



Guide de détection automatisée des menaces

pour la version 11.0



Informations de contact

RSA Link à l'adresse <https://community.rsa.com> contient une base de connaissances qui répond aux questions courantes et fournit des solutions aux problèmes connus, de la documentation produit, des discussions communautaires et la gestion de dossiers.

Marques commerciales

Pour obtenir la liste des marques commerciales de RSA, rendez-vous à l'adresse suivante : france.emc.com/legal/emc-corporation-trademarks.htm#rsa.

Contrat de licence

Ce logiciel et la documentation qui l'accompagne sont la propriété d'EMC et considérés comme confidentiels. Délivrés sous licence, ils ne peuvent être utilisés et copiés que conformément aux modalités de ladite licence et moyennant l'inclusion de la note de copyright ci-dessous. Ce logiciel et sa documentation, y compris toute copie éventuelle, ne peuvent pas être remis ou mis de quelque façon que ce soit à la disposition d'un tiers.

Aucun droit ou titre de propriété sur le logiciel ou sa documentation ni aucun droit de propriété intellectuelle ne vous est cédé par la présente. Toute utilisation ou reproduction non autorisée de ce logiciel et de sa documentation peut faire l'objet de poursuites civiles et/ou pénales.

Ce logiciel est modifiable sans préavis et ne doit nullement être interprété comme un engagement de la part d'EMC.

Licences tierces

Ce produit peut inclure des logiciels développés par d'autres entreprises que RSA. Le texte des contrats de licence applicables aux logiciels tiers présents dans ce produit peut être consulté sur la page de la documentation produit du site RSA Link. En faisant usage de ce produit, l'utilisateur convient qu'il est pleinement lié par les conditions des contrats de licence.

Remarque sur les technologies de chiffrement

Ce produit peut intégrer une technologie de chiffrement. Étant donné que de nombreux pays interdisent ou limitent l'utilisation, l'importation ou l'exportation des technologies de chiffrement, il convient de respecter les réglementations en vigueur lors de l'utilisation, de l'importation ou de l'exportation de ce produit.

Distribution

EMC estime que les informations figurant dans ce document sont exactes à la date de publication. Ces informations sont modifiables sans préavis.

février 2018

Sommaire

Détection automatisée des menaces avec NetWitness Suite	4
Détection automatique des menaces pour les domaines suspects	4
Workflow du module Domaines suspects	5
Détection automatisée des menaces de domaines suspects sur des paquets ou logs de proxy Web	7
Configurer la détection automatisée des menaces pour les domaines suspects	8
Conditions préalables	8
Configurer la fonction de détection automatisée des menaces pour les domaines suspects	9
Étape 1 : (Pour les logs uniquement) Configurer les paramètres de log	10
Pour obtenir le dernier fichier de configuration Envision, procédez comme suit :	12
Pour vérifier que le fichier de configuration Envision a été mis à jour correctement :	13
Pour vérifier que les index du fichier index-concentrator.xml ont été mis à jour :	13
Étape 2 : Créer une liste blanche Domaines (facultatif)	14
Étape 3 : Configurer le service de recherche Whois	17
Étape 4 : Mapper des sources de données à des modules ESA Analytics	17
Étape 5 : Vérifier que la règle Commande et contrôle suspect par domaine est activée et surveiller la règle	17
Étape 6 : Vérifier que l'incident est regroupé par C&C suspect	18
Étapes suivantes	18
Dépannage de la détection automatisée des menaces avec NetWitness Suite	19
Problèmes possibles	19

Détection automatisée des menaces avec NetWitness Suite

RSA NetWitness® Suite La détection automatisée des menaces utilise des modules ESA Analytics préconfigurés pour identifier des types de menaces spécifiques. Un module ESA Analytics est un pipeline composé d'objets d'activité qui enrichissent un événement avec des informations supplémentaires via des calculs mathématiques. Les modules ESA Analytics résident dans les services ESA Analytics. Les services ESA Analytics utilisent l'agrégation basée sur la requête (QBA) pour collecter des événements filtrés pour les modules à partir des Concentrators. Seules les données requises par un module sont transférées entre le service Concentrator et le système ESA Analytics.

