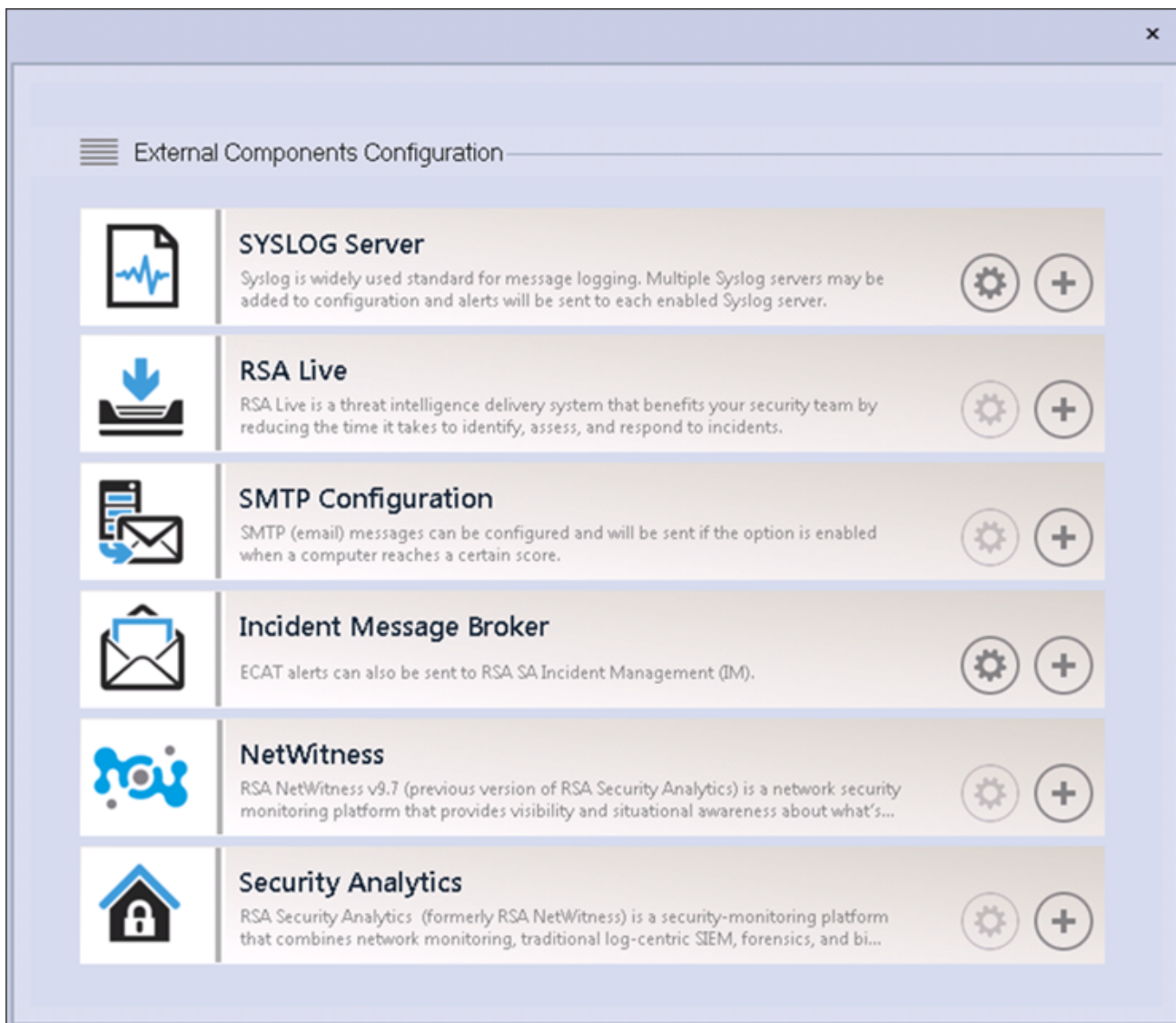
7. Sélectionnez le sous-onglet **Feeds abonnés**.
Une liste des feeds s'affiche.
8. Sélectionnez les feeds que vous souhaitez que ECAT importe à partir de RSA Live.
9. Saisissez un intervalle approprié. Le temps recommandé est de 24 heures, ce qui configure ECAT pour se connecter à RSA Live toutes les 24 heures afin de mettre à jour les données importées.
10. (Facultatif) Cliquez sur **Actualiser maintenant** pour télécharger les feeds immédiatement.
11. Cliquez sur **Enregistrer**.

Pour afficher l'état des domaines et des adresses IP incorrects, connus et importés, issus de différents feeds, sélectionnez l'onglet **État** puis le feed. Le nombre d'entrées par feed varie de quelques centaines à plusieurs milliers.



















Pour ECAT version 4.1

1. Créez un utilisateur SQL avec les informations d'identification dans ECAT :
 - a. Ouvrez l'interface utilisateur ECAT et connectez-vous en utilisant les informations d'identification adéquates.
 - b. Cliquez sur **Configurer > Gérer les utilisateurs et les rôles**.
 - c. Dans **Sécurité**, cliquez avec le bouton droit dans le volet, puis sélectionnez **Créer un nouvel utilisateur SQL**.
 - d. Fournissez le nom de connexion et le mot de passe.
2. Dans la barre de menus située en haut de la page, sélectionnez **Configurer > Composants de surveillance et externes**.

3. La fenêtre Configuration des composants externes s'affiche. Sélectionnez **RSA Live**, puis cliquez sur **+**.



The screenshot shows a window titled "External Components Configuration" with a close button (X) in the top right corner. The window contains a list of six external components, each with an icon, a title, a description, and two circular buttons (a gear for configuration and a plus sign for adding).

Icon	Component Name	Description	Configuration	Add
	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.		
	Incident Message Broker	ECAT alerts can also be sent to RSA SA Incident Management (IM).		
	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...		
	Security Analytics	RSA Security Analytics (formerly RSA NetWitness) is a security-monitoring platform that combines network monitoring, traditional log-centric SIEM, forensics, and bi...		

Feeds RSA Live pour ECAT 4.0 et version ultérieure

Nom du feed	Description
Domaines de menaces RSA FirstWatch Insider	Ce feed contient des domaines connus pour être associés à des menaces internes.
Adresses IP de menaces RSA FirstWatch Insider	Ce feed contient des adresses IP connues pour être associées à des menaces internes.
Adresses IP RSA FraudAction	Ce feed contient des adresses IP issues du feed RSA FraudAction.
Domaines RSA FraudAction	Ce feed contient des domaines issus du feed RSA FraudAction.
Réputation d'adresses IP RSA FirstWatch	Ce feed contient des adresses IP qui sont connues pour être compromises.
Adresses IP VPN criminelles RSA FirstWatch	Ce feed contient des adresses IP qui représentent des nœuds d'entrée VPN connus pour les services d'anonymisation criminels.
Adresses IP de sortie VPN criminelles RSA FirstWatch	Ce feed contient des adresses IP qui représentent des nœuds de sortie VPN connus pour les services d'anonymisation criminels.
Adresses IP de menaces APT RSA FirstWatch	Ce feed contient des adresses IP connues pour être associées à des APT.
Adresses IP d'attaques RSA FirstWatch	Ce feed contient des adresses IP connues pour être associées à la transmission de programmes malveillants.
Adresses IP de commande et contrôle RSA FirstWatch	Ce feed contient des adresses IP connues pour être associées à la commande et au contrôle des programmes malveillants.
Domaines de menaces APT RSA FirstWatch	Ce feed contient des domaines connus pour être associés à des APT.
Domaines de commande et contrôle RSA FirstWatch	Ce feed contient des domaines connus pour être associés à la commande et au contrôle de programmes malveillants.
Adresses IP de nœuds SOCKS criminelles RSA FirstWatch	Ce feed contient des adresses IP qui représentent des nœuds SOCKS connus pour les services d'anonymisation criminels.
Domaines d'indicateurs de domaines IDefense	Les services de renseignements de sécurité Verisign idefense donne accès aux responsables de la sécurité des informations à une intelligence cybernétique précise et concrète liée aux vulnérabilités, au code malveillant et aux menaces mondiales, 24 heures par jour et 7 jours par semaine. Les recommandations de l'analyse en profondeur, de la connaissance et des réponses de Verisign idefense aident à garder les entreprises et les organismes gouvernementaux en avance sur les menaces et les vulnérabilités nouvelles et en évolution.
Plages d'adresses IP Spamhaus DROP	DROP (Don't Route Or Peer) et EDROP sont des listes consultatives du trafic, composées de netblocks piratés et contrôlés entièrement par des criminels et des inondeurs professionnels.
Zeus Tracker	Zeus tracker est une liste d'adresses IP de serveurs de commande et contrôle (hôtes) Zeus (également connu sous le nom de zbot, prg, wsnpoem, gorhax et Kneber) dans le monde entier. Zeus tracker a suivi

