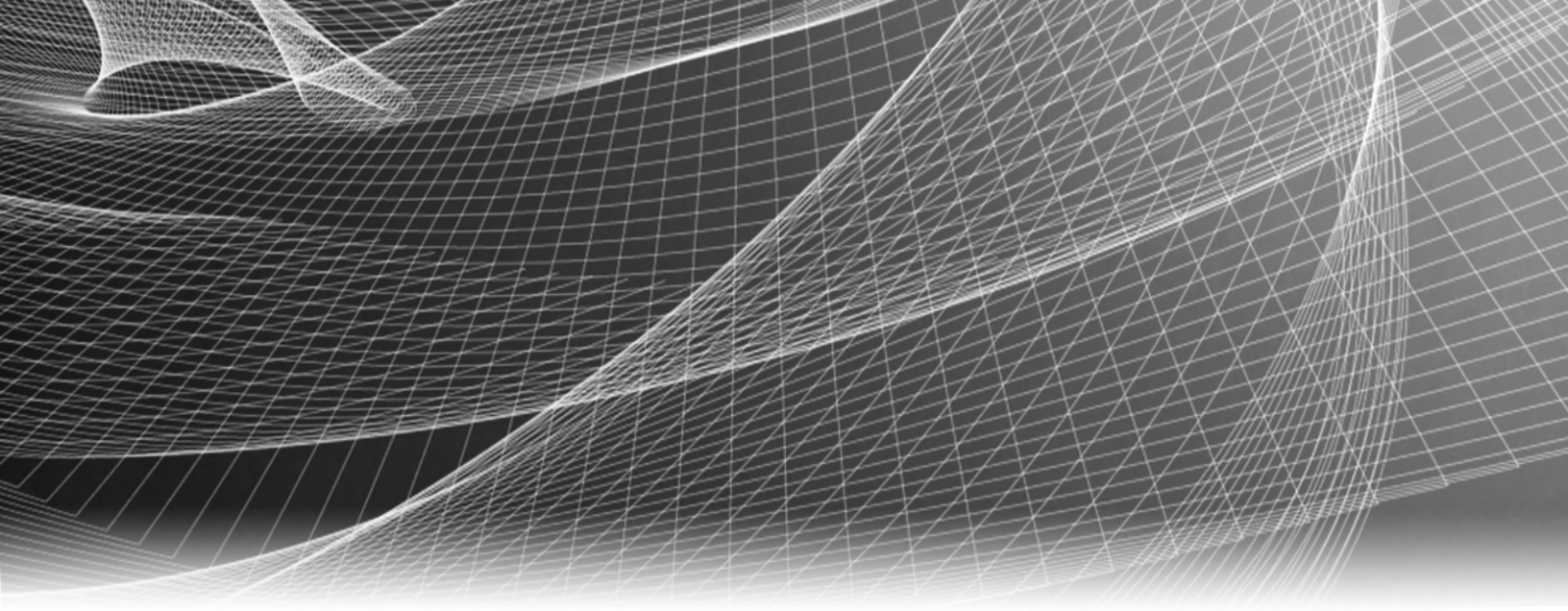


RSA Security Analytics

Guide de configuration de Context Hub pour la Version 10.6

RSA

EMC²

Trademarks

License Agreement

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.

Guide de configuration de Context Hub

RSA

Guide de configuration de Context Hub

Ce guide présente le fonctionnement du service Context Hub et fournit une liste de contrôle afin de guider les utilisateurs tout au long de la configuration. Chaque tâche de la liste de contrôle fait l'objet d'une description dans une procédure distincte, et une rubrique de référence séparée donne des détails sur les paramètres de configuration.

.

Last Modified: August 10 2016, 9:33AM

RSA

Présentation du service Context Hub

Cette rubrique présente le service Context Hub.

Context Hub est un nouveau service de RSA Security Analytics qui comporte une fonctionnalité de recherche de fournisseur d'enrichissement dans les vues Procédure d'enquête. Ce service comporte un indicateur d'enrichissement en ligne automatisé ainsi qu'une fonctionnalité de recherche de fournisseur d'enrichissement à la demande. Les analystes peuvent utiliser les informations supplémentaires envoyées par le service Context Hub comme informations et renseignements contextuels pendant la procédure d'enquête. Les sources des données d'enrichissement sont Incident Management, les listes personnalisées et ECAT.

Le service Context Hub :

- Est hébergé sur Event Stream Analysis (ESA).
- Prend en charge par défaut les recherches de fournisseur d'enrichissement pour les types de métadonnées suivants : Adresse IP, Utilisateurs, Domaines, Adresse MAC, Nom de fichier, Hachage de fichier et Hôtes.

Objectif

Le service Context Hub rassemble des informations issues de plusieurs sources de données dans Investigation pour permettre aux analystes de prendre de meilleures décisions durant leurs procédures d'enquête. En consultant les valeurs méta et les informations contextuelles dans une même interface, les analystes peuvent privilégier et identifier les domaines clés. Par exemple, les incidents et alertes récemment générés depuis Incident Management et qui englobent une valeur méta donnée s'affichent lorsque l'analyste effectue une opération de recherche contextuelle pour cette valeur méta.

Les listes personnalisées telles que les listes noires, les listes blanches ou les listes de surveillance peuvent être créées par les analystes. Vous pouvez remplir ces listes personnalisées à l'aide d'éléments, soit par importation de fichiers CSV, soit par ajout de métavaleurs via l'option **Ajouter à la liste/Supprimer de la liste** des vues Investigation. Les listes personnalisées deviennent automatiquement des sources de données pour les méta-indicateurs, ainsi que pour les recherches de fournisseur d'enrichissement à la demande.

Ces listes peuvent aussi assurer une meilleure interaction entre les analystes. Par exemple, les analystes de niveau 2 peuvent indiquer des éléments suspects et les analystes de niveau 1 peuvent utiliser ces connaissances pour confirmer des incidents ou en créer selon les besoins.

Avec les informations contextuelles issues d'ECAT, les analystes peuvent obtenir les indicateurs de module de point d'extrémité et de machine.

Last Modified: August 10 2016, 9:33AM

Workflow pour les administrateurs

La vue Configuration des services du service Context Hub permet aux administrateurs de configurer les sources de données pour le service Context Hub. Pour plus d'informations, reportez-vous à l'Étape 2. Configurer les sources de données pour Context Hub.

Les administrateurs peuvent configurer les recherches de contexte pour les clés méta personnalisées si nécessaire. Ils peuvent aussi importer ou exporter les listes qui peuvent être utilisées par l'analyste.

Workflow pour les analystes

Dans Investigation > vue Naviguer, les valeurs méta avec des informations contextuelles sont mises en évidence avec un arrière-plan gris. Il existe aussi des indicateurs en ligne pour les valeurs méta mises en évidence. Ils indiquent les sources pour lesquelles les informations contextuelles sont disponibles.

Note: Les valeurs méta mises en évidence n'auront pas toutes des informations de recherche de contexte. Cela provient du fait que les informations contextuelles peuvent avoir changées depuis le moment où elles ont été marquées comme disponibles.

Si les valeurs méta n'ont pas d'indicateurs de contexte, les analystes peuvent lancer une requête à la demande pour vérifier si les informations contextuelles peuvent être disponibles. Pour cela, ils peuvent cliquer avec le bouton droit de la souris sur une valeur méta qui prend en charge la recherche contextuelle et choisir ensuite l'option de menu **Recherche contextuelle**.

L'option Recherche contextuelle est aussi prise en charge dans la vue Procédure d'enquête > Événements. Mais les indicateurs en ligne ne sont pas disponibles dans cette vue. Vous devez donc lancer une recherche à la demande sur les valeurs méta.

Cliquez avec le bouton droit de la souris et choisissez l'option Recherche contextuelle. Un panneau Recherche contextuelle s'ouvre dans la partie droite des vues Procédure d'enquête. Il affiche les informations contextuelles issues des sources configurées liées aux valeurs méta. Pour obtenir des informations supplémentaires sur le contexte, cliquez sur les liens correspondants sur les résultats de recherche affichés dans le panneau Recherche contextuelle. Pour plus d'informations, reportez-vous à Afficher un contexte supplémentaire pour un point de données.

Les analystes peuvent ajouter ou supprimer une valeur méta à une liste nouvelle ou existante en cliquant avec le bouton droit de la souris sur la même valeur méta, puis en sélectionnant l'option **Ajouter à la liste / Supprimer de la liste**.

Rôles et autorisations de l'utilisateur

Les analystes qui utilisent Security Analytics Investigation doivent avoir les autorisations appropriées pour effectuer la recherche contextuelle et utiliser les listes personnalisées.

Last Modified: August 10 2016, 9:33AM

Deux nouvelles autorisations `Recherche contextuelle` et `Gérer la liste à partir d'Investigation` ont été ajoutées pour Investigation dans Security Analytics 10.6. Elles sont ajoutées aux rôles Analyste, Responsables du SOC et Analystes Malware par défaut. Cependant, lors de la mise à niveau vers Security Analytics 10.6 à partir de versions précédentes, l'administrateur doit configurer ces autorisations. Pour plus d'informations sur les rôles et les autorisations, reportez-vous à Autorisations du rôle et Gérer les utilisateurs avec des rôles et des autorisations.

L'analyste doté de l'autorisation `Recherche contextuelle` peut effectuer une recherche contextuelle dans les vues Procédure d'enquête. Pour plus d'informations, reportez-vous à Afficher un contexte supplémentaire pour un point de données.

L'analyste doté de l'autorisation `Gérer la liste à partir d'Investigation` peut gérer des listes et des valeurs de liste dans les vues Procédure d'enquête. Pour plus d'informations, reportez-vous à Gérer les listes et les valeurs de liste dans Investigation.

Exemple

Les cas d'utilisation suivants expliquent certains scénarios où le service Context Hub est utilisé avec des sources de données comme Incident Management, ECAT et les listes personnalisées.

Cas d'utilisation d'Incident Management dans le service Context Hub

Lorsqu'un analyste de niveau 2 explore les valeurs méta pour trouver de nouveaux indicateurs de compromis, les commentaires fournis par la source d'enrichissement de contexte Incident Management sont très utiles. L'analyste peut constater la présence d'une alerte ou d'un incident existant lié à la valeur méta sélectionnée. Cette possibilité permet aux analystes d'ignorer les valeurs méta pour lesquelles il existe déjà des incidents et de se concentrer sur la recherche de nouveaux indicateurs de compromis spécifiques.

Les informations deviennent disponibles dans la même vue Investigation > Naviguer. L'accessibilité de ces informations est efficace, car l'analyste peut accéder aux données d'enrichissement sans naviguer d'une vue à l'autre ou recourir à un outil différent.

Cas d'utilisation d'ECAT dans le service Context Hub

Lorsqu'un analyste de niveau 2 affiche les résultats de recherche dans les vues Procédure d'enquête, il peut afficher les adresses IP, les hôtes et l'adresse MAC qui exécutent les agents ECAT. Cela facilite plus que jamais les compromis éventuels, directement dans les vues de Security Analytics Investigation. Les détails de la recherche contextuelle comportent des informations générales liées au point d'extrémité qui exécute l'agent ECAT, ce qui permet à l'analyste de comprendre si le système est compromis ou non. Si l'analyste a besoin de davantage d'informations sur le risque et qu'IIOC effectue une évaluation à cet égard, il peut afficher l'état et les remarques documentés dans ECAT, ainsi que les modules principaux par valeur IOC. Si d'autres détails sont nécessaires, l'analyste peut cliquer sur les détails fournis dans le panneau de recherche contextuelle pour accéder directement à l'interface utilisateur ECAT. Il peut ensuite

utiliser les machines indiquées comme points de pivot pour ses enquêtes afin de voir les autres machines avec lesquelles le système a communiqué pour rechercher les autres hôtes compromis.

Cas d'utilisation de liste dans le service Context Hub

Cas d'utilisation 1

Un analyste de niveau 3 explore Incident Management pour rechercher le contexte des adresses IP et des domaines associés aux sessions suspectes. Si n'existe aucun incident ou aucune alerte associée et que l'adresse IP et le domaine soumis à l'enquête doivent être surveillés afin de détecter un comportement anormal.
L'analyste peut inclure ces valeurs méta dans une liste. Par exemple, pour améliorer la visibilité des adresses IP suspectes, l'analyste peut ajouter les mêmes valeurs méta à deux listes. La première liste concerne les domaines suspectés d'être liés aux connexions de commande et contrôle, et l'autre liste concerne les adresses IP liées aux connexions de chevaux de Troie autorisant un accès à distance.

Or, un analyste de niveau 2 peut utiliser cette liste de contextes pour repérer les indicateurs de compromis. L'analyste peut aussi exporter les listes au format CSV et les envoyer à l'analyste de niveau 1 pour créer des incidents en vue de leur suivi et de leur analyse.

Cas d'utilisation 2

Comme l'analyste de niveau 3 a créé un contenu personnalisé pour détecter certains indicateurs de compromis, il souhaite fournir d'autres détails sur ce nouveau contenu pour guider les autres analystes lorsqu'ils rencontrent les nouvelles valeurs méta générées. Il peut créer trois nouvelles listes (liste critique personnalisée, liste suspecte personnalisée et consultative personnalisée) dans lesquelles sont classées les nouvelles valeurs méta qu'un analyste verra éventuellement lorsque le nouveau contenu aura été déclenché. La description fournie par l'analyste pour chaque liste apporte un historique aux autres analystes concernant ce que les valeurs méta illustrent et l'action nécessaire à entreprendre lorsqu'elles sont repérées dans la procédure d'enquête. Elle ne remplace pas la création d'un incident ou d'une alerte, mais constitue le moyen de fournir d'autres détails à l'analyste lorsqu'il voit ces nouvelles valeurs méta dans la procédure d'enquête pour la première fois.