Il existe deux services ESA pouvant s'exécuter sur un hôte ESA :

- Event Stream Analysis (règles de corrélation ESA)
- Event Stream Analytics Server (ESA Analytics)

Le premier service est le service Event Stream Analysis qui crée des alertes à partir de règles ESA, également appelé ESA Correlation Rules, que vous créez manuellement ou téléchargez à partir de Live. Le deuxième service est le service ESA Analytics, qui est utilisé pour la détection automatisée des menaces. Étant donné que le service ESA Analytics utilise des modules préconfigurés pour la détection automatisée des menaces, vous n'avez pas besoin de créer ou de télécharger des règles pour utiliser la détection automatisée des menaces.

La détection automatisée des menaces NetWitness Suite dispose actuellement de deux modules Domaines suspects, Commande et contrôle (C2) pour les paquets et C2 pour les logs.

Étant donné que chaque module ESA Analytics possède différentes exigences de données, vérifiez que toutes les exigences spécifiques au module sont remplies avant de déployer un module pour la détection automatisée des menaces.

Détection automatique des menaces pour les domaines suspects

Le module Domaines suspects examine votre trafic HTTP pour détecter les domaines susceptibles d'être des serveurs de commande et contrôle de malware se connectant à votre environnement. Une fois que la détection automatisée des menaces NetWitness Suite examine votre trafic HTTP, il génère des scores basés sur différents aspects du comportement de votre trafic (comme la fréquence et la régularité à laquelle un domaine donné est contacté). Si ces scores atteignent un seuil précis, une alerte ESA est générée. Cette alerte ESA est dirigée vers la vue Répondre. L'alerte dans la vue Répondre est complétée par des données qui vous aident à interpréter les scores afin de déterminer quelles étapes prendre pour la correction.

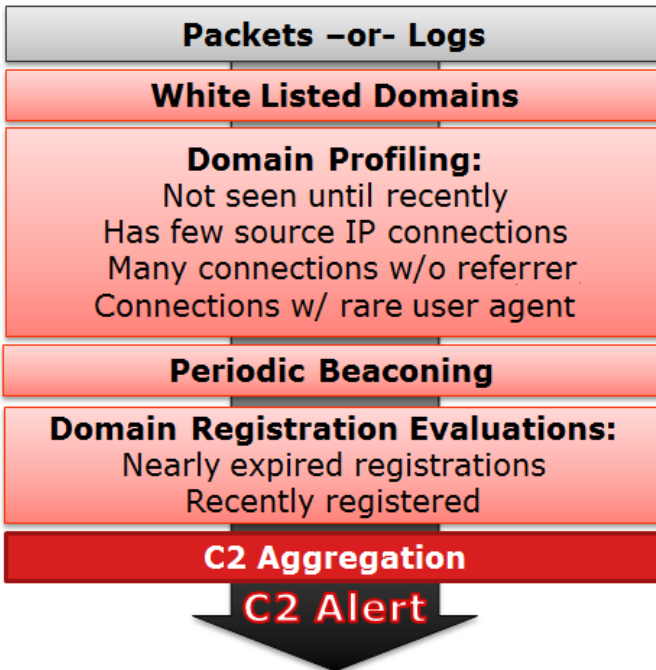
Les modules de Domaine suspect de la détection automatisée des menaces proposent des scores pour détecter les communications de commande et contrôle. Les communications de commande et contrôle se produisent lorsque du malware a compromis un système et renvoie des données à une source. Souvent, le malware de commande et contrôle peut être détecté grâce à un comportement de balisage. Le balisage se produit lorsque le malware envoie des communications régulières au serveur de commande et contrôle afin de le notifier qu'une machine a été compromise et qu'il attend de nouvelles instructions. La capacité à intercepter le malware à ce moment de la compromission peut empêcher tout dommage supplémentaire sur la machine compromise, et elle est considérée comme une étape critique dans le processus d'éradication.