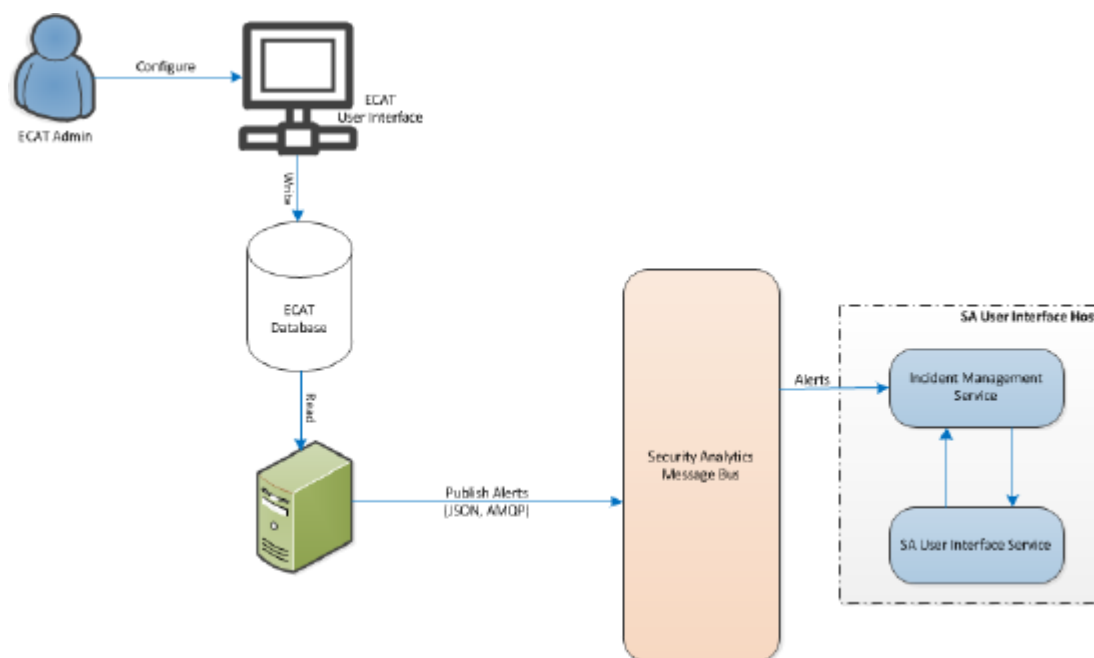
Nom du feed	Description
	plus de 2 800 serveurs de commande et contrôle Zeus malveillants. Zeus se propage principalement par l'intermédiaire de téléchargements à l'insu de l'utilisateur et de phishing.
Zeus Domain Tracker	Zeus domain tracker est une liste de noms de domaine de commande et contrôle Zeus (également connu sous le nom zbot, prg, wsnpoem, gorhax et Kneber). Zeus tracker a suivi plus de 2 800 serveurs de commande et contrôle Zeus malveillants. Zeus se propage principalement par l'intermédiaire de téléchargements à l'insu de l'utilisateur et de phishing.
Liste de domaines de programmes malveillants	Liste des domaines souvent associés à des programmes malveillants provenant de www.malwaredomainlist.com
SpyEye Domain Tracker	SpyEye domain tracker est une liste de noms de domaine de commande et contrôle SpyEye (également connu sous le nom zbot, prg, wsnpoem, gorhax et Kneber). SpyEye tracker a suivi plus de 2 800 serveurs de commande et contrôle SpyEye malveillants. SpyEye se propage principalement par l'intermédiaire de téléchargements à l'insu de l'utilisateur et de phishing.
Adresses IP d'utilisateurs socks criminelles RSA FirstWatch	Ce feed contient les adresses IP qui ont été observées en utilisant les services d'anonymisation criminels.
Nœuds de sortie Tor	Ce feed contient les adresses IP qui sont répertoriées comme nœuds de sortie actifs pour le réseau Tor.
Nœuds Tor	Ce feed contient les adresses IP qui sont répertoriées comme nœuds actifs dans le réseau Tor.
Domaines de programmes malveillants	Liste des domaines associés à des programmes malveillants provenant de www.malwaredomainlist.com
Liste d'adresses IP de programmes malveillants	Liste des adresses IP souvent associées à des programmes malveillants provenant de www.malwaredomainlist.com



Configurer des alertes ECAT via les bus de messages

Cette procédure est requise pour intégrer ECAT avec Security Analytics de façon à ce que les alertes ECAT soient relevées par le composant Incident Management de Security Analytics et affichées dans la vue **Incident > Alertes**.

Le diagramme ci-dessous représente le flux d'alertes ECAT dans la file d'attente de gestion des incidents de Security Analytics et affiche les alertes dans la vue **Incident > Alertes**.



Conditions préalables

Veillez à disposer des informations suivantes :

- Le service Incident Management est installé et en cours d'exécution sur Security Analytics 10.4 ou version ultérieure.
- ECAT 4.0 ou version ultérieure est installé et en cours d'exécution.

Configurez le Broker Incident Management en tant que composant ECAT externe

Pour ECAT version 4.0

Pour configurer ECAT de manière à envoyer des alertes sur le bus de messages à l'interface utilisateur Security Analytics :

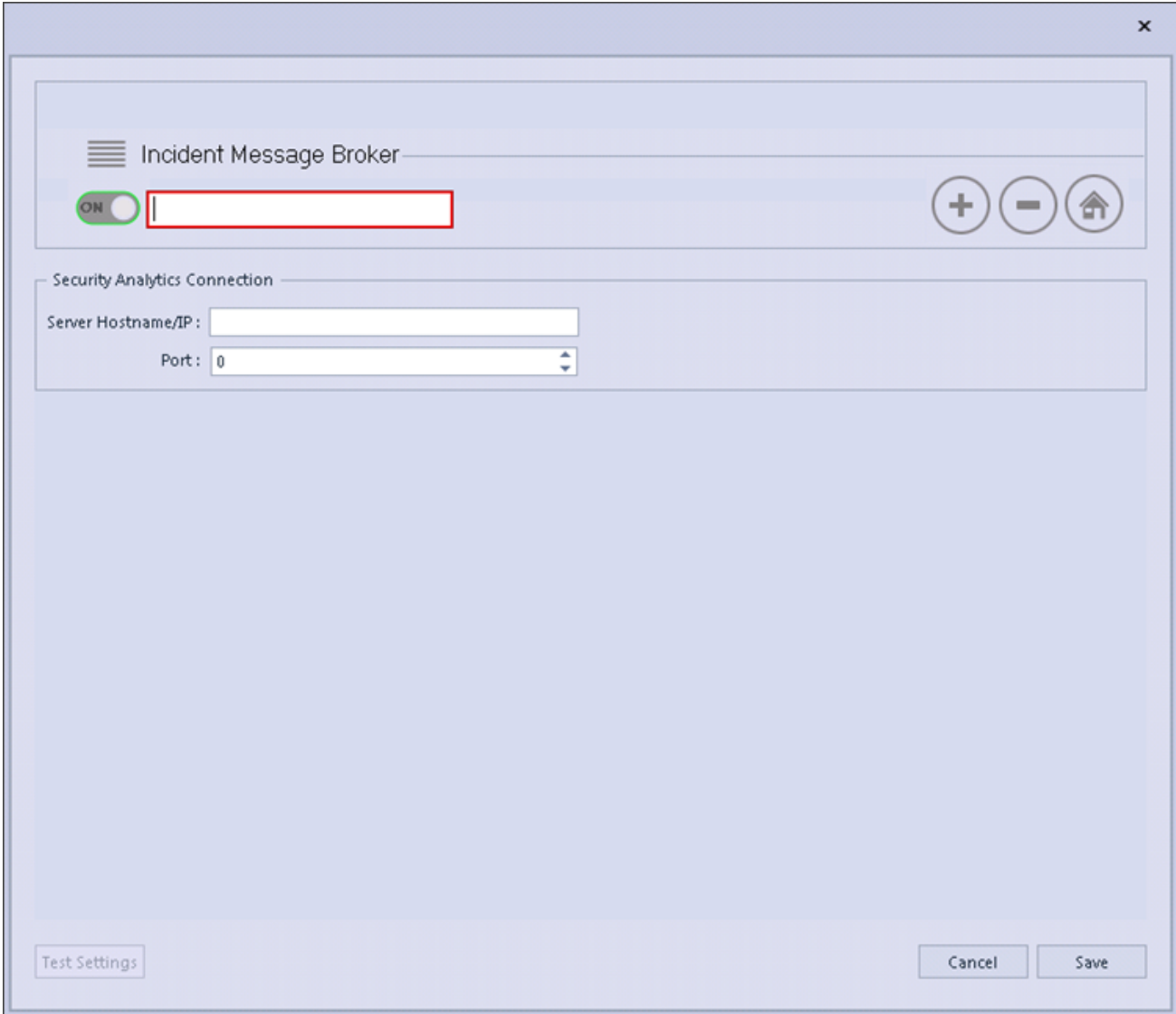
1. Ouvrez l'interface utilisateur ECAT et connectez-vous en utilisant les informations d'identification adéquates.
2. Dans la barre du menu, sélectionnez **Configurer > Composants de surveillance et externes**.
La boîte de dialogue Composants de surveillance et externes s'affiche.
3. Cliquez avec le bouton droit de la souris n'importe où dans la boîte de dialogue et sélectionnez **Ajouter un composant**.
La boîte de dialogue Ajouter un composant s'affiche.
4. Fournissez les informations suivantes :
 - Sélectionnez le type de composant IM Broker dans les options de la liste déroulante.
 - Saisissez un nom d'utilisateur pour identifier le composant IM Broker.
 - Saisissez le DNS de l'hôte ou l'adresse IP du composant IM Broker.
 - Saisissez le numéro de port.
5. Cliquez sur **Enregistrer** et **fermer** pour fermer toutes les boîtes de dialogue.