Last Modified: August 10 2016, 9:33AM

Configuration basique

L'administrateur doit effectuer chaque étape dans l'ordre approprié pour configurer le service. Après la configuration initiale du service Context Hub, vous pouvez afficher du contexte supplémentaire pour un point de données à partir des vues Investigation. Pour des instructions, consultez Afficher le contexte supplémentaire d'un point de données.

.

Last Modified: August 10 2016, 9:33AM

RSA

Étape 1. Ajouter le service Context Hub

Cette rubrique fournit des informations sur le mode d'ajout du service Context Hub sur un hôte Event Stream Analysis (ESA).

Dans Security Analytics 10.6, le service Context Hub est pré-installé sur l'hôte ESA, mais est désactivé par défaut. Utilisez la procédure de cette rubrique pour activer le service Context Hub.

Note: Vous ne pouvez avoir qu'une seule instance de service Context Hub activée dans votre déploiement Security Analytics. En cas d'existence de plusieurs services ESA dans Security Analytics, vous devez choisir l'hôte ESA approprié au service Context Hub. Un minimum de 8 Go d'espace est requis pour configurer Context Hub sur l'hôte ESA.

Conditions préalables

Vérifiez que cet hôte ESA avec SA 10.6 est disponible. Si une ancienne version est utilisée, l'administrateur doit effectuer au préalable une mise à niveau de l'hôte ESA vers la version 10.6.

Procédure

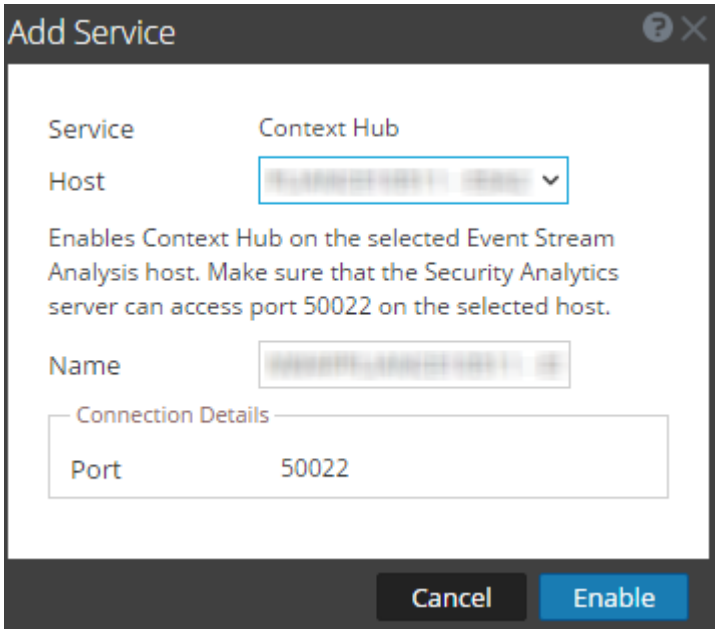
Lorsque vous accédez au panneau **Administration > Services** , si le service Context Hub n'est pas activé, la boîte de dialogue **Activer Context Hub** s'affiche. Pour plus d'informations, reportez-vous à la rubrique Boîte de dialogue Activer Context Hub.

Pour ajouter le service Context Hub :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
   La vue Services s'affiche.
2. Dans le panneau Services, sélectionnez + **> Context Hub**.
   La boîte de dialogue **Ajouter un service** s'affiche.

Last Modified: August 10 2016, 9:33AM

3. Sélectionnez l'hôte ESA dans la liste des hôtes compatibles.
   Les autres champs tels que **Nom** et **Port** sont remplis automatiquement. Le port par défaut est **50022**.



4. Cliquez sur **Activer**.
   Le service Context Hub est ajouté à Security Analytics.

Note: Vous ne pouvez avoir qu'une seule instance de service Context Hub activée dans votre déploiement Security Analytics. Si vous exécutez plusieurs services ESA et que vous souhaitez leur appliquer la fonctionnalité Context Hub, vous devez configurer la connexion aux services ESA qui exécutent le service Context Hub. Pour obtenir des instructions, consultez la rubrique Configurer la connexion d'un service ESA au service Context Hub sur un autre service ESA.

Last Modified: August 10 2016, 9:33AM

Étape 2. Configurer les sources de données pour Context Hub

Cette procédure est requise pour ajouter une source de données pour Context Hub et configurer les types de réponse pour la source de données. Vous pouvez ajouter les sources de données prises en charge (Incident Management, ECAT et les listes personnalisées) pour rechercher les informations contextuelles.

Conditions préalables

Vérifiez que le service Context Hub est activé.

Last Modified: August 10 2016, 9:33AM

RSA

Configurer Incident Management comme source de données pour Context Hub

Cette rubrique décrit la procédure permettant de configurer Incident Management en tant que source de données pour Context Hub.

Pour utiliser le service Context Hub afin qu'il récupère des informations contextuelles à partir du service Incident Management, vous devez configurer Incident Management en tant que source de données pour Context Hub. Utilisez les procédures de cette rubrique pour ajouter Incident Management en tant que source de données pour le service Context Hub et configurer les réponses (si nécessaire) pour Incident Management.

Les réponses sont différents types d'informations contextuelles disponibles pour une source de données. La configuration de ces réponses pour la source Incident Management contrôle ce qui apparaît dans le panneau Recherche contextuelle qui s'affiche dans les vues Investigation lorsqu'une recherche contextuelle est réalisée. Les types de réponse pour la source de données Incident Management sont **Incidents** et **Alertes**.

Les réponses pour chaque source de données sont déjà configurées avec des valeurs par défaut afin d'optimiser la performance. Vous pouvez afficher ou modifier les valeurs par défaut en utilisant la procédure de cette rubrique.

Conditions préalables

Vérifiez les points suivants :

- Context Hub est activé et le service est disponible dans la vue Administration > Services de Security Analytics.
- Le service Incident Management est disponible et le mot de passe de la base de données Incident Management est mis de côté.

Procédures

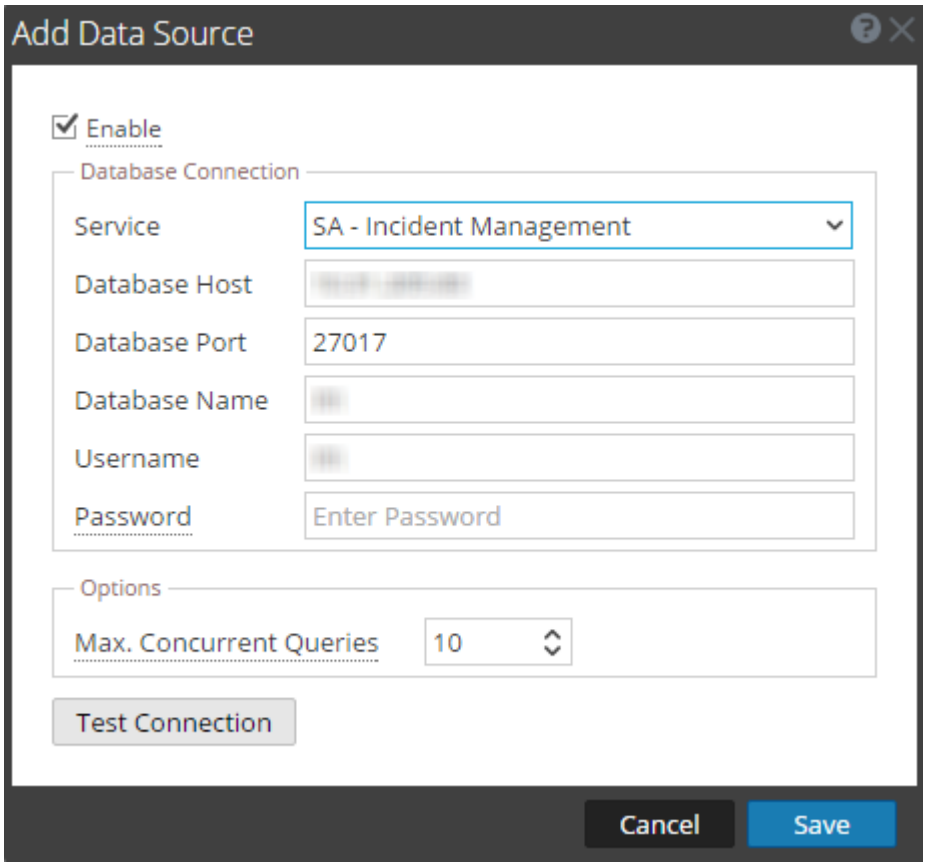
Ajouter une source de données Incident Management

Pour ajouter Incident Management en tant que source de données pour Context Hub :

1. Dans le menu Security Analytics, sélectionnez **Administration > Services**.
   La vue Services s'affiche.
2. Dans le panneau Services, sélectionnez le service Context Hub et cliquez sur  **> Vue > Configuration.**
   La vue Configuration des services de Context Hub s'affiche.

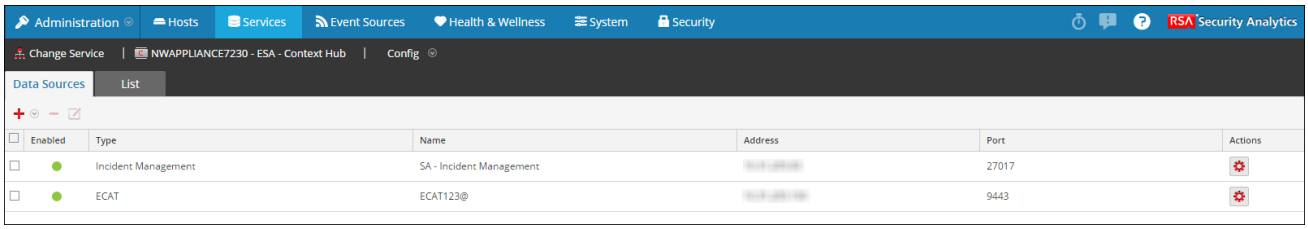
Last Modified: August 10 2016, 9:33AM

3. Sous l'onglet **Sources de données**, cliquez sur  **> Incident Management**.
   La boîte de dialogue **Ajouter une source de données** s'affiche.



4. Fournissez les détails suivants sur la connexion de la base de données :
   - **Activer** : sélectionnez **Activer** pour activer la source de données Incident Management. Cette option est activée par défaut (cochée).
   - **Service** : sélectionnez le service Gestion des incidents disponible.
     Les valeurs sont générées automatiquement pour les champs suivants. Modifiez les valeurs si nécessaire.
     - **Hôte de base de données :** nom d'hôte ou adresse IP de la base de données Incident Management.
     - **Port de la base de données :** le port par défaut est 27017.
     - **Nom de la base de données :** le nom par défaut de la base de données est im.
     - **Nom d'utilisateur :** le nom d'utilisateur par défaut est im.
   - **Mot de passe** : saisissez le mot de passe pour se connecter à la base de données Incident Management. Le mot de passe par défaut est im.
   - **Nbre max. de requêtes simultanées** : vous pouvez configurer le nombre maximum de requêtes simultanées définies par le service Context Hub à exécuter sur les sources de données configurées. La valeur par défaut est 10.
5. Cliquez sur **Tester la connexion** pour tester la connexion entre Context Hub et la source de données.
6. Cliquez sur **Enregistrer** pour enregistrer les paramètres.
   Incident Management est ajouté en tant que source de données pour le Context Hub configuré. La source de données Incident

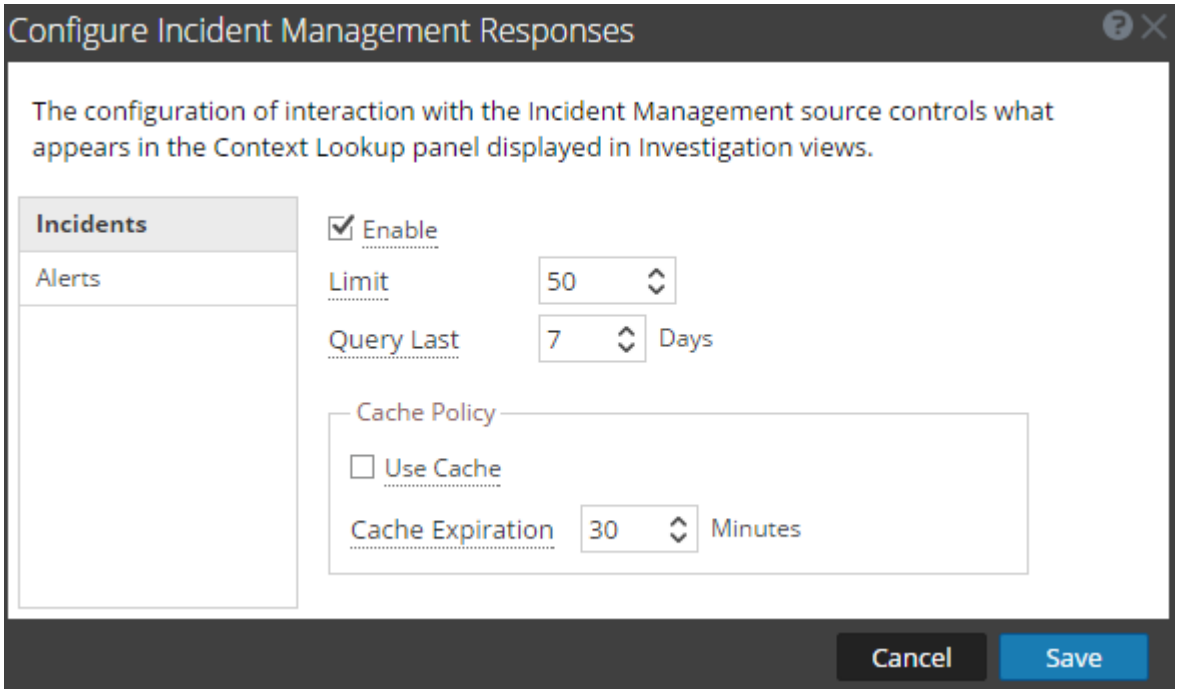
Management s'affiche sous l'onglet **Sources de données**.