La détection automatisée des menaces NetWitness Suite résout plusieurs problèmes qui se produisent lors de la recherche des programmes malveillants :

- **Capacité à utiliser des algorithmes plutôt que des signatures.** Parce que de nombreux créateurs de malware ont commencé à utiliser des segments de code polymorphique ou chiffré dont la signature est très difficile à créer, il est possible que cette approche ne détecte pas le malware. Parce que la détection automatisée des menaces NetWitness Suite utilise un algorithme basé sur le comportement, elle est capable de détecter le malware plus rapidement et plus efficacement.
- **Capacité à automatiser la chasse aux données.** La recherche manuelle dans les données est une méthode efficace mais extrêmement chronophage de trouver du malware. L'automatisation de ce processus permet à un analyste d'utiliser son temps plus efficacement.
- **Capacité à trouver rapidement une attaque.** Au lieu de regrouper les données par lot puis de les analyser, la détection automatisée des menaces analyse les données au moment de leur ingestion dans NetWitness Suite, ce qui permet une détection des attaques en temps presque réel.

Workflow du module Domaines suspects

La détection automatisée des menaces NetWitness Suite fonctionne comme un système de filtrage. Elle vérifie si certains comportements se produisent (ou si certaines conditions existent), et si ce comportement ou cette condition se produit, elle passe à l'étape suivante du processus. Cela améliore l'efficacité du système et libère des ressources de façon à ce que les événements qui ne s'avèrent pas dangereux ne soient pas retenus dans la mémoire. Le diagramme suivant propose une version simplifiée du workflow du module Domaines suspects.



- 1.) **Les paquets ou logs sont acheminés vers ESA.** Les paquets ou logs HTTP sont analysés par le Decoder ou le Log Decoder et envoyés vers l'hôte ESA.
- 2.) **La liste blanche est vérifiée.** Si vous avez créé une liste blanche via le Context Hub, ESA vérifie la liste pour éliminer des domaines. Si le domaine d'un événement est répertorié sur la liste blanche, l'événement est ignoré.
- 3.) **Le profil du domaine est vérifié.** La détection automatisée des menaces vérifie pour savoir si le domaine est nouveau (environ trois jours), s'il dispose de peu de connexions IP source, de nombreuses connexions sans référent ou de connexions avec un agent utilisateur rare. Si une ou plusieurs de ces conditions sont vraies, le domaine est ensuite vérifié par des balisages périodiques.
- 4.) **Le domaine est vérifié par un balisage périodique.** Le balisage se produit lorsque le malware envoie des communications régulières au serveur de commande et contrôle afin de le notifier qu'une machine a été compromise et qu'il attend de nouvelles instructions. Si le site présente un comportement de balisage, les informations d'enregistrement du domaine sont vérifiées.
- 5.) **Les informations d'enregistrement sont vérifiées.** Le service Whois est utilisé pour savoir si le domaine a été enregistré récemment ou s'il est sur le point d'expirer. La durée de vie très courte d'un domaine est caractéristique du malware.

6.) **Scores d'agrégation de commande et contrôle (C2)**. Chacun de ces facteurs génère un score individuel qui est pondéré pour indiquer différents niveaux d'importance. Les scores pondérés déterminent si une alerte doit être générée. Si une alerte est générée, les alertes agrégées apparaissent dans la vue Répondre et peuvent ensuite être examinées plus en détail. Lorsque les alertes commencent à apparaître dans la vue Répondre, elles continuent à s'agréger sous l'incident associé. Cela facilite le triage de nombreuses alertes qui peuvent être générées lors d'un incident de commande et contrôle.

Les analystes peuvent afficher les alertes dans la vue Répondre.