Pour ECAT version 4.1

Pour configurer ECAT de manière à envoyer des alertes sur le bus de messages à l'interface utilisateur Security Analytics :

1. Ouvrez l'interface utilisateur ECAT et connectez-vous en utilisant les informations d'identification adéquates.
2. Dans la barre du menu, sélectionnez **Configurer > Composants de surveillance et externes**.
La boîte de dialogue Configuration des composants externes s'affiche.

3. Dans **Incident Message Broker**, cliquez sur **+** pour ajouter un Incident Message (IM) Broker. La boîte de dialogue Incident Message Broker s'affiche.



The screenshot shows a configuration dialog box titled "Incident Message Broker". At the top left, there is a hamburger menu icon and the title. Below the title, there is a green "ON" toggle switch and a red-bordered text input field. To the right of these are three circular icons: a plus sign (+), a minus sign (-), and a home icon. Below this section is a "Security Analytics Connection" section containing two input fields: "Server Hostname/IP:" and "Port:". The "Port:" field currently shows the value "0". At the bottom left of the dialog is a "Test Settings" button, and at the bottom right are "Cancel" and "Save" buttons.

4. Sous **Incident Message Broker**, dans **Activé**, saisissez un nom pour le composant Message Broker.
5. Sous **Connexion Security Analytics**, effectuez la procédure suivante.
 - a. Dans **Nom d'hôte/IP du serveur**, saisissez l'adresse IP du serveur Security Analytics.
 - b. Dans **Port**, le numéro de port par défaut est 5671. Actualisez le champ si nécessaire.
6. Cliquez sur **Enregistrer**.

Configurer le certificat AC ECAT sur le service Security Analytics Broker

Pour configurer une connexion SSL pour les alertes de gestion d'incidents :