Configurer les réponses pour la source de données Incident Management

Pour afficher/modifier les réponses pour la source de données Incident Management :

1. Sous l'onglet **Sources de données**, sélectionnez la source Incident Management et cliquez sur .
   La boîte de dialogue **Configurer les réponses Incident Management** s'affiche.



2. Dans le panneau de gauche, sélectionnez chaque réponse (Incidents ou Alertes) pour afficher et modifier les paramètres.
3. Configurez les champs suivants :

Champ	Description
Activer	Cette option est désactivée par défaut (cochée) et peut être utilisée pour activer ou désactiver la réponse sélectionnée.
Limite	Saisissez le nombre maximum d'enregistrements (incidents ou alertes) à afficher dans le panneau **Recherche contextuelle** des vues Investigation

	lorsque la recherche contextuelle est réalisée. La valeur par défaut est **50**. Par exemple, si la limite est fixée à 10, seuls 10 enregistrements s'affichent, selon un critère de temps puis de priorité, pour les incidents et la gravité des alertes.
Requête dans les derniers	Sélectionnez la période (en jours) pendant laquelle les informations contextuelles du type de réponse sélectionné seront collectées. La valeur par défaut est **7 derniers jours**.
Utiliser le cache	Cochez la case pour activer le cache de réponse. Lorsque cette option est activée, Context Hub stocke les résultats de la recherche dans le cache. Les requêtes suivantes pour la même valeur méta sont gérées à partir du cache pour la durée configurée (Expiration du cache).
Expiration du cache	Période (en minutes) pendant laquelle les résultats de la recherche sont stockés dans le cache lorsque la recherche contextuelle est réalisée. La valeur par défaut est **30 minutes**.

4. Cliquez sur **Enregistrer** pour enregistrer les paramètres de la source de données Incident Management.

Étapes suivantes

Après avoir terminé la configuration, vous pouvez utiliser l'option Recherche contextuelle dans la vue Examiner > Naviguer ou la vue Investigation > Événements pour récupérer des informations contextuelles. Pour obtenir des instructions, consultez la rubrique Afficher du contexte supplémentaire pour un point de données.

Last Modified: August 10 2016, 9:33AM

Configurer RSA ECAT comme source de données pour Context Hub

Cette rubrique décrit la procédure permettant de configurer ECAT en tant que source de données pour Context Hub.

Pour utiliser le service Context Hub afin qu'il récupère des informations contextuelles à partir d'ECAT, vous devez configurer ECAT en tant que source de données pour Context Hub. Utilisez les procédures de cette rubrique pour ajouter ECAT en tant que source de données pour le service Context Hub et configurer les réponses (si nécessaire) pour ECAT.

Les réponses sont différents types d'informations contextuelles disponibles pour une source de données. La configuration de ces réponses pour la source ECAT contrôle ce qui apparaît dans le panneau Recherche contextuelle qui s'affiche dans les vues Investigation lorsqu'une recherche contextuelle est réalisée. Les types de réponses pour la source de données ECAT sont les machines, les modules et les indicateurs de compromission (IOC) instantanés.

Les réponses pour chaque source de données sont déjà configurées avec des valeurs par défaut afin d'optimiser la performance. Vous pouvez afficher ou modifier les valeurs par défaut en utilisant la procédure de cette rubrique.

Conditions préalables

Vérifiez les points suivants :

- Context Hub est activé et le service est disponible dans la vue Administration > Services de Security Analytics.
- RSA ECAT (v4.1.1 et supérieure) est installé et configuré.
  Les documents RSA ECAT 4.1.1 donnent des informations détaillées sur l'installation et la configuration d'ECAT. Reportez-vous aux documents ECAT disponibles dans https://knowledge.rsasecurity.com.

Procédures

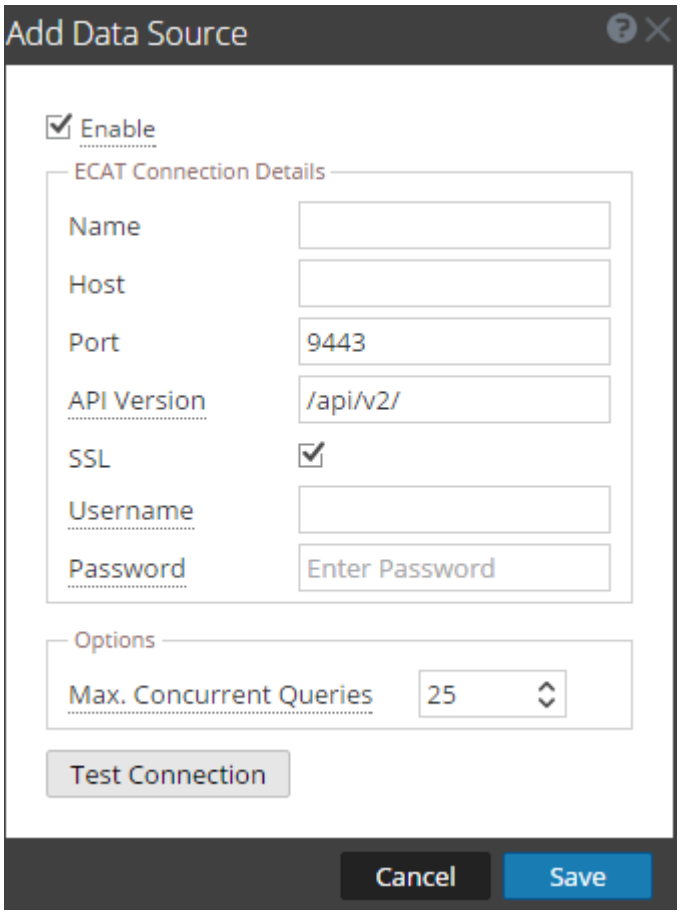
Ajouter une source de données RSA ECAT

Pour ajouter RSA ECAT en tant que source de données pour Context Hub :

1. Dans le menu Security Analytics, sélectionnez **Administration > Services**.
   La vue Services s'affiche.
2. Dans le panneau **Services**, sélectionnez le service Context Hub, puis  **> Vue > Configuration.**
   La vue Configuration des services s'affiche.

Last Modified: August 10 2016, 9:33AM

3. Sous l'onglet **Sources de données**, cliquez sur **> ECAT**.
La boîte de dialogue **Ajouter une source de données** s'affiche.



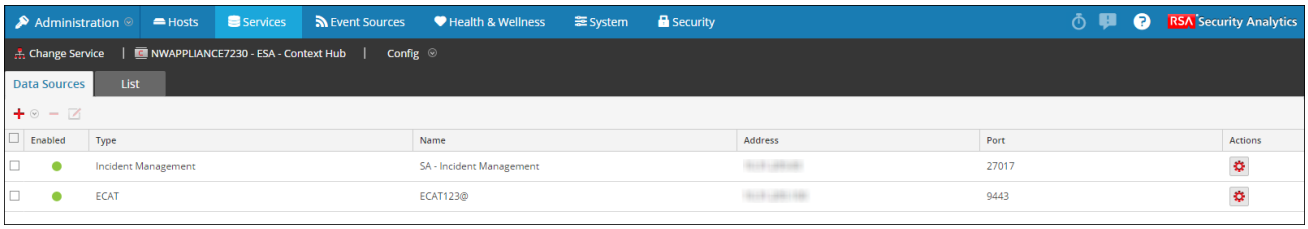
4. Fournissez les informations suivantes :

Champ	Description
Activer	Sélectionnez **Activer** pour activer la source de données ECAT. Cette option est activée par défaut (cochée).
Nom	Donnez un nom à la source de données ECAT.
Hôte	Saisissez le nom d'hôte ou adresse IP où le serveur ECAT API est installé.
Port	Le port par défaut est 9443.
Version API	La version API par défaut (/api/v2) prend en charge la connexion à ECAT 4.1.1 et versions ultérieures
SSL	Sélectionnez SSL si vous souhaitez que Security Analytics communique avec l'hôte via SSL. Cette option est activée par défaut.
Nom d'utilisateur	Saisissez le nom d'utilisateur du serveur ECAT API.
Mot de passe	Saisissez le mot de passe du serveur ECAT API.

Last Modified: August 10 2016, 9:33AM

Nbre max. de requêtes simultanées	Vous pouvez configurer le nombre maximum de requêtes simultanées définies par le service Context Hub à exécuter sur les sources de données configurées. La valeur par défaut est 25.

5. Cliquez sur **Tester la connexion** pour tester la connexion entre Context Hub et la source de données ECAT.
6. Cliquez sur **Enregistrer** pour enregistrer les paramètres.
   ECAT est ajouté en tant que source de données pour Context Hub. La source de données ECAT s'affiche dans l'onglet **Sources de données**.



Modifier le mot de passe administrateur ECAT

L'administrateur du serveur API assigne les rôles et autorisations aux nouveaux utilisateurs. L'administrateur n'est pas créé par défaut au moment de l'installation.

Le nom d'utilisateur et mot de passe de l'administrateur ECAT sont les suivants :

- Nom d'utilisateur : admin
- Mot de passe : il doit être défini à l'aide de la commande suivante :
  `ApiServer.exe /setadminpswd A_Strong_Password`

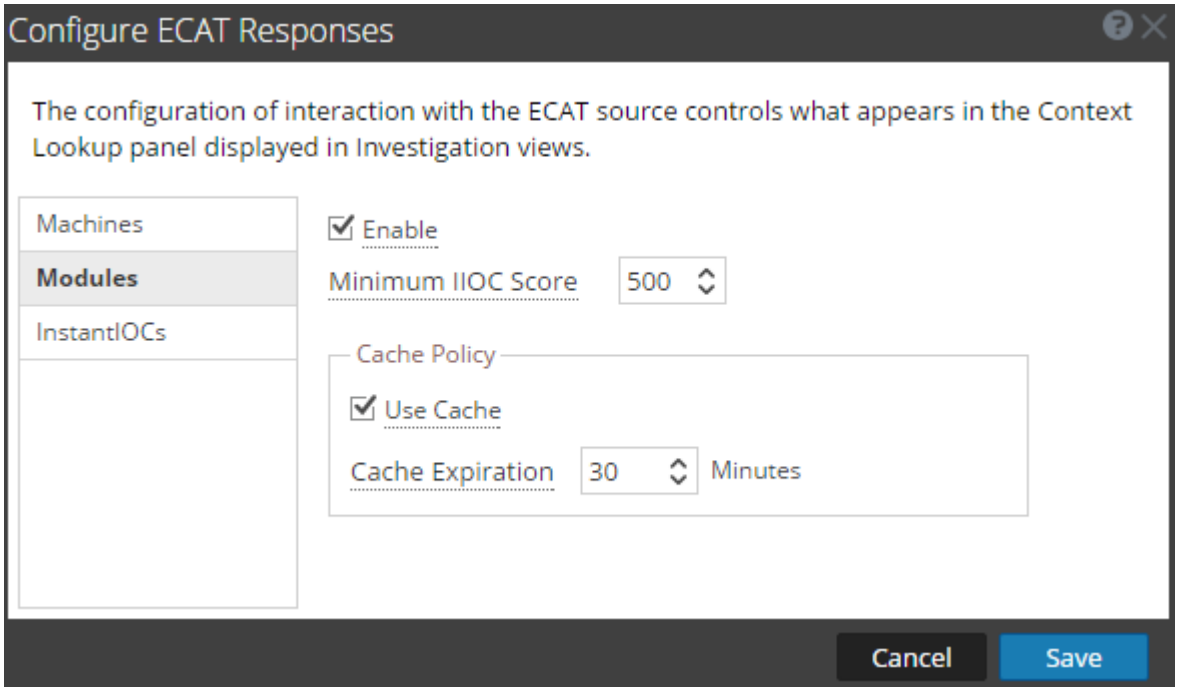
Après avoir défini le mot de passe, redémarrez le serveur.

Pour plus d'informations sur le serveur RSA ECAT REST API, reportez-vous aux documents ECAT documents disponibles à l'adresse https://knowledge.rsasecurity.com.

Configurer les réponses pour la source de données ECAT

Pour afficher/modifier les réponses pour la source de données ECAT :

1. Dans l'onglet **Sources de données**, sélectionnez la source ECAT et cliquez sur .
   La boîte de dialogue **Configurer les réponses ECAT** s'affiche.



2. Dans le panneau de gauche, sélectionnez chaque réponse (machines, modules et indicateurs de compromission instantanés) pour afficher et modifier les paramètres.
3. Configurez les champs suivants :

Champ	Description
Activer	Cette option est désactivée par défaut (cochée) et peut être utilisée pour activer ou désactiver la réponse sélectionnée.
Utiliser le cache	Cochez la case pour activer le cache de réponse. Lorsque cette option est activée, Context Hub stocke les résultats de la recherche dans le cache. Les requêtes suivantes pour la même valeur méta sont gérées à partir du cache pour la durée configurée (Expiration du cache).
Expiration du cache	Période (en minutes) pendant laquelle les résultats de la recherche sont stockés dans le cache lorsque la recherche contextuelle est réalisée. La valeur par défaut est **30 minutes**.
Valeur IIOC minimale (pour les modules uniquement)	Score minimum de l'indicateur de compromission instantané (IIOC) permettant d'extraire les informations contextuelles des modules ECAT Les informations contextuelles des modules ECAT présentant un score IIOC supérieur ou égal au score minimum configuré sont extraites. Le score IIOC pour les modules ECAT est compris entre 0 et 1024, où 1024 est considéré comme critique.

	Par défaut, le score IIOC minimum est défini sur **500**.

4. Cliquez sur **Enregistrer** pour enregistrer vos modifications.

Étapes suivantes

Après avoir terminé la configuration, vous pouvez utiliser l'option Recherche contextuelle dans la vue Examiner > Naviguer ou la vue Investigation > Événements pour récupérer des informations contextuelles. Pour obtenir des instructions, consultez la rubrique Afficher du contexte supplémentaire pour un point de données.