Détection automatisée des menaces de domaines suspects sur des paquets ou logs de proxy Web

RSA NetWitness Suite vous offre la possibilité d'effectuer la détection automatisée des menaces pour les domaines suspects à l'aide de deux paquets ou de logs de proxy Web. Alors que les données de paquets peuvent être transmises directement à partir du réseau dans l'installation NetWitness Suite et analysées directement, si vous avez la possibilité d'utiliser un proxy Web dans votre installation, cela peut être bénéfique. Certaines installations utilisant la traduction de réseau ou le chiffrement SSL, l'IP source réel d'une connexion sortante peut être masqué si vous l'observez au niveau du paquet. En utilisant un proxy Web, vous pouvez bénéficier de sa capacité à accélérer et à déchiffrer le trafic SSL, ainsi que de sa capacité à analyser les adresses IP source réelles du trafic qu'il surveille.

Les deux domaines suspects pour les paquets (C2 pour les paquets) et les domaines suspects pour les logs (C2 pour les logs) doivent produire les mêmes résultats. Du point de vue des résultats, l'utilisation de l'un plutôt que de l'autre n'apporte aucun avantage réel.

Configurer la détection automatisée des menaces pour les domaines suspects

Cette rubrique présente aux administrateurs et analystes la procédure à suivre pour configurer un module de domaines suspects dédié à la fonction de détection automatisée des menaces de NetWitness Suite. La fonction de détection automatisée des menaces vous permet d'analyser les données qui résident sur un ou plusieurs services Concentrator en utilisant des modules ESA Analytics préconfigurés. Par exemple, en utilisant un module de domaines suspects, un service ESA Analytics peut examiner votre trafic HTTP pour déterminer la probabilité que des activités malveillantes se produisent dans votre environnement.

Deux types de modules de domaines suspects préconfigurés sont disponibles dans NetWitness Suite : Commande et Contrôle (C2) pour les paquets et C2 pour les logs. Le module de domaines suspects définit un sous-ensemble d'événements et les activités exécutées sur ces événements pour identifier les domaines C2 suspects.

Avant de déployer un module ESA Analytics pour la fonction de détection automatisée des menaces, il importe de noter que de nombreuses configurations d'installation potentielles peuvent être installées sur le service ESA, notamment : ESA Analytics, les règles de corrélation ESA et Context Hub. Chacune de ces configurations utilise des ressources et il importe donc de penser à effectuer un dimensionnement avant de déployer la fonction de détection automatisée des menaces sur votre service ESA.

Conditions préalables

- Si vous utilisez des données de paquet, vous devez avoir configuré un service Decoder pour les données de paquet HTTP. En outre, vous devez avoir configuré un parser HTTP Lua ou Flex.
- Si vous utilisez des données de fichiers logs de proxy Web, vous devez avoir configuré le service Log Decoder approprié avec le parser correct pour votre proxy Web.
- Si vous utilisez des données de fichiers logs de proxy Web, vous devez avoir effectué une mise à jour vers les parsers de logs les plus récents. Les parsers suivants sont pris en charge : Blue Coat Cache Flow (cacheflowelff), Cisco IronPort WSA (ciscoportwsa) et Zscaler (zscalernss).
- Si vous utilisez des données de fichiers logs de proxy Web et que vous souhaitez obtenir de meilleurs résultats, vous devez configurer tous les proxys Web de la même manière (les définir sur le même fuseau horaire, utiliser la même méthode de collecte (syslog ou de

traitement par lots). Pour la méthode de traitement par lots, vous devez utiliser la même cadence de traitement par lots).

- Une connexion entre l'hôte ESA et le service Whois (même emplacement que RSA Live cms:netwitness.com:443) doit être ouverte sur le port 443. Vérifiez auprès de votre administrateur système que cette opération est terminée.
- Pour ajouter un domaine à la liste blanche, vous devez activer le service Context Hub.

Important : La fonction de détection automatisée des menaces nécessite une période de préparation qui acclimate l'algorithme au trafic sur votre réseau. Vous devez prévoir de configurer la fonction de détection automatisée des menaces de telle manière que la période de préparation puisse s'exécuter pendant le trafic normal. Par exemple, le fait de démarrer la fonction de détection automatisée des menaces un mardi à 8 h 00 dans le fuseau horaire qui contient la majorité de vos utilisateurs permet au module d'analyser avec précision une journée de trafic normal.