1. Sur le serveur de console primaire ECAT, exportez le certificat AC ECAT au format `.cer` (base-64 codé X.509) à partir du magasin de certificats personnel de l'ordinateur (sans sélectionner la clé privée).
2. Sur le serveur de console primaire ECAT (sur l'ordinateur, à l'emplacement où se trouve le fichier exécutable ECAT `makecert`), générez un certificat client pour ECAT à l'aide du certificat AC ECAT. (Vous devez définir le nom CN sur `ecat`).

```
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. Sur le serveur de console primaire ECAT, notez l'empreinte du certificat client généré à l'étape 2. Saisissez la valeur d'empreinte du certificat client dans la section `IMBrokerClientCertificateThumbprint` du fichier `ConsoleServer.Exe` comme indiqué.

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

Note: Lorsque vous saisissez une valeur d'empreinte dans le champ Valeur, veuillez à supprimer le point d'interrogation (?), saisissez la valeur, puis enregistrez le fichier.

4. Sur le serveur Security Analytics, ajoutez le contenu du fichier de certificat AC ECAT au format `.cer` format (à partir de l'étape 1) vers
`/etc/puppet/modules/rabbitmq/files/truststore.pem`
5. Sur le serveur Security Analytics, procédez de l'une des façons suivantes :
 - Exécutez l'agent puppet avec la commande suivante : `puppet agent -t`
 - Attendez 30 minutes que le serveur Security Analytics exécute l'agent.
6. Sur le serveur de console primaire ECAT, importez le fichier `/var/lib/puppet/ssl/certs/ca.pem` à partir du serveur Security Analytics vers le magasin Autorités de certification racines de confiance. Ceci permet de s'assurer que l'ECAT, en tant que client, peut faire confiance au certificat de serveur Incident Management.
7. Redémarrez le serveur ECAT pour activer ECAT et envoyer des alertes à Security Analytics.



Configurer des données contextuelles à partir d'ECAT via un feed récurrent

Cette rubrique fournit les instructions permettant de configurer des données RSA ECAT dans Security Analytics pour fournir des données contextuelles ECAT aux sessions Decoder et Log Decoder. Cette configuration ajoute des métavaleurs contextuelles en plus des alertes IOC instantanées qui permettent de créer des corrélations à d'autres métadonnées dans l'écosystème Security Analytics.

Les administrateurs peuvent configurer Security Analytics afin d'utiliser les données contextuelles d'analyse du système ECAT via un feed récurrent Security Analytics Live. Cette intégration peut enrichir la session d'un Decoder ou Log Decoder avec des informations contextuelles affichées dans une procédure d'enquête de Security Analytics. Certains exemples incluent dans les sessions Decoder ou Log Decoder, le système d'exploitation hôte, l'adresse MAC, le score et bien d'autres données qui peuvent ne pas être présentes dans les données de logs ou de paquets.

Note: Bien que cette fonctionnalité soit ciblée pour les clients avec un paquet {nd}}, un flux récurrent peut également être mis en œuvre dans les Log Decoders.

Caution: Dans les environnements avec de nombreux hôtes ECAT, l'utilisation de ce feed récurrent peut entraîner une diminution des performances sur les périphériques d'acquisition Security Analytics (Decoder et Log Decoder).

Conditions préalables

- Serveur de Console version 4.0 ECAT et serveur Security Analytics version 10.4 et supérieure installés.
- RSA Decoder et Concentrator version 10.4 ou supérieure connectés au serveur Security Analytics sur le réseau.

Configuration

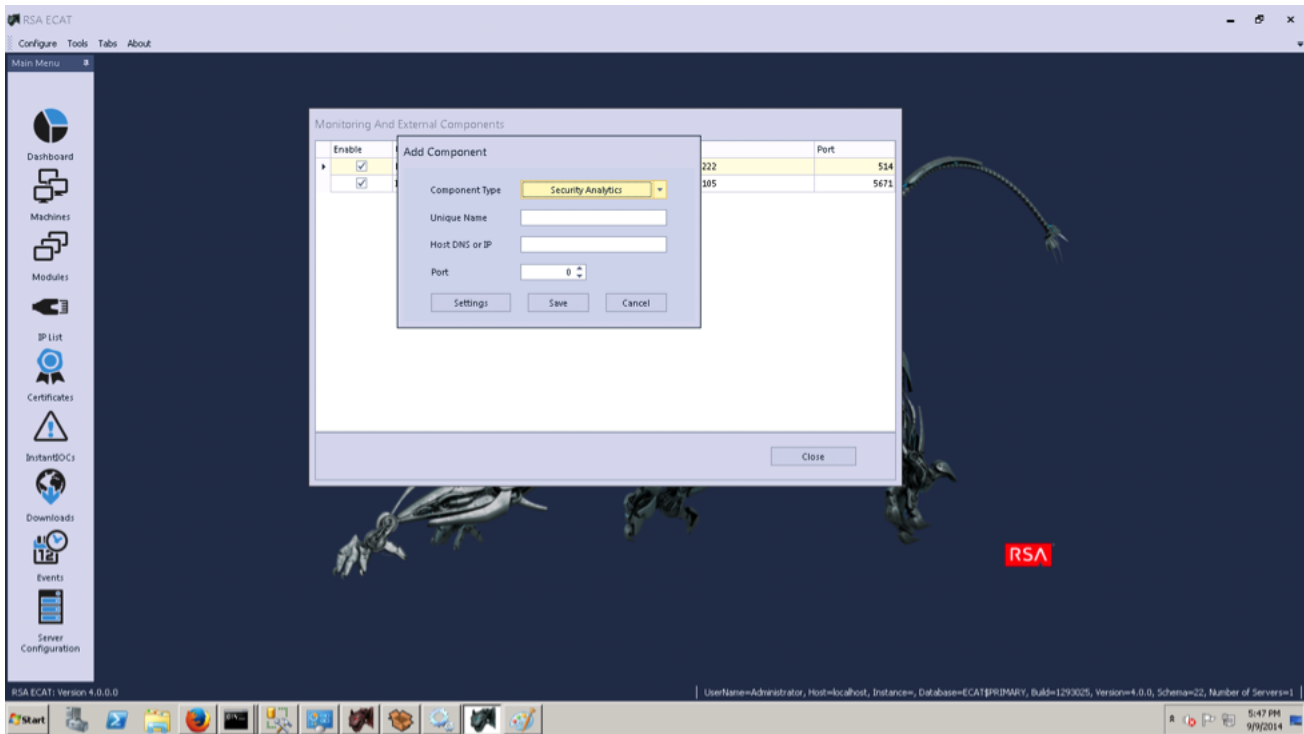
Pour configurer cette intégration :

1. Activez le feed ECAT pour Security Analytics dans l'interface utilisateur ECAT.
2. Exportez le certificat de l'autorité de certification ECAT du serveur de Console eCAT et importez-le vers le magasin d'approbations Security Analytics.
3. Configurez le service Security Analytics Concentrator pour définir les clés méta à indexer.
4. Créez un feed récurrent dans Security Analytics Live.

Activer le feed ECAT pour Security Analytics

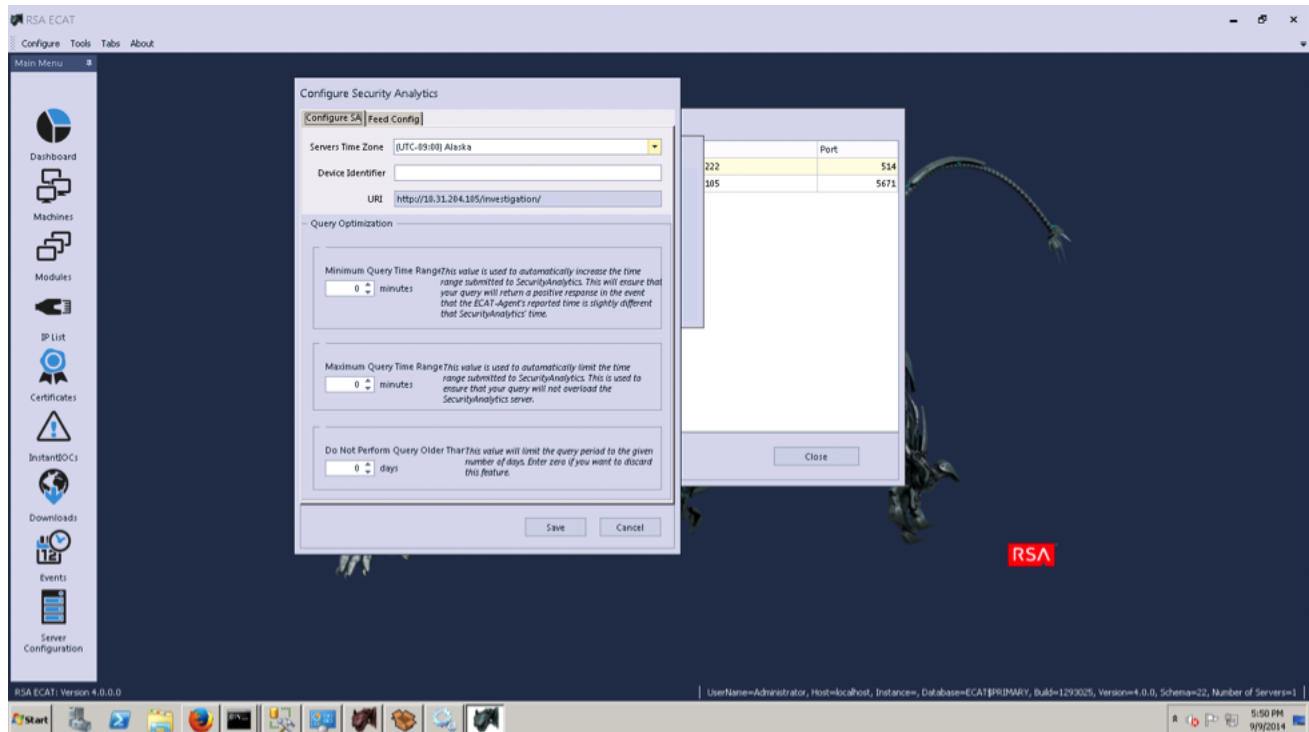
Pour ECAT version 4.0

1. Ouvrez l'interface utilisateur ECAT et connectez-vous en utilisant les informations d'identification adéquates.
2. Dans la barre de menus, sélectionnez **Configurer > Composants de surveillance et externes**. La boîte de dialogue Ajouter des composants s'affiche.

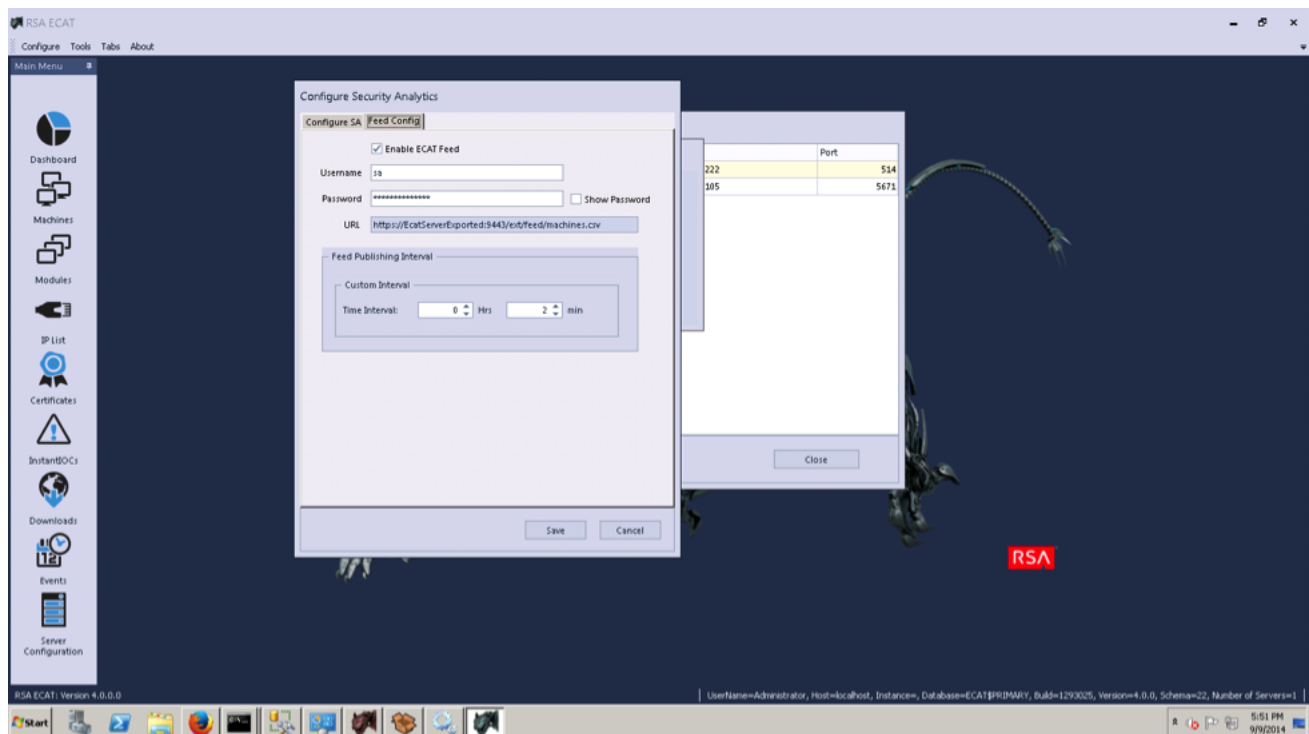


3. Ajoutez un composant Security Analytics. Saisissez le **nom unique**, le **DNS de l'hôte** ou **l'adresse IP**, puis cliquez sur **Paramètres**.

La boîte de dialogue Configurer Security Analytics s'affiche.



4. Renseignez le champ **Fuseau horaire** et cliquez sur l'onglet **Config. feed**.



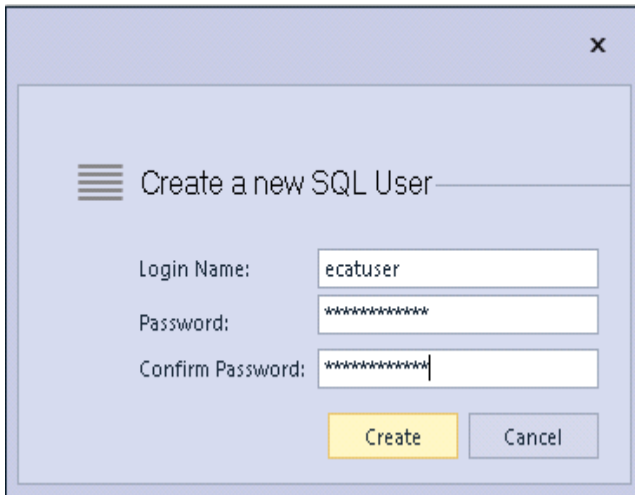
5. Sélectionnez **Activer le feed ECAT**, puis saisissez le **nom d'utilisateur** et le **mot de passe**. Configurez l'**intervalle de publication des feeds**. Cliquez sur **Enregistrer**.
Un feed est créé.

6. Relevez l'URL attribuée, ainsi que le nom d'utilisateur et le mot de passe. Ces informations seront utilisées dans Security Analytics.
7. Pour vérifier que le feed a été créé correctement, ouvrez un navigateur et saisissez l'URL. À l'invite, saisissez le nom d'utilisateur et le mot de passe. Vérifiez si un fichier nommé `machines.csv` est téléchargé.

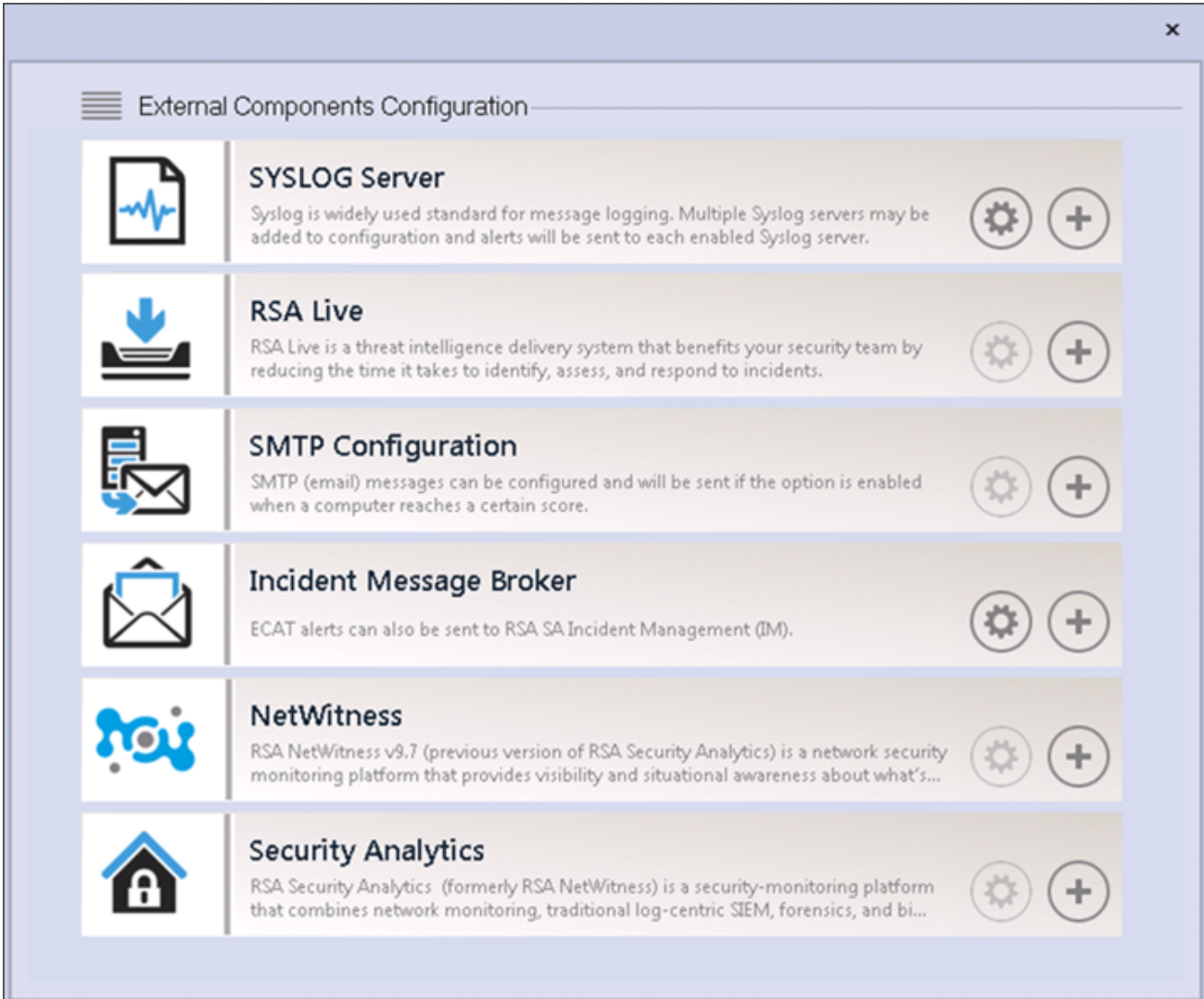
Pour ECAT version 4.1

Dans l'interface utilisateur ECAT :