Last Modified: August 10 2016, 9:33AM

Configurer des listes en tant que sources de données pour Context Hub

Cette rubrique décrit la procédure permettant de créer et configurer des listes personnalisées pour Context Hub. Ces listes sont automatiquement considérées comme des sources de données pour Context Hub.

Pour utiliser le service Context Hub afin d'extraire des informations contextuelles des types de métadonnées prenant en charge la recherche contextuelle, vous pouvez créer une ou plusieurs listes, et y ajouter les valeurs de liste appropriées. Veillez à créer une liste significative, par exemple les adresses IP sur liste noire, les adresses IP sur liste blanche, etc. Vous pouvez remplir ces listes personnalisées à l'aide d'éléments, soit par importation de fichiers CSV, soit par ajout de métavaleurs via l'option **Ajouter à la liste/Supprimer de la liste** des vues Investigation.

Vous pouvez également importer et exporter une liste. Pour plus d'informations, reportezvous à Importer ou exporter des listes pour Context Hub.

Vous pouvez également créer des listes et ajouter des valeurs de liste à partir des vues Investigation. Pour plus d'informations, reportezvous à Gérer les listes et les valeurs de liste dans Investigation.

Conditions préalables

Assurezvous que le service Context Hub est activé et qu'il est ajouté dans Administration > vue Services de Security Analytics.

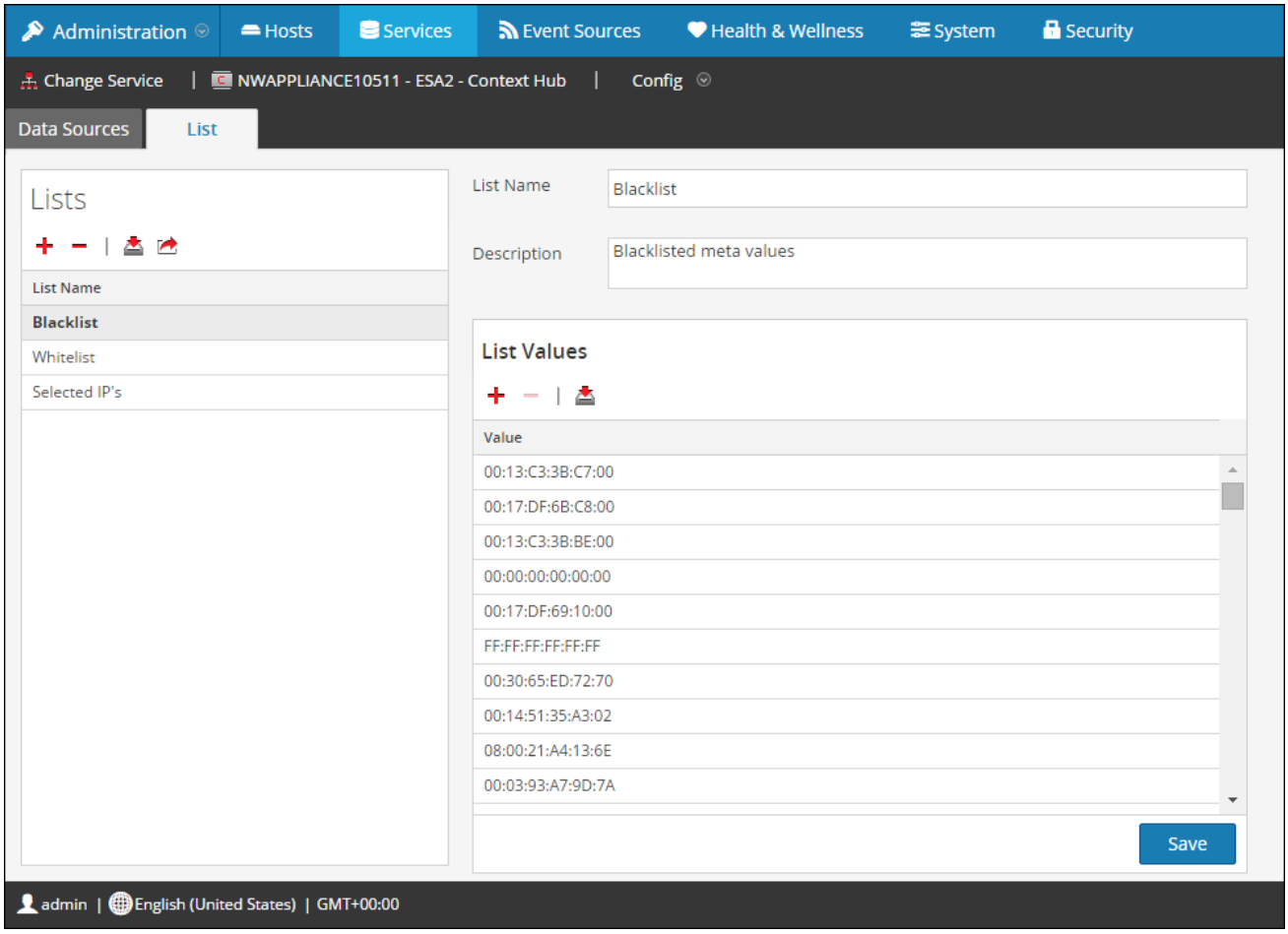
Procédure

Pour ajouter une nouvelle liste pour Context Hub :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
2. Dans la grille **Services**, sélectionnez le service Context Hub, puis  **> Vue > Config**.
   La vue Configuration des services du service Context Hub sélectionné s'affiche.

Last Modified: August 10 2016, 9:33AM

3. Cliquez sur l'onglet **Liste**.
   L'onglet **Liste** comprend le panneau **Listes** et le panneau **Valeurs de la liste**.



4. Cliquez sur + dans le panneau **Listes** pour ajouter une nouvelle liste, puis effectuez les étapes suivantes :
   a. Dans le champ **Nom de la liste**, entrez un nom unique pour la liste.
   b. Dans le champ **Description**, entrez la description de la liste.
   c. Dans le panneau **Valeurs de la liste**, cliquez sur + pour ajouter des valeurs de liste uniques.
   d. Pour importer une liste, cliquez sur dans le panneau **Listes**.
   e. Pour importer les valeurs de liste spécifiques d'une liste, cliquez sur dans le panneau **Valeurs de la liste**.
      Pour plus d'informations sur l'importation de listes et de valeurs de liste, reportez-vous à Importer ou exporter des listes pour Context Hub.
5. Cliquez sur **Enregistrer**.
   La liste est enregistrée avec les valeurs. Ces listes sont considérées comme des sources de données permettant de récupérer des informations contextuelles.

Étapes suivantes

Après avoir terminé la configuration, vous pouvez utiliser l'option Recherche contextuelle dans Investigation > vue Naviguer ou Investigation > vue Événements pour interroger et afficher les informations contextuelles. Pour obtenir des instructions, reportezvous à Visualiser le contexte supplémentaire d'un point de données.

Last Modified: August 10 2016, 9:33AM

Procédures supplémentaires

Utilisez cette section si vous recherchez des instructions pour effectuer une tâche spécifique après la configuration initiale du service Context Hub.

Last Modified: August 10 2016, 9:33AM

Modifier le mot de passe de stockage du service Context Hub

Dans Security Analytics, cette procédure est facultative. Cependant, c'est une bonne pratique de sécurité pour les administrateurs que de modifier les mots de passe par défaut. Certaines organisations n'autorisent pas de mots de passe par défaut et rendent cette procédure obligatoire.

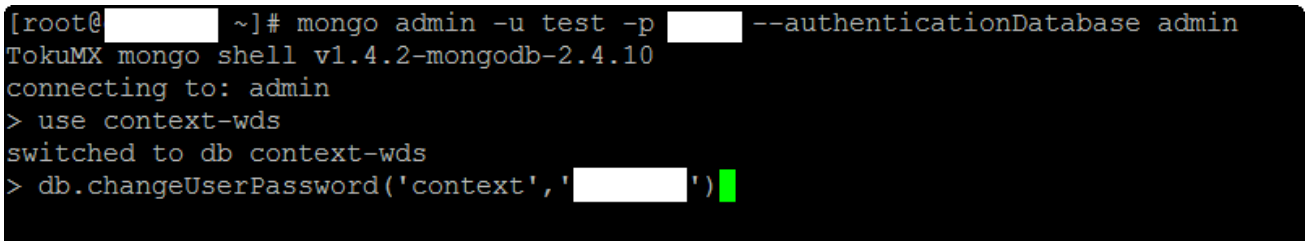
Conditions préalables

Vous devez disposer des privilèges du rôle administrateur.

Procédures

Modifier le mot de passe de la base de données Context Hub

1. Connectez-vous à l'hôte ESA qui exécute le service Context Hub :
   a. SSH sur l'hôte ESA.
   b. Connectez-vous en tant qu'utilisateur **root** (racine).
2. Connectez-vous à MongoDB en tant qu'utilisateur administrateur.
   mongo admin -u admin -p <mot de passe_admin_actuel> --authenticationDatabase admin
3. Basculez vers la base de données Context Hub.
   use context-wds

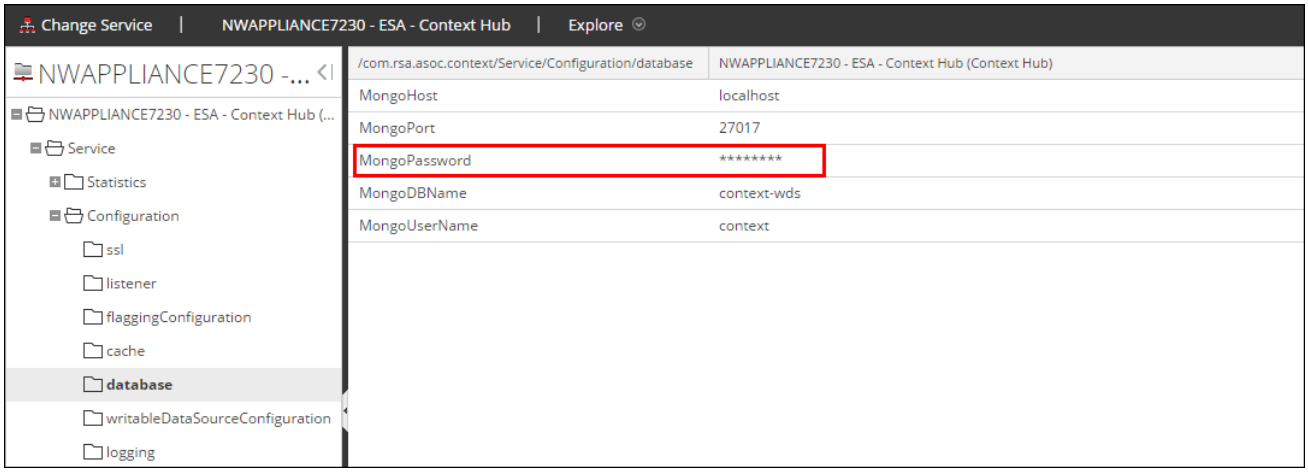


4. Saisissez la commande suivante pour changer le mot de passe du compte Context Hub. Le mot de passe par défaut est `context`.
   db.changeUserPassword('context','<nouveau_mot de passe>')

Last Modified: August 10 2016, 9:33AM

Mettre à jour la base de données Context Hub avec le nouveau mot de passe

1. Connectez-vous à Security Analytics en tant qu'administrateur.
2. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
3. Sélectionnez le service Context Hub, puis **> Vue > Explorer**.
4. Dans la vue Explorer située à gauche, sélectionnez **Configuration > base de données**.



5. Dans le panneau de droite, saisissez le mot de passe mis à jour de la base de données dans le champ **MongoPassword**.
6. Redémarrez le service Context Hub pour accepter le changement de mot de passe et forcez la session à démarrer en utilisant le nouveau mot de passe.
   a. Sélectionnez **Administration > Services**.
   b. Sélectionnez le service Context Hub, puis cliquez sur **> Redémarrer**.
7. Pour valider le changement de mot de passe, accédez à la vue Config du service Context Hub, puis vérifiez les sources de données et les listes configurées. Si le contenu apparaît sous l'onglet Sources de données et listes, les mots de passe correspondent et ont été modifiés avec succès.
   Si vous ne voyez pas le contenu requis sous l'onglet Sources de données et listes, examinez le mot de passe du service pour qu'il corresponde au mot de passe MongoDB.

Last Modified: August 10 2016, 9:33AM

Importer ou exporter des listes pour Context Hub

Cette rubrique fournit des instructions aux administrateurs pour importer ou exporter une liste configurée dans le service Context Hub. Le fichier à importer ou exporter doit être un fichier CSV.

Les utilisateurs ayant un rôle d'administrateur peuvent importer ou exporter des listes utilisables par l'analyste.

Note: Le fichier CSV que vous importez sous forme de liste doit être un fichier comportant une seule colonne.

Conditions préalables

Assurezvous que le service Context Hub est activé et qu'il est disponible dans Administration > vue Services de Security Analytics.