Configurer la fonction de détection automatisée des menaces pour les domaines suspects

Cette procédure fournit les étapes nécessaires à la configuration d'un module de domaines suspects ESA Analytics pour la fonction de détection automatisée des menaces. Les modules ESA Analytics, tels que les modules de domaines suspects, sont considérés comme préconfigurés, car vous n'êtes pas obligé de créer manuellement des règles ESA pour eux.

Les étapes de base nécessaires sont les suivantes :

1. **Configurer les paramètres de log (pour les logs uniquement).** Pour utiliser la fonction de détection automatisée des menaces, vous devez définir quelques paramètres. Ignorez cette étape si vous prévoyez d'utiliser cette fonction pour les paquets.
2. **Créez une liste blanche (facultatif) à l'aide du service Context Hub.** En créant une liste blanche, vous vous assurez que les sites couramment visités sont exclus de l'évaluation effectuée par la fonction de détection automatisée des menaces.
3. **Configurez le service de recherche Whois.** Le service de recherche Whois vous permet d'obtenir des données précises sur les domaines auxquels vous vous connectez. Afin de garantir une évaluation efficace, il importe de configurer ce service. Vérifiez que le service Whois est accessible à partir de votre environnement.
4. **Mappez des sources de données aux modules ESA Analytics.** Vous pouvez définir la manière dont la fonction de détection automatisée des menaces de NetWitness Suite doit détecter automatiquement les menaces avancées en mappant un module ESA Analytics

préconfiguré à plusieurs sources de données, telles que les services Concentrator et un service ESA Analytics.


5. **Vérifiez que la règle d'incident C2 est activée et surveillez-la pour repérer l'activité.**
Après le mappage de votre module de domaines suspects, un laps de temps est requis pour que l'algorithme de notation se mette en route. Après la période de préparation, vérifiez que la règle C2 est activée dans les règles de l'incident et surveillez si elle se déclenche.
6. **Vérifiez que les règles de l'incident sont correctement configurées.** Lorsque vous affichez les incidents dans la vue Répondre, il est judicieux de les regrouper par C&C suspect.

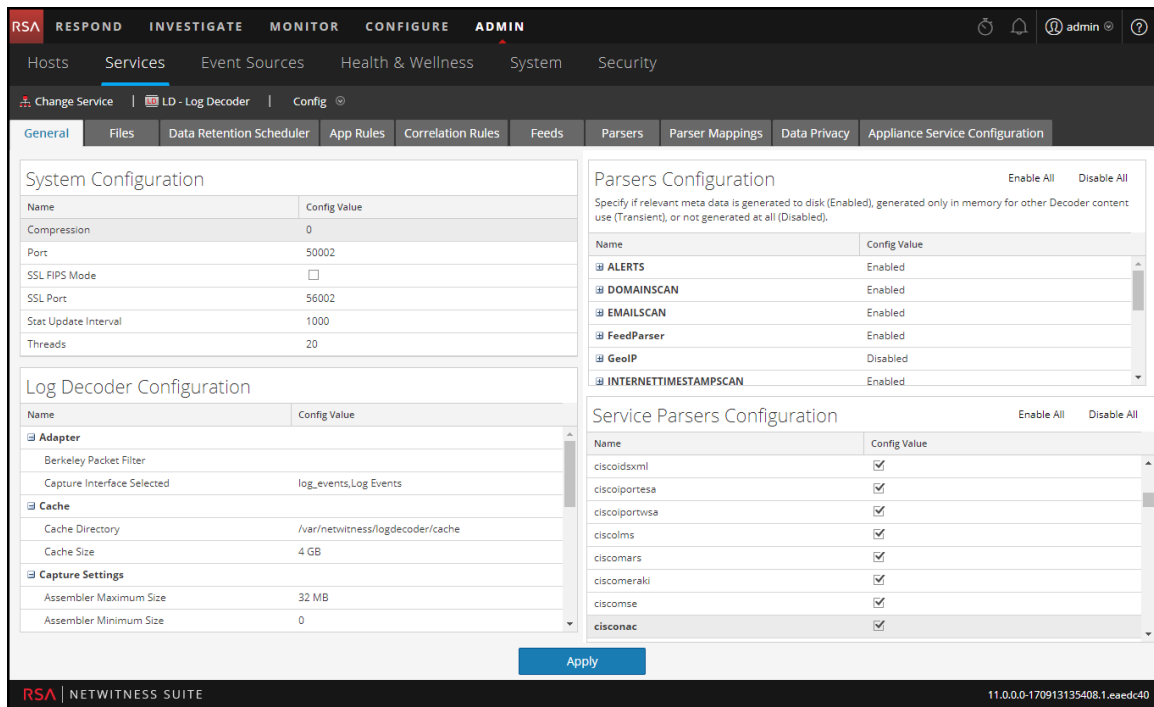
Étape 1 : (Pour les logs uniquement) Configurer les paramètres de log