1. Créez un utilisateur SQL dans ECAT :
 - a. Ouvrez l'interface utilisateur ECAT et connectez-vous en utilisant les informations d'identification adéquates.
 - b. Sous Sécurité, cliquez avec le bouton droit de la souris dans le panneau et sélectionnez **Créer un utilisateur SQL**. La boîte de dialogue Créer un utilisateur SQL s'affiche.



- c. Indiquez le nom de connexion et le mot de passe.
2. Dans la barre de menus, sélectionnez **Configurer > Composants de surveillance et externes**. La boîte de dialogue Configuration des composants externes s'affiche.



The screenshot shows a window titled "External Components Configuration" with a close button (X) in the top right corner. The window contains a list of six external components, each with an icon, a title, a description, and two circular buttons (a gear for settings and a plus sign for adding).

Icon	Component Name	Description	Settings	Add
	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.		
	Incident Message Broker	ECAT alerts can also be sent to RSA SA Incident Management (IM).		
	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...		
	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. Dans Security Analytics, cliquez sur +.
La boîte de dialogue Security Analytics s'affiche.

4. Sous **Security Analytics**, dans **Sur**, saisissez un nom pour identifier le composant Security Analytics.
5. Sous **Connexion Security Analytics**, procédez comme suit :
 - a. Dans **Nom d'hôte/IP du serveur**, saisissez le nom d'hôte ou l'adresse IP du serveur Security Analytics.
 - b. Dans **Port**, entrez le numéro de port par défaut 443. Si nécessaire, mettez à jour le champ.
6. Sous **Configurer Security Analytics**, procédez comme suit :
 - a. Dans **Fuseau horaire des serveurs**, entrez un fuseau horaire pour le composant.
 - b. Dans **Identifiant du périphérique**, saisissez l'ID du périphérique du Concentrator Security Analytics.

Note: Pour trouver l'identifiant du périphérique dans Security Analytics, vous devez rechercher un Concentrator ou un Broker dans **Procédure d'enquête > Naviguer > <Nom du Concentrator ou du Broker>**. L'identifiant du périphérique est le numéro figurant dans l'URL après « investigation ». Par exemple, dans l'URL `https://<adresse IP>investigation/319/navigate/values`, l'identifiant du périphérique est **319**.

Le champ **URI** est renseigné lorsque vous cliquez sur **Enregistrer**.

8. Dans **Optimisation de requête**, effectuez les opérations suivantes :
 - a. Dans **Min**, entrez le nombre de minutes correspondant à la période de requête minimale. Cette valeur sert à augmenter automatiquement la période soumise à Security Analytics. Une requête retourne ainsi une réponse positive si l'heure signalée par l'agent ECAT diffère légèrement de celle de Security Analytics.
 - b. Dans **Max**, entrez le nombre de minutes pour limiter la période. Cette valeur sert à limiter automatiquement la période soumise à Security Analytics afin que les requêtes ne surchargent pas le serveur Security Analytics.
 - c. Dans **Ne pas exécuter de requête pour une période supérieure à**, entrez un nombre de jours pour limiter la période de la requête. Entrez **0** pour ignorer cette fonctionnalité.
9. Dans **Configurer les feeds ECAT pour SA**, effectuez les opérations suivantes :
 - a. Sélectionnez **Activer le feed ECAT**.
 - b. Entrez le **Nom d'utilisateur** et le **Mot de passe** SQL (configurés à l'étape 1) pour accéder à l'emplacement du feed. Le champ **URL** est renseigné lorsque vous cliquez sur **Enregistrer**.
 - c. Entrez l'intervalle de temps correspondant à la fréquence à laquelle les feeds sont publiés.
10. Cliquez sur **Enregistrer**.
Un feed est créé.

Exporter le certificat SSL ECAT

Note: Cette procédure ne fonctionne que pour Security Analytics 10.5 et version ultérieure, car la prise en charge de Java 8 a été ajoutée pour la version 10.5. Si vous utilisez une version antérieure de Security Analytics, reportez-vous à la version applicable de ce guide.

Pour exporter le certificat de l'autorité de certification ECAT à partir du serveur de Console ECAT et le copier sur l'hôte Security Analytics :

1. Connectez-vous à la Console ECAT.
2. Ouvrez **MMC**.
3. Ajoutez un composant logiciel enfichable de certificat pour le **compte d'ordinateur**.
4. Exportez le certificat nommé **EcatCA**.
 - a. Effectuez l'exportation sans clé privée.
 - b. Exportez au format binaire X.509 encodé DER (**.CER**).
 - c. Nommez le fichier **EcatCA.cer**.
5. Copiez le certificat de l'autorité de certification ECAT vers l'hôte Security Analytics :
`scp EcatCA.cer root@<machine-sa> :.`
6. Pour importer le certificat de l'autorité de certification ECAT vers le magasin d'approbations Security Analytics, saisissez les commandes suivantes :
`JDK=/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.31-0.b17.e16_7.x86_64/jre/
$JDK/bin/keytool -import -v -trustcacerts -alias ecatca -file ~/EcatCA.cer -keystore $JDK/lib/
security/cacerts -storepass changeit`
Lorsque vous êtes invité à confirmer la mise à jour du certificat, saisissez **Yes**.
7. Sur l'hôte Security Analytics, modifiez `/etc/hosts` pour mapper l'adresse IP du serveur de Console ECAT au nom **ecatserverexported** en ajoutant la ligne suivante au fichier :
`<ip-address-ecat-cs> ecatserverexported`

8. Pour redémarrer Security Analytics, saisissez les commandes suivantes :