Procédures

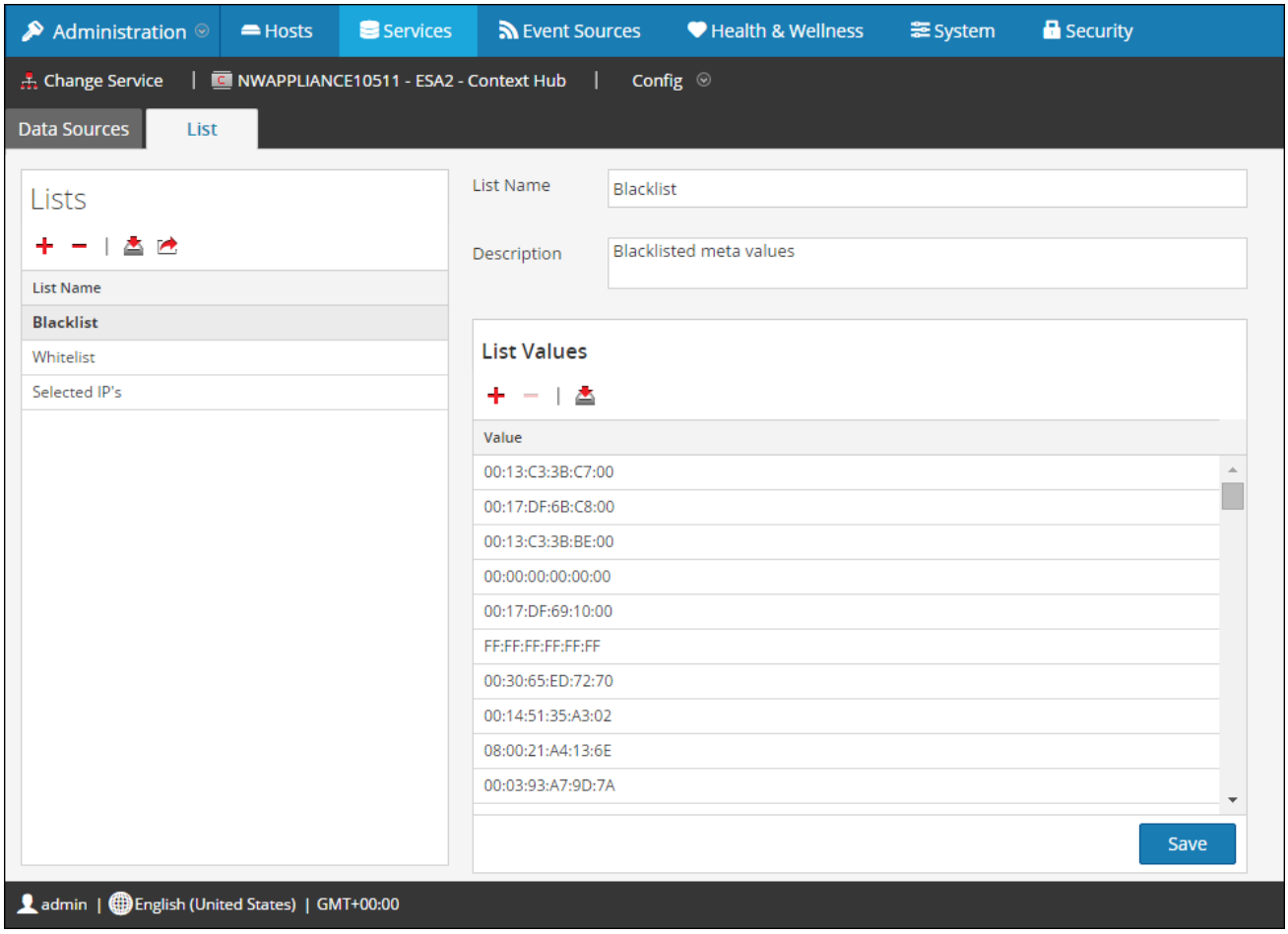
Importer une liste pour Context Hub

Pour importer une liste :

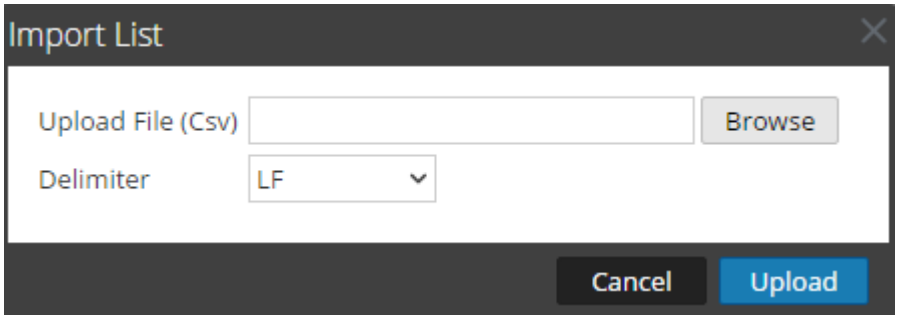
1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
   La vue Services s'affiche.
2. Dans le panneau **Services**, sélectionnez le service Context Hub, puis cliquez sur  **> Vue > Config**.
   La vue Configuration des services du service Context Hub s'affiche.

Last Modified: August 10 2016, 9:33AM

3. Cliquez sur l'onglet **Liste**.
   L'onglet Liste comprend le panneau **Listes** et le panneau **Valeurs de la liste**.



4. Cliquez sur dans le panneau **Listes**.
   La boîte de dialogue **Importer la liste** s'affiche.



5. Dans la boîte de dialogue **Importer la liste**, effectuez les étapes suivantes :
   a. Dans le champ **Télécharger le fichier (csv)**, recherchez et sélectionnez le fichier CSV.
   b. Dans le champ **Délimiteur**, sélectionnez le délimiteur des valeurs de liste parmi les options —**Virgule**, **CR** (Retour chariot) et **LF** (Saut de ligne).
6. Cliquez sur **Télécharger** pour télécharger le fichier CSV dans Security Analytics.

La liste est importé dans Security Analytics. Ces listes sont considérées comme des sources de données permettant de récupérer des informations contextuelles.

Importer les valeurs de liste d'une liste

Pour importer les valeurs de liste d'une liste :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Services**.
   La vue Services s'affiche.
2. Dans le panneau **Services**, sélectionnez le service Context Hub, puis cliquez sur  **> Vue > Config**.
   La vue Configuration des services du service Context Hub s'affiche.
3. Cliquez sur l'onglet **Liste**.
   L'onglet Liste comprend le panneau **Listes** et le panneau **Valeurs de la liste**.
4. Dans le panneau Listes, sélectionnez la liste dont vous souhaitez importer les valeurs.
5. Cliquez sur  dans le panneau **Valeurs de la liste**.
   La boîte de dialogue **Importer la liste** s'affiche.
6. Dans la boîte de dialogue **Importer la liste**, effectuez les étapes suivantes :
   a. Dans le champ **Télécharger le fichier (csv)**, recherchez et sélectionnez le fichier `CSV`.
   b. Dans le champ **Délimiteur**, sélectionnez le délimiteur des valeurs de liste parmi les options —**Virgule**, **CR** (Retour chariot) et **LF** (Saut de ligne).

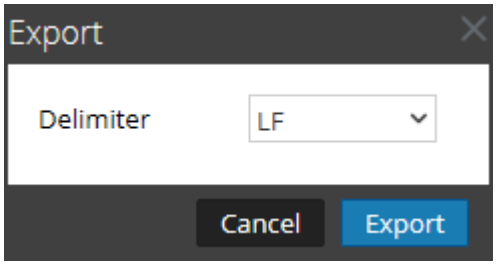
   Note: Vous pouvez importer des valeurs de liste dans une liste uniquement après avoir enregistré la liste. Le bouton d'importation () dans le panneau **Valeurs de la liste** est désactivé si la liste n'est pas enregistrée.
7. Cliquez sur **Télécharger** pour télécharger le fichier CSV dans Security Analytics.

Les valeurs de liste sont importées dans la liste sélectionnée. Ces listes sont considérées comme des sources de données permettant de récupérer des informations contextuelles.

Exporter une liste pour Context Hub

Pour exporter une liste :

1. Sous l'onglet Liste de la vue Configuration des services du service Context Hub, cliquez sur  .
   La boîte de dialogue Exporter s'affiche.



Last Modified: August 10 2016, 9:33AM

2. Dans le champ Délimiteur, sélectionnez le délimiteur des valeurs d'une liste exportée parmi les options —**Virgule**, **CR** (Retour chariot) et **LF** (Saut de ligne).
3. Cliquez sur **Exporter**.

La liste est exportée sous forme de fichier CSV sur la machine locale.

Gérer le mappage du type de méta et de la clé méta

Cette rubrique fournit des instructions aux administrateurs pour gérer le mappage des types de métadonnées Context Hub aux clés méta Investigation.

Le service Context Hub fournit une recherche contextuelle des métavaleurs dans les vues Investigation. Ces métavaleurs sont regroupées en types de métadonnées selon la catégorie à laquelle ils appartiennent. Les clés méta de Security Analytics Investigation, par exemple `ip.src` et `ip.dst`, sont regroupées dans le type de métadonnées `IP` au sein de Context Hub. Le type de métadonnées `IP` est à son tour mappé à des métavaleurs comme `alert.events.source.device.ip_address` et `alert.events.destination.device.ip_address` dans la base de données Incident Management.

Dans Administration > Système > vue Investigation, l'onglet Recherche contextuelle permet à l'administrateur de configurer le mappage des clés méta aux types de métadonnées Investigation. L'administrateur peut ajouter ou supprimer des clés méta de procédure d'enquête à la liste des types de métadonnées pris en charge par Context Hub.

Le service Context Hub est préconfiguré avec un mappage par défaut des types de métadonnées aux clés méta. Il est censé fonctionner pour la plupart des déploiements, sauf si des mappages personnalisés sont créés pour votre déploiement spécifique.

Note: Vous ne pouvez pas ajouter un nouveau type de métadonnées.

Le mappage par défaut est indiqué cidessous :

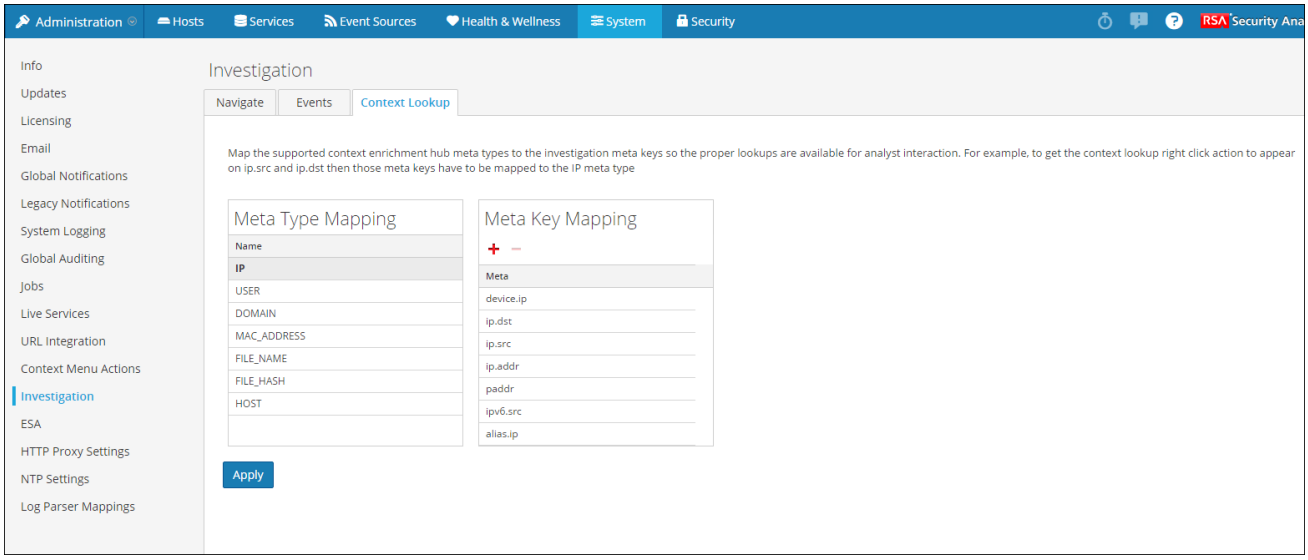
Nom de type de métadonnées	Clés méta
IP	device.ip, ip.src, ip.dst, paddr, ip.addr, alias.ip
USER	user.src, user.dst, username
DOMAIN	domain.src, domain.dst
MAC_ADDRESS	eth.dst, eth.src, alias.mac
FILE_NAME	filename, sourcefile
FILE_HASH	checksum
HÔTE	device.host, alias.host

Last Modified: August 10 2016, 9:33AM

Procédure

Pour gérer le mappage des clés méta Investigation :

1. Dans le menu **Security Analytics**, sélectionnez **Administration > Système**.
2. Dans le panneau des options, sélectionnez **Investigation**.
   Le panneau Configuration des procédures d'enquête s'affiche.
3. Sélectionnez l'onglet **Recherche contextuelle**.



4. Sélectionnez un type de métadonnées pour visualiser les clés méta par défaut mappées à ce type de métadonnées.
5. Pour ajouter une clé méta, cliquez sur +, puis entrez la clé méta.
6. Pour supprimer une clé méta, sélectionnezla, puis cliquez sur −.
7. Pour enregistrer les modifications, cliquez sur **Appliquer**.

Si une nouvelle clé méta est ajoutée, l'option de menu Recherche contextuelle est activée pour les métavaleurs situées sous la clé méta en question dans les vues Investigation.

Pour plus d'informations sur le Panneau Configuration des procédures d'enquête, reportezvous à Panneau Configuration des procédures d'enquête.

Last Modified: August 10 2016, 9:33AM

Références du service Context Hub

Les rubriques de référence contenues dans cette section sont classées dans l'ordre alphabétique.

Last Modified: August 10 2016, 9:33AM

Boîte de dialogue Configurer les réponses

Cette rubrique décrit les fonctions et les caractéristiques de la boîte de dialogue Configurer les réponses pour les sources de données Incident Management et ECAT.

Sous la vue Configuration des services > onglet Sources de données dans Context Hub, vous pouvez configurer les réponses pour les sources de données Incident Management et ECAT.