Pour configurer la fonction de détection automatisée des menaces pour les logs, vous devez effectuer quelques étapes de configuration supplémentaires :

- Vérifiez que les parsers pris en charge sont activés pour votre service Log Decoder.
- Obtenez les dernières versions du parser de proxy Web approprié à partir de RSA Live.
- Mettez à jour le mappage dans le fichier de configuration Envision. Ce fichier est nécessaire pour mettre à jour le service Log Decoder afin qu'il fonctionne avec les nouvelles métadonnées disponibles via les parsers.
- Vérifiez que le fichier table-map.xml a été mis à jour correctement.
- Vérifiez que les index ont été mis à jour correctement.

Pour vérifier que vos parsers sont en cours d'exécution sur votre service Log Decoder :

1. Accédez à **ADMIN > Services**.
2. Sélectionnez votre Log Decoder, puis  > **Vue > Config**.
La section Configuration des analyseurs de service affiche la liste des parsers activés.
3. Vérifiez que le parser de proxy Web approprié est activé.



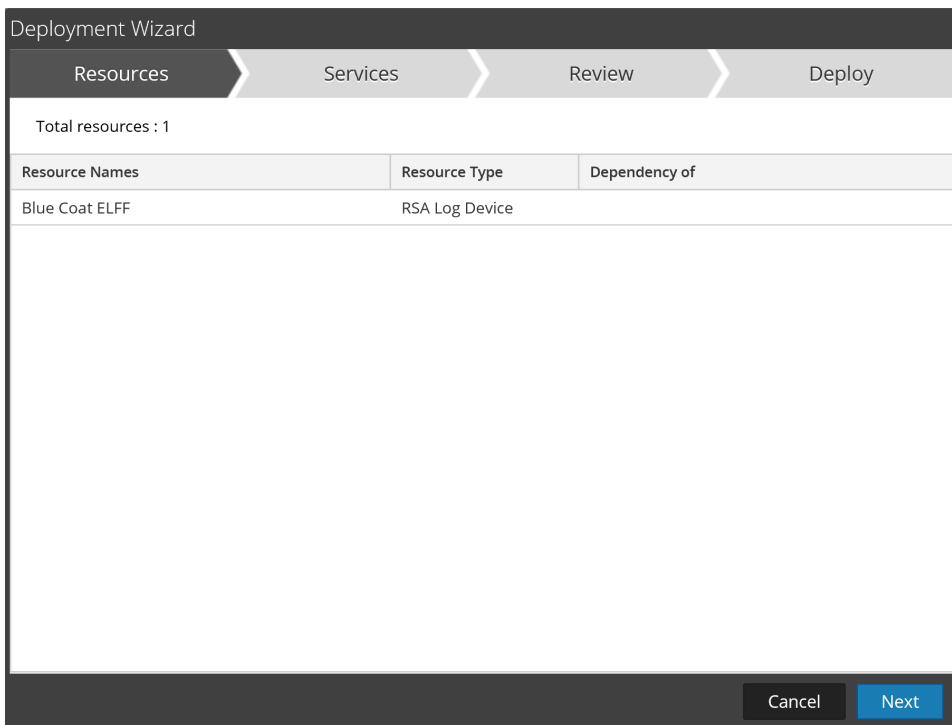
Pour obtenir les derniers parsers à partir de RSA Live :

1. Accédez à **CONFIGURER > Live Content**.
2. Saisissez un terme de recherche pour l'un des parsers de proxy Web pris en charge.
3. Sélectionnez le parser de proxy Web approprié [par exemple, le parser Blue Coat ELFF (cacheflowelf)].