```
stop jettysrv
start jettysrv
```

Configurer le service Security Analytics Concentrator

1. Connectez-vous à Security Analytics et accédez à **Administration > Services**.
2. Sélectionnez un Concentrator dans la liste, puis sélectionnez **Vue > Config**.
3. Sélectionnez l'onglet **Fichiers**, et dans le menu déroulant **Fichiers à modifier**, sélectionnez **index-concentrator-custom.xml**.
4. Ajoutez les clés métas ECAT suivantes au fichier, puis cliquez sur **Appliquer**. Vérifiez que ce fichier contient déjà les sections XML et si ce n'est pas le cas, ajoutez-les. Les lignes suivantes sont des exemples ; assurez-vous que les valeurs correspondent à votre configuration et aux noms de colonnes que vous avez inclus dans la définition de feed, où :
 - description** est le nom de la clé méta que vous souhaitez afficher dans Security Analytics Investigation.
 - level** correspond à "IndexValues"
 - name** correspond au nom de colonne du fichier CSV utilisé par Security Analytics lors de la définition du feed récurrent (voir le tableau de la rubrique *Configurer la tâche de feed personnalisée récurrente dans Security Analytics* ci-après).

```
<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"/>
```

5. Redémarrez le Concentrator pour activer les mises à jour personnalisées.

Configurer la tâche de feed personnalisée récurrente dans Security Analytics

Pour configurer la tâche de feed récurrente dans Security Analytics :

1. Connectez-vous à Security Analytics et accédez à **Live > Feeds**.
2. Sélectionnez **Feed personnalisé > Suivant**.
3. Effectuez les actions suivantes :
 - a. Sélectionnez **Récurrent**.
 - b. Saisissez un **nom**, par exemple : **EcatFeed**.
 - c. Saisissez l'URL avec le nom d'hôte du serveur Windows sur lequel est installé ECAT :
 - Pour RSA ECAT version 4.0, utilisez l'URL <https://<EcatServerHostname>:9443/ext/feed/machines.csv>.
 - Pour RSA ECAT version 4.1, utilisez l'URL <https://<EcatServerExported>:9443/api/v2/feed/machines.csv>.
4. Activez la case à cocher **Authentifié** et saisissez le nom d'utilisateur et le mot de passe tels que notés dans *Activer le feed ECAT* ci-dessus.
5. Sélectionnez **Vérifier** pour vérifier que Security Analytics peut atteindre la ressource Web.

6. Définissez le planning. Cliquez sur **Suivant**.

7. Sous l'onglet **Sélectionner des services**, sélectionnez le Decoder ou les groupes pour utiliser le feed. Cliquez sur **Suivant**.

8. Sous l'onglet **Définir des colonnes**, saisissez les noms de colonnes comme indiqué dans le tableau ci-dessous et enregistrez le feed.

Column	1	2 (Index)	3	4
Key	alias.host		stransaddr	gateway
	WIN2K8-60	10.31.204.60	10.31.204.60	10.31.204.1

Il s'agit des colonnes du fichier CSV pour le feed ECAT.

Colonne	Nom	Description	Nom de la colonne dans Security Analytics (Nom de la clé méta)
1	MachineName	Nom d'hôte de l'agent Windows	alias.host
2	LocalIp	Adresse IPv4	index
3	Remotelp	Adresse IP distante telle qu'elle est vue par le routeur	stransaddr
4	GatewayIp	Adresse IP de la passerelle	gateway
5	MacAddress	Adresse MAC	eth.src
6	OperatingSystem	Système d'exploitation utilisé par l'agent Windows	OS
7	AgentID	ID d'agent de l'hôte (ID unique attribué à l'agent)	client
8	ConnectionUTCTime	Dernière heure à laquelle l'agent s'est connecté au serveur ECAT	ecat.ctime
9	Domaine source	Domaine	domain.src
10	ScanUTCTime	La dernière fois que l'agent a été analysé	ecat.stime
11	Note de l'ordinateur	Score de l'agent indiquant le niveau suspect	risk.num

Note: Dans le tableau, le paramètre d'index recommandé est LocalIp. Cependant, si le LocalIp du PC de l'agent ECAT est alloué par un serveur DHCP, que la durée du bail DHCP a expiré et que l'adresse IP est ensuite réaffectée à un autre PC, les métadonnées créées par le feed seront incorrectes. Pour éviter ce risque, utilisez le nom de machine ou l'adresse Mac au lieu de l'adresse localIP comme index du feed. Par exemple, pour utiliser une adresse Mac, vous pouvez entrer les valeurs comme il est indiqué dans la figure ci-dessous.

The screenshot shows the 'Configure a Custom Feed' interface with the 'Define Columns' step active. In the 'Define Index' section, the 'Non IP' radio button is selected, and the 'Index Column' dropdown is set to '5'. The 'Callback Key (5)' field contains 'eth.src'. In the 'Define Values' table, the '5 (Index)' column is highlighted.

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

Résultat

Lors de la visualisation des sources de données dans Security Analytics, en cas de correspondance de la valeur indexée (ip.src), les métadonnées sont renseignées dans les interfaces Procédure d'enquête, Reporting et Alertes.

Dépannage

Cette section suggère comment résoudre les problèmes que vous pouvez rencontrer lors de l'utilisation de feeds récurrents.

Problèmes connus	Solutions
Avec ECAT 4.1.0.2 et ECAT 4.1.1, l'intégration des feeds ECAT ne fonctionne pas pour Security Analytics.	Vous devez utiliser ECAT 4.1.1.1 pour que le feed fonctionne.



Configurer des alertes ECAT via Syslog dans un Log Decoder

Cette rubrique fournit les instructions permettant de configurer l'utilisation des données RSA ECAT dans Security Analytics pour fournir des alertes ECAT aux sessions Log Decoder via Syslog. Cette configuration génère des métadonnées utilisées par les services Investigation, Alerts et Reporting Engine de Security Analytics.

Pour les réseaux Security Analytics qui consomment des logs, l'intégration d'ECAT avec Security Analytics transmet les événements ECAT vers Log Decoder via des messages syslog au format CEF (Common Event Format) et génère des métadonnées utilisées par Security Analytics Investigation, Alerts et Reporting Engine. Le cas d'utilisation pour cette intégration est l'intégration SIEM pour permettre la gestion centralisée des événements, la corrélation entre des événements ECAT et d'autres données Log Decoder, le reporting Security Analytics sur les événements ECAT, et les alertes Security Analytics sur les événements ECAT.

Conditions préalables

Cette intégration requiert ce qui suit :

- Interface utilisateur ECAT Version 4.0 ou supérieure
- Security Analytics Server Version 10.4 ou supérieure installée.
- RSA Log Decoder et Concentrator version 10.4 ou supérieure connectés à Security Analytics Server sur le réseau.
- Port 514 ouvert entre le serveur ECAT et Log Decoder derrière le pare-feu.

Procédure

Pour configurer cette intégration, effectuez les étapes suivantes :

1. Déployez le parser requis (CEF ou ECAT) vers le Log Decoder comme l'indique la rubrique [Gérer les ressources Live](#).

Note: N'utilisez qu'un seul de ces parsers. Lorsque le parser CEF est déployé, il prévaut sur le parser ECAT, et tous les messages CEF dans Security Analytics sont traités par le parser CEF. L'activation des deux parsers est un fardeau inutile sur les performances.

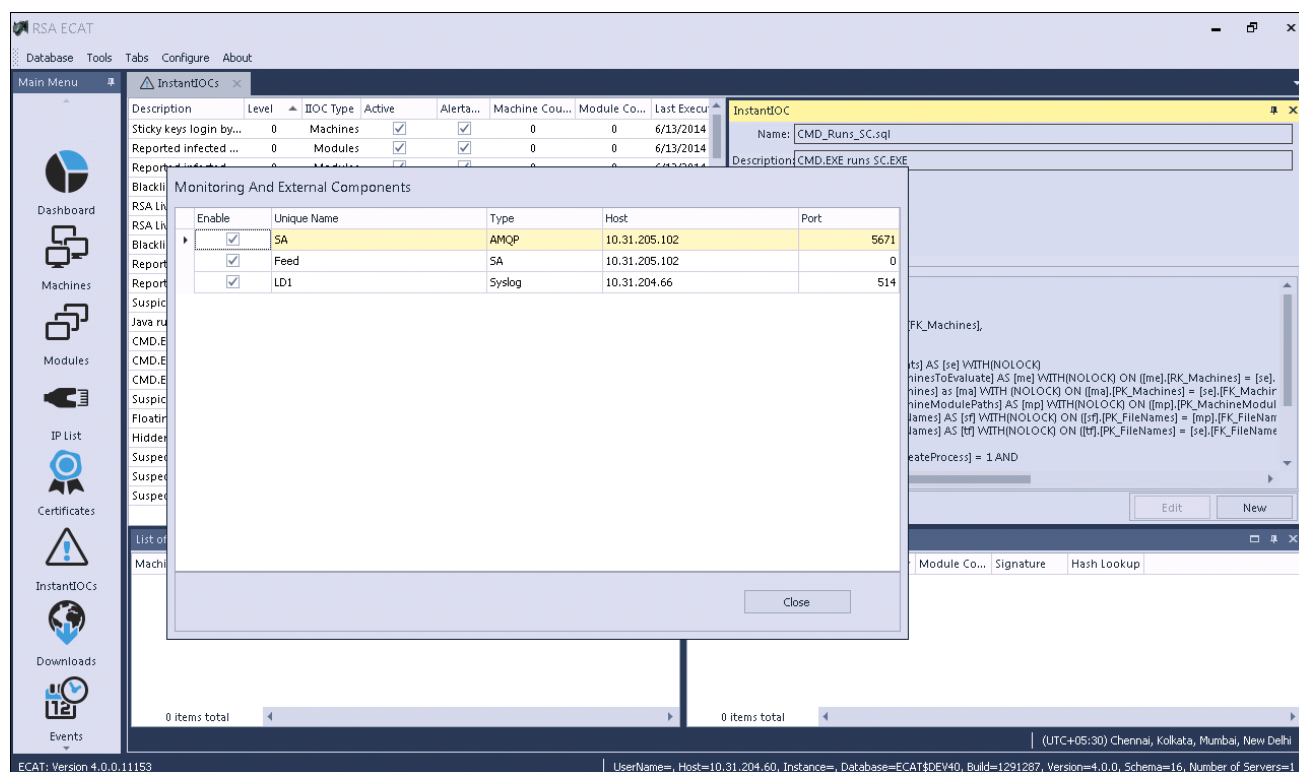
2. Configurez ECAT afin qu'il envoie la sortie syslog vers Security Analytics et qu'il génère des alertes eCAT dans Log Decoder.
3. (Facultatif) Modifiez le mappage de table dans `table-map-custom.xml` et `index-concentrator-custom.xml` pour ajouter des champs basés sur les préférences utilisateur pour les métadonnées à mapper dans Security Analytics.

Configurer ECAT afin d'envoyer la sortie Syslog vers Security Analytics

Pour ajouter Log Decoder en tant que composant externe Syslog et générer des alertes ECAT vers Log Decoder :

Pour ECAT version 4.0

1. Ouvrez l'interface utilisateur ECAT et connectez-vous en utilisant les informations d'identification adéquates.
2. Dans la barre de menus, sélectionnez **Configurer > Composants de surveillance et externes**.
3. Cliquez avec le bouton droit sur la boîte de dialogue, puis sélectionnez **Ajouter un composant**. Dans la boîte de dialogue, renseignez les champs requis pour activer les messages Syslog :
Type de composant = Syslog
Nom unique = Nom descriptif du Log Decoder
IP = Adresse IP du RSA Log Decoder
Port = 514
4. Cliquez sur **Paramètres**.
5. Dans la boîte de dialogue **Configurer Syslog**, sélectionnez **UDP** ou **TCP** selon les besoins de votre serveur syslog comme protocole de transport.
6. Cliquez deux fois sur **Enregistrer** pour fermer les boîtes de dialogue.
7. Cochez la case **Activer** pour activer le composant.
8. Cliquez sur **Fermer** pour terminer.



9. Cliquez sur **IOC instantanés** et modifiez les paramètres afin que des alertes puissent se déclencher.

The screenshot shows the RSA ECAT interface. The main window displays a table of IOC configurations. The InstantIOCs window is open, showing configuration for 'CMD_Runs_SC.sql' with a description 'CMD.EXE runs SC.EXE'. The query editor shows a complex SQL query for detecting suspicious processes. Below the main table, there are two smaller tables: 'List of Machines with Current IOC' and 'List of Modules with Current IOC', both currently empty.

Lorsque les IOC instantanés sont déclenchés, les alertes Syslog du serveur ECAT sont envoyées au Log Decoder. Les alertes Log Decoder sont alors ajoutées au Concentrator. Ces événements sont alors injectés au Concentrator comme métadonnées.

Pour ECAT version 4.1

1. Ouvrez l'interface utilisateur ECAT et connectez-vous en utilisant les informations d'identification adéquates.
2. Dans la barre de menus, sélectionnez **Configurer > Composants de surveillance et externes**. La boîte de dialogue Configuration des composants externes s'affiche.

3. Dans **SYSLOG Server**, cliquez sur **+**.
La boîte de dialogue SYSLOG Server s'affiche.

The screenshot shows the 'SYSLOG Server' configuration dialog. At the top, there is a title bar with a hamburger menu icon on the left and three icons (+, -, home) on the right. Below the title bar, there is a green 'ON' toggle switch and a red-bordered text input field. The main area is titled 'Syslog Connection' and contains three fields: 'Server Hostname/IP:' with an empty text box, 'Port:' with a dropdown menu showing '514', and 'Transport Protocol:' with radio buttons for 'TCP' and 'UDP' (selected). At the bottom left is a 'Test Settings' button, and at the bottom right are 'Cancel' and 'Save' buttons.

4. Renseignez les champs obligatoires pour activer les messages Syslog :
Activé = Nom descriptif du Log Decoder
Nom d'hôte/IP du serveur = adresse DNS ou IP du Log Decoder RSA
Port = 514
Protocole de transport = sélectionnez **UDP** ou **TCP** comme protocole de transport de votre serveur Syslog.
5. Cliquez sur **Enregistrer**.

6. Cliquez sur **IOC instantanés** et modifiez les paramètres afin que des alertes puissent se déclencher.

Lorsque les IOC instantanés sont déclenchés, les alertes Syslog du serveur ECAT sont envoyées au Log Decoder. Les alertes Log Decoder sont alors ajoutées au Concentrator. Ces événements sont alors injectés au Concentrator comme métadonnées.

Modifiez le mappage de table dans table-map-custom.xml

Dans le fichier table-map.xml fourni par RSA par défaut, les clés méta du fichier table-map.xml sont définies sur [Transitoire](#). Dans le but d'afficher les clés méta dans Investigation, les clés doivent être définies sur [Aucun](#). Pour apporter des modifications au mappage, vous devez créer une copie du fichier intitulé table-map-custom.xml, dans Log Decoder et définir les clés méta sur [Aucun](#).

Voici la liste des clés méta de table-map.xml.

Champs ECAT	Mappage de Security Analytics	Transitoire dans Security Analytics
agentid	client	Non
CEF Header Hostname Field	alias.host	Non
CEF Header Product Version	version	Oui
CEF Header Product Name	Product	Oui
CEF Header Severity	severity	Oui
CEF Header Signature ID	event.type	Non

Champs ECAT	Mappage de Security Analytics	Transitoire dans Security Analytics
CEF Header Signature Name	event.desc	Non
destinationDnsDomain	ddomain	Oui
deviceDnsDomain	domain	Oui
dhost	host.dst	Non
dst	ip.dst	Non
end	endtime	Oui
fileHash	checksum	Oui
fname	filename	Non
fsize	filename.size	Non
gatewayip	gateway	Oui
instantIOCLevel	threat.desc	Non
instantIOCName	threat.category	Oui
machineOU	dn	Oui
machineScore	risk.num	Non
md5sum	checksum	Oui
os	OS	Oui
port	ip.dstport	Non
protocol	protocol	Oui
Raw Message	msg	Oui
remoteip	stransaddr	Oui
rt	alias.host	Non
sha256sum	checksum	Oui
shost	host.src	Non
smac	eth.src	Oui
src	ip.src	Non
start	starttime	Oui

Champs ECAT	Mappage de Security Analytics	Transitoire dans Security Analytics
suser	user.dst	Non
timezone	timezone	Oui
totalreceived	rbytes	Oui
totalsent	bytes.src	Non
useragent	user.agent	Oui
userOU	org	Oui

Ces sept clés ne se trouvent pas dans `table-map.xml`. Pour utiliser ces clés dans Security Analytics, vous devez les ajouter à `table-map-custom.xml`, et définir les balises sur `Aucun`.

Champs ECAT	Mappage de Security Analytics	Transitoire dans Security Analytics
moduleScore	cs.modulescore	Oui
moduleSignature	cs.modulesign	Oui
Target module	cs.targetmodule	Oui
YARA result	cs.yarareult	Oui
Source module	cs.sourcemodule	Oui
OPSWATResult	cs.opswatresult	Oui
Bit9Status	cs.bit9status	Oui

Voici les entrées à ajouter à `table-map-custom.xml` si nécessaire.