Les procédures associées sont disponibles dans les rubriques suivantes :

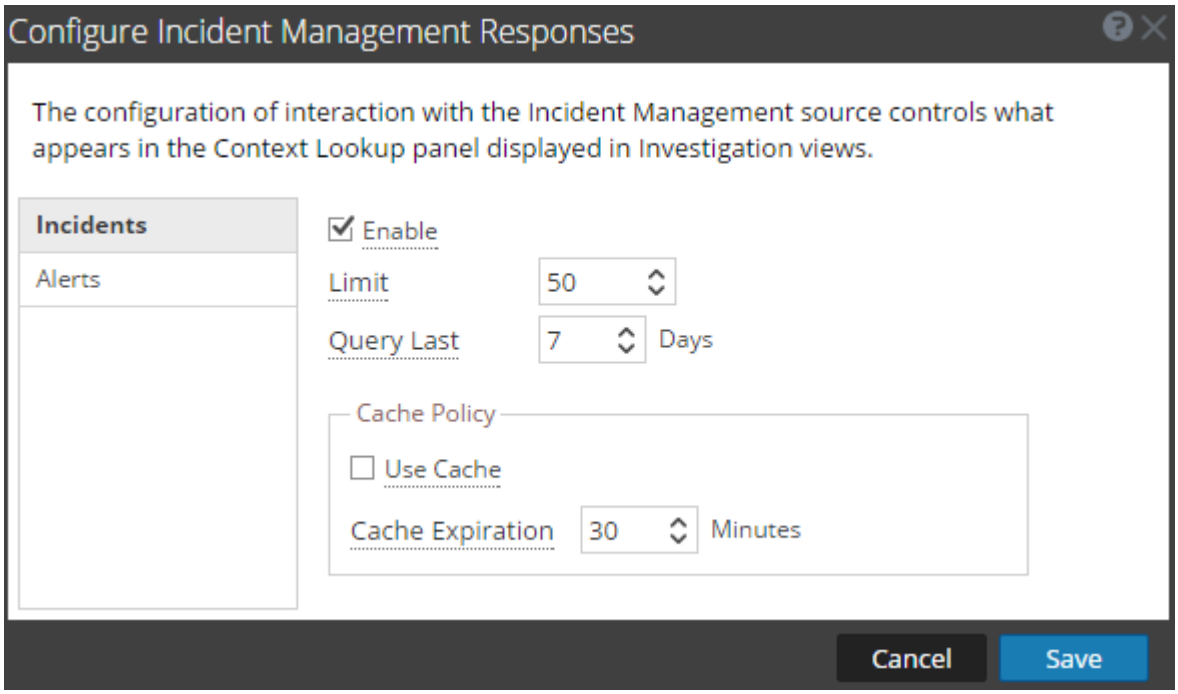
- Configurer les réponses pour une source Incident Management. Voir la rubrique Configurer Incident Management en tant que source de données pour Context Hub.
- Configurer les réponses pour la source de données ECAT. Voir la rubrique Configurer ECAT en tant que source de données pour Context Hub.

Pour accéder à cette boîte de dialogue :

1. Dans le menu Security Analytics, sélectionnez **Administration > Services**.
   La vue Services s'affiche.
2. Dans le panneau Services, sélectionnez le service Context Hub, puis cliquezsur  **> Vue > Config**.
   La vue Configuration des services de Context Hub s'affiche.
3. Sélectionnez la source de données (Incident Management ou ECAT) pour laquelle vous souhaitez configurer les réponses, puis cliquez sur  dans la colonne **Actions**.

Boîte de dialogue Configurer les réponses pour Incident Management

Les types de réponses pour une source de données Incident Management sont **Incidents** et **Alertes**. La figure suivante montre la boîte de dialogue Configurer les réponses pour Incident Management.



Caractéristiques

Le tableau suivant décrit les fonctions de la boîte de dialogue Configurer les réponses pour Incident Management.

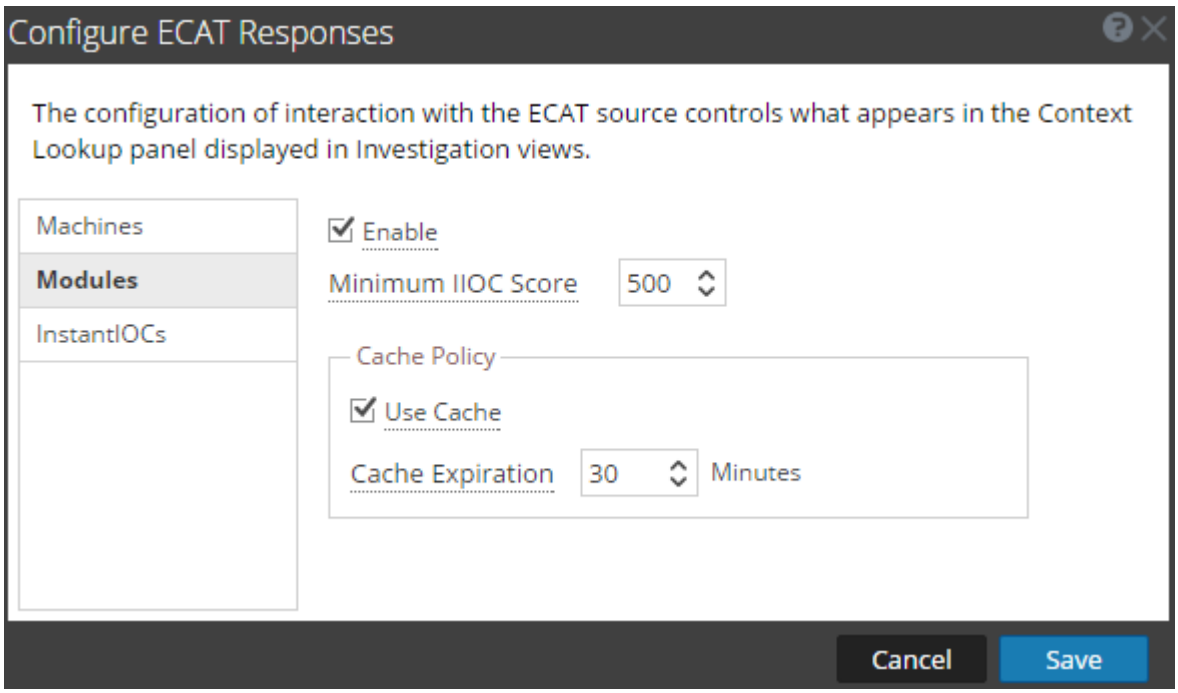
Fonction	Description
Activer	Cette option détermine si le type de réponse sélectionné doit être activé pour la source de données, et si les résultats de la recherche doivent apparaître dans le panneau Recherche contextuelle figurant dans les vues Investigation. Le paramètre par défaut est activé.
Limite	Nombre maximal d'enregistrements (incidents ou alertes) à afficher dans le panneau Recherche contextuelle des vues Investigation lorsque la recherche contextuelle est exécutée. La valeur par défaut est **50**.
Requête dans les derniers	Durée (en jours) pendant laquelle les informations contextuelles du type de réponse sélectionné doivent être récupérées. La valeur par défaut est **7 derniers jours**.
Utiliser le cache	Cette option détermine si la réponse mise en cache est activée. Lorsqu'elle est activée, Context Hub stocke les résultats de recherche dans le

Last Modified: August 10 2016, 9:33AM

	cache. Les requêtes suivantes pour la même valeur méta sont gérées à partir du cache pour la durée configurée (Expiration du cache).
Expiration du cache	Période (en minutes) pendant laquelle les résultats de la recherche sont stockés dans le cache après l'exécution de la recherche contextuelle. La valeur par défaut est **30 minutes**.

Boîte de dialogue Configurer les réponses ECAT

Les types de réponses pour la source de données ECAT sont Modules, Machines et InstantIOCs. La figure suivante présente la boîte de dialogue Configurer les réponses ECAT.



Le tableau suivant décrit les fonctions de la boîte de dialogue Configurer les réponses ECAT.

Fonction	Description
Activer	Cette option détermine si le type de réponse sélectionné doit être activé pour la source de données, et si les résultats de la recherche doivent apparaître dans le panneau Recherche contextuelle figurant dans les vues Investigation. Le paramètre par défaut est activé.
Valeur IIOC minimale [Pour les modules uniquement]	Score minimum de l'indicateur de compromission instantané (IIOC) pour extraire les informations contextuelles des modules ECAT Les informations contextuelles des modules ECAT ayant une valeur IIOC supérieure ou égale à la valeur minimale configurée sont extraites.

Last Modified: August 10 2016, 9:33AM

	La valeur IIOC des modules ECAT est comprise entre 0 et 1024, 1024 étant considéré comme un seuil critique. Par défaut, la valeur IIOC minimale est définie sur **500**.
Utiliser le cache	Cette option détermine si la réponse mise en cache est activée. Lorsqu'elle est activée, Context Hub stocke les résultats de recherche dans le cache. Les demandes suivantes pour la même valeur méta sont gérées à partir du cache pour la durée configurée (Expiration du cache).
Expiration du cache	Période (en minutes) pendant laquelle les résultats de la recherche sont stockés dans le cache après l'exécution de la recherche contextuelle. La valeur par défaut est **30 minutes**.

Onglet Sources de données de Context Hub

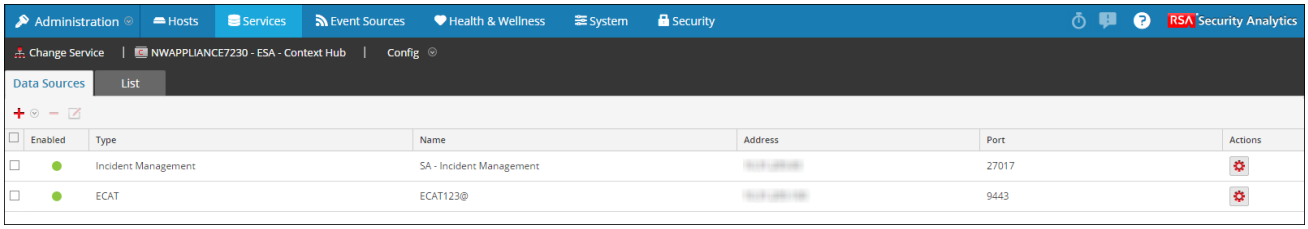
Cette rubrique décrit les fonctions de l'onglet Sources de données de la vue Configuration des services du service Context Hub.

La vue Configuration des services > onglet Sources de données pour Context Hub sert à configurer les sources de données du service Context Hub.

Pour accéder à cet onglet :

1. Dans le menu Security Analytics, sélectionnez **Administration > Services**.
   La vue Services s'affiche.

2. Dans le panneau Services, sélectionnez le service Context Hub, puis cliquez sur  **> Vue > Config**.
   La vue Configuration des services de Context Hub s'affiche avec l'onglet Sources de données sélectionné.



Caractéristiques

Le tableau suivant décrit les fonctions de l'onglet Sources de données.

Fonction	Description
+	Ouvre la boîte de dialogue Ajouter une source de données pour vous permettre d'ajouter une source de données. Vous ne pouvez ajouter qu'une seule source de données de chaque type. Pour obtenir des instructions détaillées sur l'ajout d'une source de données, reportezvous à l'Étape 2 : Configurer des sources de données pour Context Hub.
−	Supprime une source de données. Si vous supprimez une source de données, Context Hub ne considère pas le service supprimé comme une source de données. Toutes les informations contextuelles extraites précédemment cessent d'être disponibles.
	Ouvre la boîte de dialogue Modifier une source de données. Pour obtenir une description de chaque champ du panneau Modifier une source de données, reportezvous à l'Étape 2 : Configurer des sources de données pour Context Hub.

Last Modified: August 10 2016, 9:33AM

Fonction	Description
	Ouvre la boîte de dialogue Configurer les réponses. Vous pouvez afficher et modifier les réponses des sources de données. Par exemple, les alertes et les incidents sont des réponses qui peuvent être récupérées lorsque des informations contextuelles sont extraites de la source de données Incident Management. Pour obtenir une description de chaque champ de la boîte de dialogue Configurer les réponses, reportezvous à l'Étape 2 : Configurer des sources de données pour Context Hub.
Enabled	Indique si la source de données est activée ou désactivée. Un cercle vert plein indique que la source de données est activée ( ). Un cercle blanc vide indique que la source de données est désactivée.
Type	Type de sources de données. Par exemple, Incident Management ou ECAT.
Nom	Nom unique qui identifie la source de données. Par exemple, Incident Management.
Adresse	Adresse IP ou nom d'hôte de la source de données.
Port	Port de connexion de la source de données.

Last Modified: August 10 2016, 9:33AM

Onglet Liste de Context Hub

Cette rubrique décrit les fonctions de la vue Configuration des services > onglet Listes pour Context Hub.

À l'aide de l'onglet **Liste** du service Context Hub, vous pouvez créer une ou plusieurs listes, et y ajouter les valeurs de liste appropriées. Ces listes sont automatiquement considérées comme des sources de données pour le service Context Hub.