```
<mapping envisionName="cs_bit9status" nwName="cs.bit9status" flags="None"
envisionDisplayName="Bit9Status"/>
<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"/>
```

Note: Redémarrez le Log Decoder ou rechargez les parsers de logs afin que les changements prennent effet.

Configurer le service Security Analytics Concentrator

1. Connectez-vous à Security Analytics et accédez à **Administration > Services**.
2. Sélectionnez un concentrateur dans la liste, puis sélectionnez **Vue > Config**.
3. Sélectionnez l'onglet **Fichiers**, et dans le menu déroulant **Fichiers à modifier**, sélectionnez **index-concentrator-custom.xml**.
4. Ajoutez les clés méta ECAT au fichier et cliquez sur **Appliquer**. Vérifiez que ce fichier contient déjà les sections XML et si ce n'est pas le cas, ajoutez-les.
5. Redémarrez le Concentrator.
6. Pour ajouter le Concentrator en tant que source de données dans Reporting Engine, dans Administration > vue Services, sélectionnez Reporting Engine et **RE > Vue > Config > Sources**.
Les méta ECAT sont générées dans Reporting Engine, et vous pouvez exécuter des rapports en sélectionnant les clés méta appropriées.

Exemple

Note: Les lignes suivantes sont données à titre d'exemple. Assurez-vous que les valeurs sont adaptées à votre configuration et que les noms de colonnes compris dans la définition de feed sont :
description est le nom de la clé méta que vous souhaitez afficher dans Security Analytics Investigation.
level est "IndexValues"
name est le nom de la métaclé dans le tableau ci-dessous