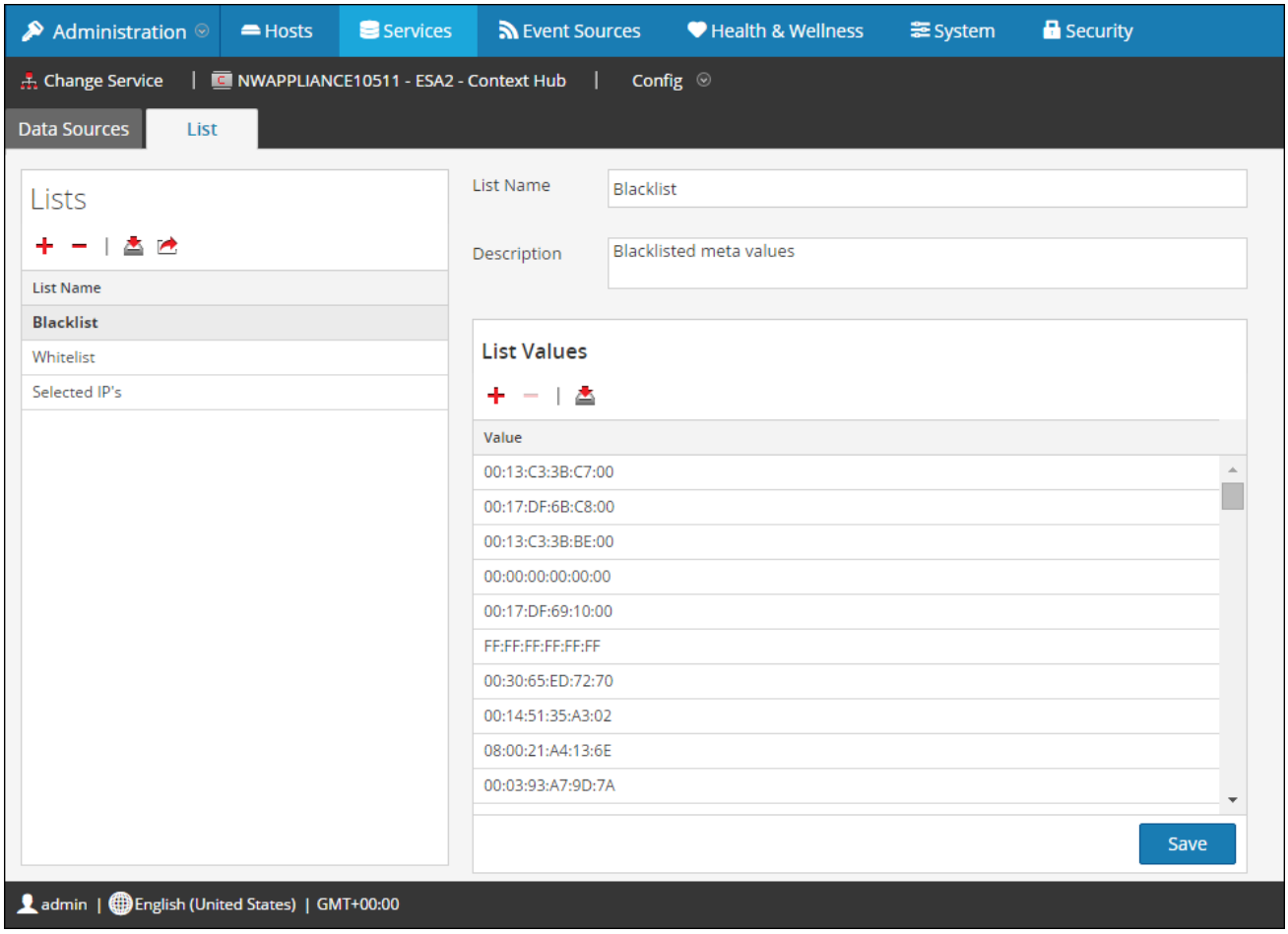
Note: Vous pouvez également créer des listes et ajouter des valeurs de liste à partir des vues Investigation. Pour plus d'informations, reportezvous à Gérer les listes et les valeurs de liste dans Investigation.

Pour accéder à cet onglet :

1. Dans le menu Security Analytics, sélectionnez **Administration > Services**.
   La vue Services s'affiche.
2. Dans le panneau Services, sélectionnez le service Context Hub, puis cliquez sur  **> Vue > Config**.
   La vue Configuration des services de Context Hub s'affiche.

Last Modified: August 10 2016, 9:33AM

3. Cliquez sur l'onglet **Liste**.
   Le panneau Liste s'affiche.



Caractéristiques

L'onglet Liste comprend le panneau **Listes** et le panneau **Valeurs de la liste**. Le panneau **Listes** comporte une barre d'outils avec des options permettant d'ajouter, de supprimer, d'importer et d'exporter des listes. Les entrées situées sous **Nom de la liste** sont des listes ajoutées ou importées pour le service Context Hub.
Le panneau **Valeurs de la liste** comporte une barre d'outils avec des options permettant d'ajouter, de supprimer et d'importer des valeurs de liste dans la liste sélectionnée. Les entrées situées sous **Valeur** identifient chaque entrée de la liste.

Le tableau suivant décrit les fonctions de l'onglet **Liste** dans la vue Configuration des services pour le service Context Hub.

Fonction	Description
+	Ajoutez une nouvelle liste. Pour plus d'informations, reportezvous à Configurer des listes en tant que sources de données pour Context Hub.

Last Modified: August 10 2016, 9:33AM

Fonction	Description
	Supprimez une liste. Si vous supprimez une liste de Context Hub, elle n'est plus considérée comme une source de données permettant de récupérer des informations contextuelles.
	Importez des listes dans Context Hub. Pour plus d'informations, reportezvous à Importer ou exporter des listes pour Context Hub.
	Exportez une liste vers la machine locale. Pour plus d'informations, reportezvous à Importer ou exporter des listes pour Context Hub.
Nom de la liste	Nom unique permettant d'identifier la liste.
Description	Description de la liste.
Enregistrer	Enregistre et ferme la boîte de dialogue.

Le tableau suivant décrit les fonctions de la section **Valeurs de la liste** sous l'onglet **Liste**.

Paramètre	Description
	Ajoutez une nouvelle valeur de liste à la liste sélectionnée.
	Supprimez une ou plusieurs valeurs de la liste.
	Importez des valeurs de liste dans la liste sélectionnée.
Enregistrer	Enregistre et ferme la boîte de dialogue.

Panneau de recherche contextuelle

Après avoir configuré le service Context Hub, vous pouvez afficher le panneau Recherche contextuelle dans la vue Naviguer et Événements du module Investigation. Lorsque vous affichez ce panneau pour la première fois, il propose des instructions pour réaliser une recherche contextuelle. Ce panneau est ensuite réduit et peut être développé si nécessaire.

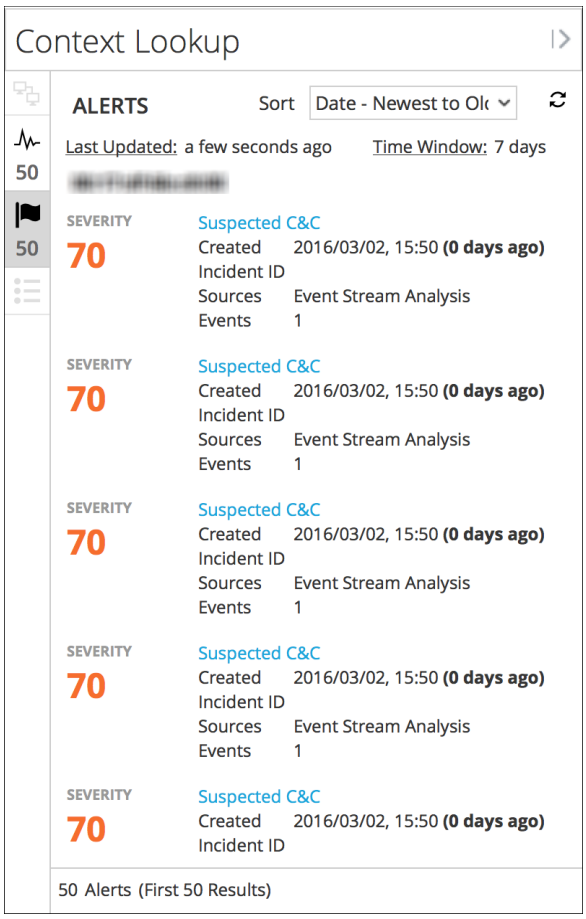
Le panneau Recherche contextuelle n'affiche aucune donnée jusqu'à ce que vous réalisiez une Recherche contextuelle sur une valeur méta. Les valeurs méta disposant d'informations de contexte associées sont surlignées à l'aide d'un arrière-plan gris. Les résultats de la recherche s'affichent dans le panneau Recherche contextuelle des différentes sources configurées pour la valeur méta sélectionnée. Les procédures liées à ce panneau sont décrites dans la rubrique Afficher du contexte supplémentaire pour un point de données.

Pour accéder à ce panneau :

1. Dans le menu **Security Analytics**, sélectionnez **Investigation > Naviguer** ou **Événements**.
2. Cliquez avec le bouton droit sur une valeur méta et sélectionnez **Recherche contextuelle** dans le menu contextuel.
   Le panneau Recherche contextuelle affiche les informations contextuelles.
3. Dans la barre d'icônes, sélectionnez la source pour laquelle vous souhaitez afficher les informations contextuelles en cliquant sur l'icône correspondante.

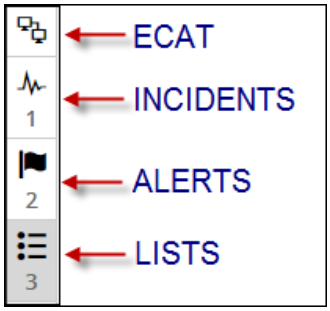
La figure suivante donne un exemple du panneau de Recherche.

Last Modified: August 10 2016, 9:33AM



Caractéristiques

Le panneau Recherche contextuelle propose les contrôles et fonctions suivantes :

Fonction	Description
Barre Options de la source 	Affiche les icônes des sources disponibles : ECAT, Incidents, Alertes et Listes.

Last Modified: August 10 2016, 9:33AM

Fonction	Description
Nom de la source	Affiche le nom de la source en fonction des icônes sélectionnées : • ECAT • INCIDENTS • ALERTES • LISTES
Trier	Propose une liste déroulante d'options pour trier les informations de contexte répertoriées. Les options de tri possibles sont Gravité - Élevée à faible, Gravité - Faible à élevée, Date - La plus ancienne à la plus récente, et Date - La plus récente à la plus ancienne. Les options de tri varient par type de source.
	Actualise les résultats de la recherche.
n éléments (n premiers résultats)	Le pied de page indique le nombre total de résultats et le nombre de résultats actuellement affichés. Par exemple, 50 alertes (50 premières alertes).

Résultats de la recherche

Le panneau Recherche contextuelle affiche les informations suivantes lors de la récupération des données contextuelles à partir des différentes sources configurées :

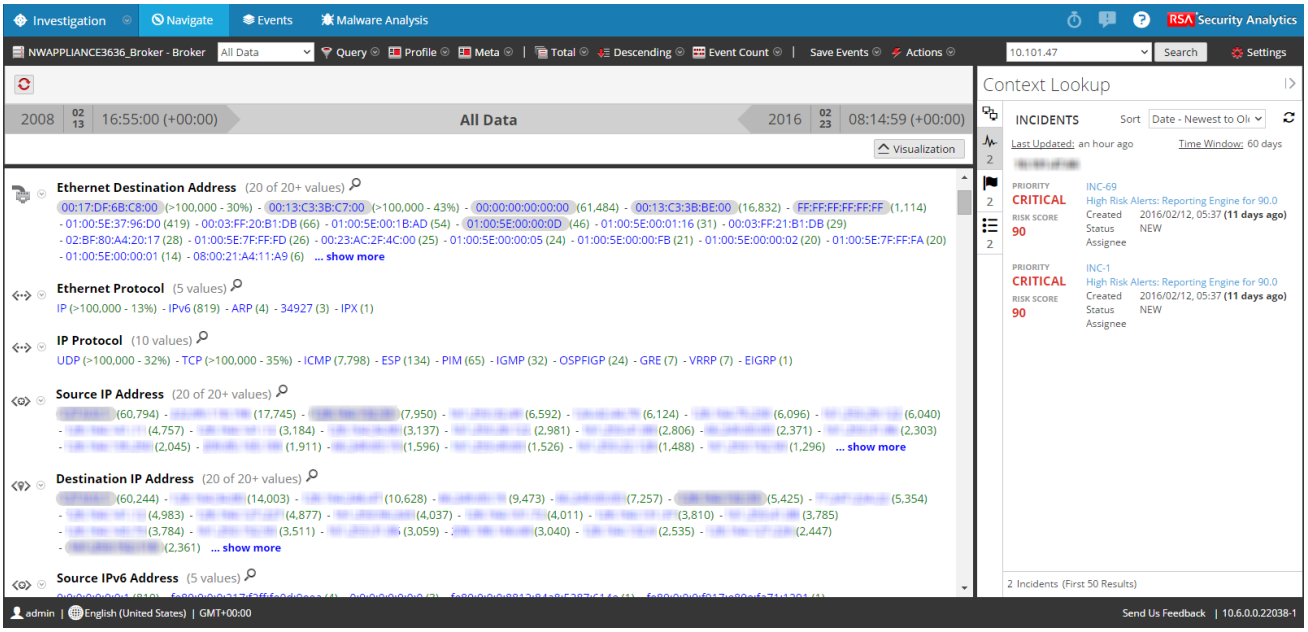
Incidents

Les incidents s'affichent d'abord selon un critère de temps (du plus récent au plus ancien), puis sur un critère de priorité. Les informations suivantes s’affichent pour les recherches d'incidents :

- Nom et ID de l'incident
- Priorité des incidents
- Score de risque des incidents
- Date de création de l'incident
- État de l'incident
- Personne affectée à l'incident
- Dernière mise à jour : indique lorsque les données contextuelles ont été extraites de la source de données pour la dernière fois et mises à jour dans le cache.
- Période : elle se base sur la valeur définie dans le champ « Requête dans les derniers » de la fenêtre Configurer les réponses Incident Management.
- Trier : Ce champ déroulant permet de modifier l'ordre de tri en fonction de la période et de la priorité.

Last Modified: August 10 2016, 9:33AM

La figure ci-après présente un exemple des résultats de recherche pour les incidents.