```
<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="Bit9Status" format="Text" level="IndexValues" name="cs.bit9status"
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>
```

Clés méta ECAT

Voici les noms et descriptions pour les clés méta utilisées dans l'exemple de fichier d'index.

Nom de clé méta Security Analytics	Utilisez	Clé méta ECAT (nom)
MachineName	Nom d'hôte de l'agent Windows	alias.host
LocalIp	Adresse IPv4	index
Remotelp	Adresse IP distante telle qu'elle est vue par le routeur	stransaddr
GatewayIp	Adresse IP de la passerelle	gateway
MacAddress	Adresse MAC	eth.src
OperatingSystem	Système d'exploitation utilisé par l'agent Windows	OS
AgentID	ID d'agent de l'hôte (ID unique attribué à l'agent)	client
ConnectionUTCTime	La dernière fois que l'agent s'est connecté au serveur ECAT	ecat.ctime
Domaine source	Domaine	domain.src
ScanUTC time	La dernière fois que l'agent a été analysé	ecat.stime
Note de l'ordinateur	Score de l'agent indiquant le niveau de suspicion	risk.num

Résultat

Les analystes peuvent :

- Créer des alertes Security Analytics en fonction des événements ECAT en configurant des événements ECAT comme source d'enrichissement.
- Créer des règles ESA en utilisant les méta ECAT comme décrit dans la rubrique [Ajouter des règles à la Bibliothèque de règles](#).
- Créer des rapports sur les événements ECAT comme décrit dans la rubrique [Règles](#).
- Afficher des alertes ECAT dans Incident Management comme décrit dans la rubrique [Vue Alertes](#).
- Afficher les clés méta ECAT dans Investigation avec les clés méta standard SA Core comme décrit dans la rubrique [Mener une procédure d'enquête](#).