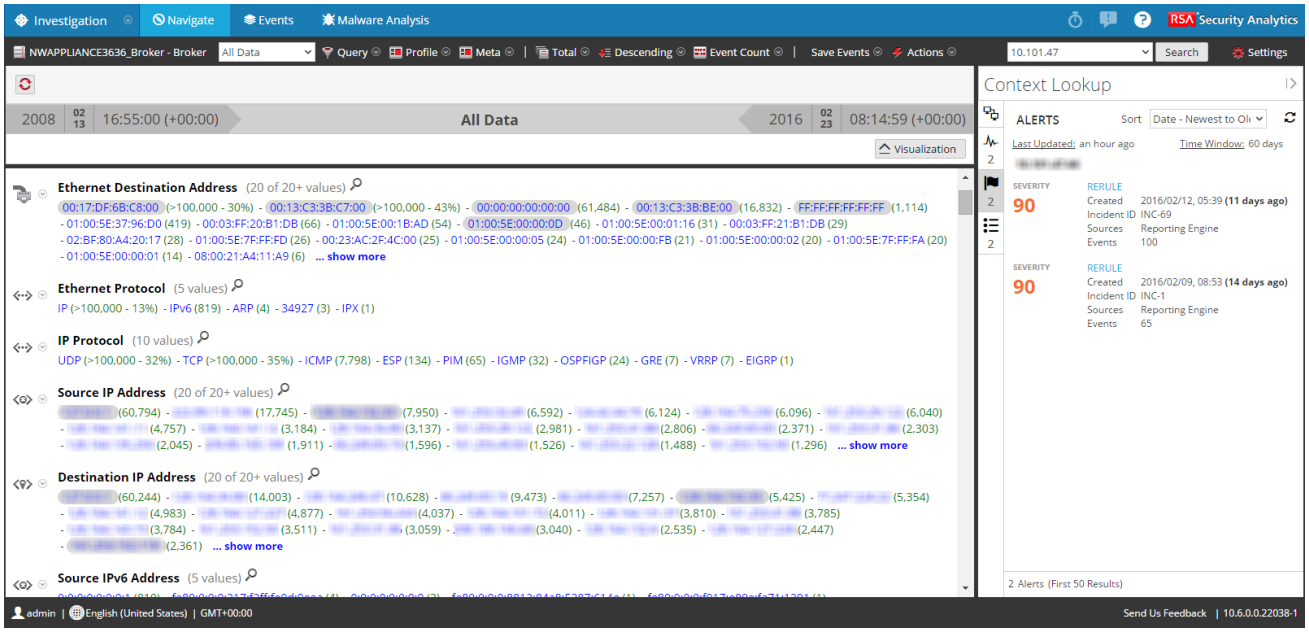


Alertes

Les alertes s'affichent en fonction de la Gravité. Les informations suivantes s'affichent pour les recherches d'alertes :

- Nom de l'alerte
- Gravité de l'alerte
- Date de création de l'alerte
- ID d'incident : ID de l'incident associé à alerte (le cas échéant).
- Sources : nom de la source d'événements.
- Nombre d'événements associés à l'alerte.
- Dernière mise à jour : indique lorsque les données contextuelles ont été extraites de la source de données pour la dernière fois et mises à jour dans le cache.
- Période : elle se base sur la valeur définie dans le champ « Requête dans les derniers » de la fenêtre Configurer les réponses Incident Management.
- Trier : Ce champ déroulant permet de modifier l'ordre de tri en fonction de la période et de la priorité.

La figure ci-après présente un exemple des résultats de recherche pour les alertes.

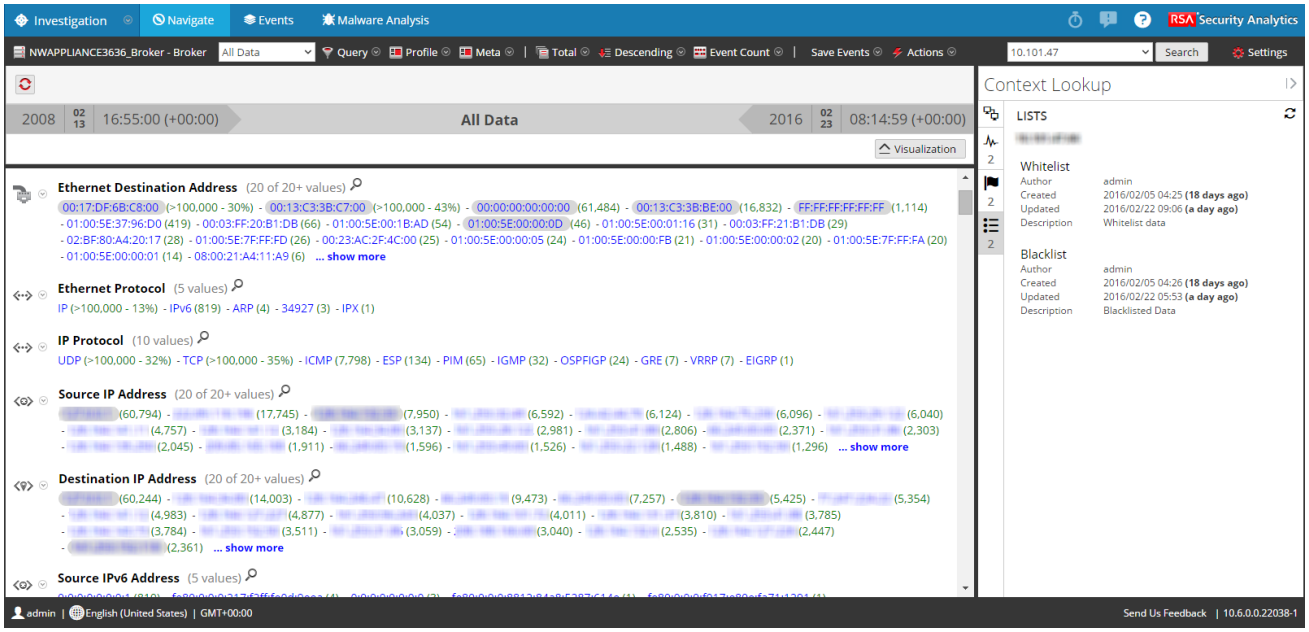


Listes

Les informations suivantes s'affichent pour les recherches de listes :

- Nom de la liste
- Propriétaire ayant créé la liste
- Date de création
- Date de dernière mise à jour
- Description de la liste

La figure ci-après présente un exemple des résultats de recherche pour la source de données Listes.

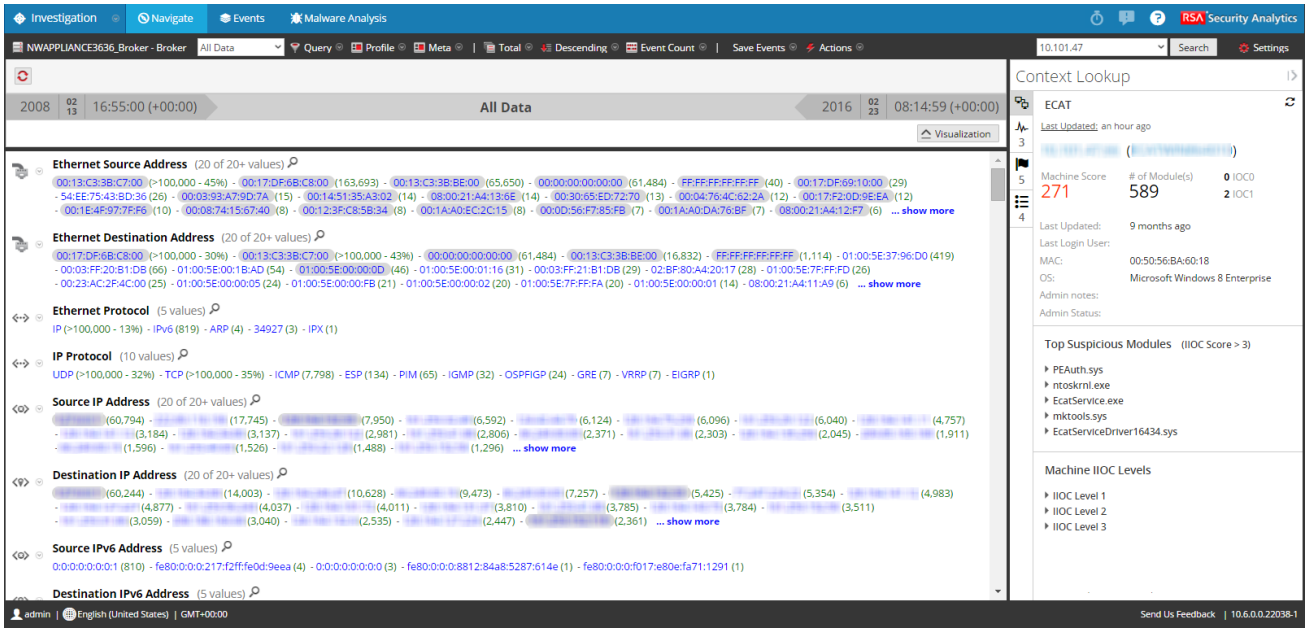


ECAT

Les informations suivantes s'affichent pour les recherches ECAT :

- Nom et adresse IP de la machine.
  En cliquant sur le nom ou l'adresse IP de la machine ECAT, vous serez dirigé vers l'UI ECAT pour approfondir la procédure d'enquête.
- Dernière mise à jour : indique lorsque les données contextuelles ont été extraites de la source de données pour la dernière fois et mises à jour dans le cache.
- Note de l'ordinateur : le score IIOC de la machine est agrégé en fonction des scores des modules.
- Nombre de modules : nombre de fichiers actifs pour la machine sélectionnée.
- Dernière mise à jour : indique lorsque les résultats de l'analyse ont été mis à jour pour la dernière fois dans la base de données ECAT.
- Dernière connexion utilisateur
- Adresse MAC de la machine
- Version du système d'exploitation
- Notes Admin (le cas échéant)
- État Admin (le cas échéant)
- Modules les plus suspects (modules dont le score IIOC est supérieur à 500). Cet élément se base sur la valeur définie dans le champ « Valeur IIOC minimale » de la fenêtre Configurer les réponses Incident Management. La valeur par défaut pour la « Valeur IIOC minimale » est de 500.
- Niveaux IIOC de la machine

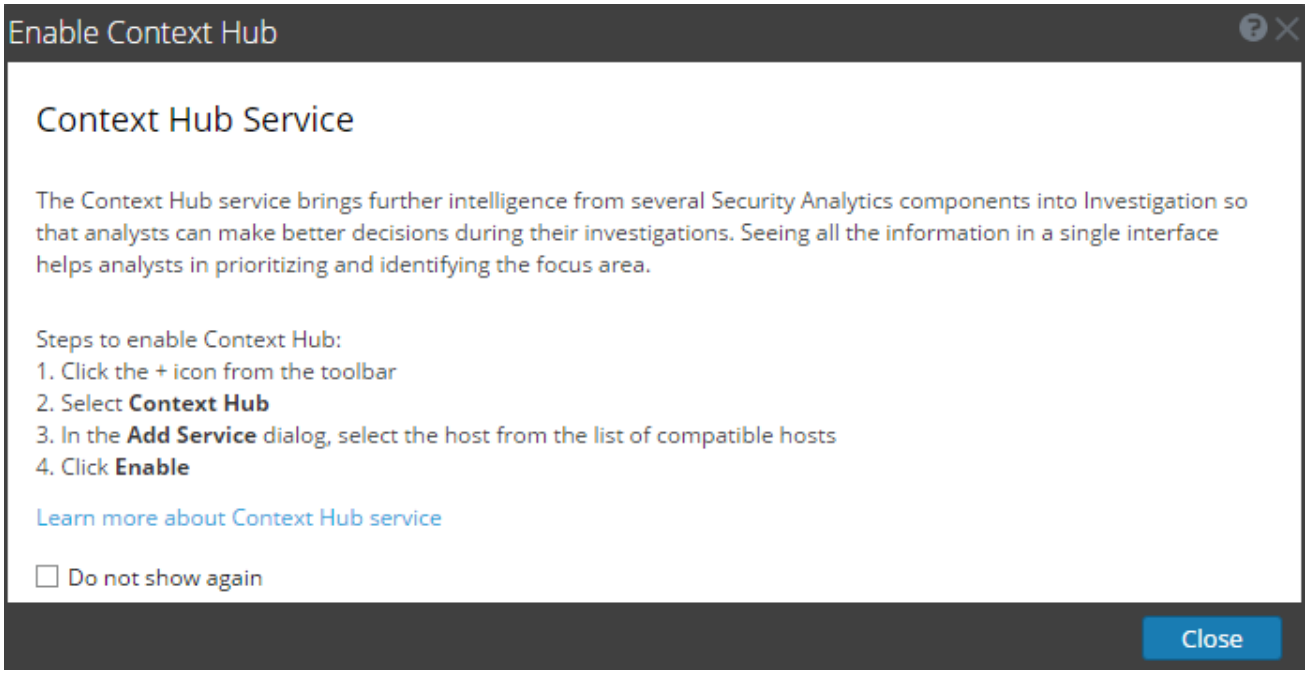
La figure ci-après présente un exemple des résultats de recherche pour la source de données ECAT.



Boîte de dialogue Activer Context Hub

Cette rubrique fournit des détails techniques sur la boîte de dialogue **Activer Context Hub**.

Lorsque vous accédez au panneau **Administration > Services**, si le service Context Hub n'est pas activé, la boîte de dialogue **Activer Context Hub** s'affiche.



Pour activer le service Context Hub, suivez les étapes fournies dans la boîte de dialogue **Activer Context Hub** ou consultez l'Étape 1. Ajoutez le service Context Hub.

Si vous ne souhaitez pas que cette boîte de dialogue s'affiche sans activer le service Context Hub, cliquez sur **Ne plus afficher**.

Last Modified: August 10 2016, 9:33AM

RSA

Dépannage

Cette rubrique fournit des informations sur les problèmes que les utilisateurs de Security Analytics peuvent rencontrer lors de la configuration du service Context Hub dans Security Analytics.

Problèmes possibles

Problème	Solutions
La création de la base de données a échoué durant l'installation ou la base de données est corrompue.	Exécutez manuellement le script `mongoDbConfig.sh` situé sous `/opt/rsa/context/bin`
Avec ECAT 4.1.1, le feed ECAT ne fonctionne pas pour Security Analytics.	Vous devez utiliser ECAT 4.1.1.1 pour que le feed puisse fonctionner.

Last Modified: August 10 2016, 9:33AM