Remarque : Vous devez avoir suivi les étapes de configuration de la consignation de manière à ce qu'elle s'effectue correctement sur votre parser de proxy Web.

4. Cliquez sur **Déployer**.

L'assistant de déploiement s'ouvre.



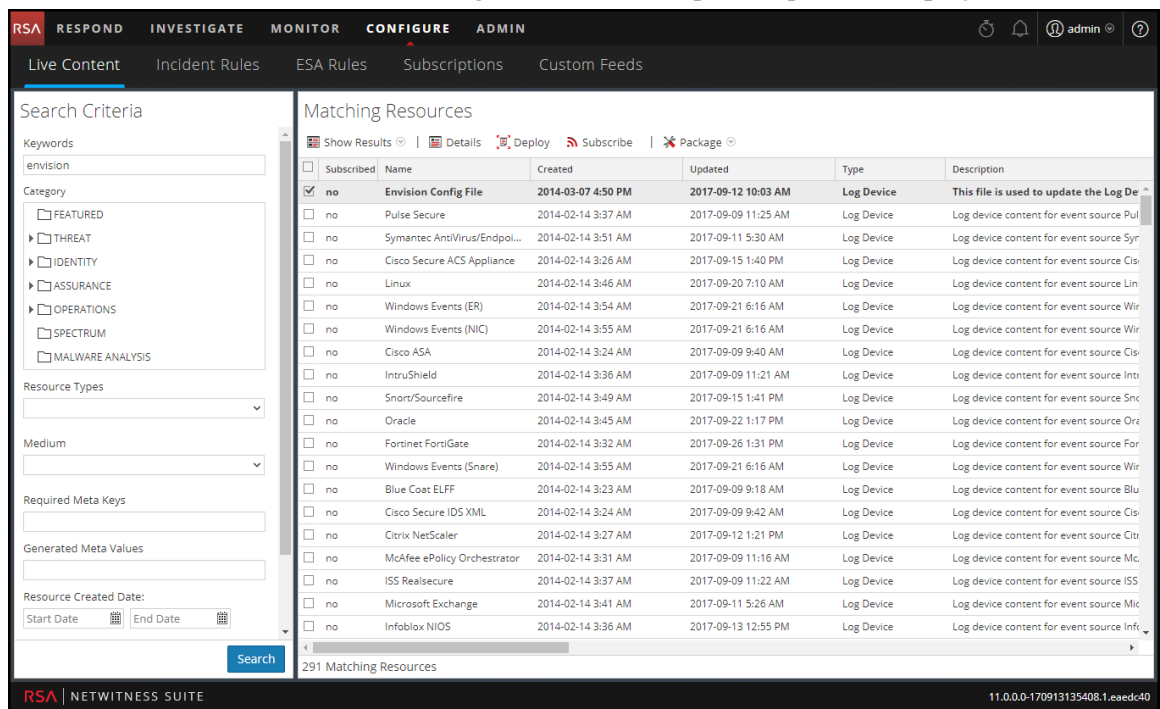
5. Sous **Services**, sélectionnez le service Log Decoder.

6. Cliquez sur **Déployer** pour déployer le parser sur votre Log Decoder.

Pour obtenir le dernier fichier de configuration Envision, procédez comme suit :


1. Accédez à **CONFIGURER > Live Content**.
2. Saisissez **envision** comme mot clé pour effectuer la recherche.

- Sélectionnez le dernier fichier de configuration Envision, puis cliquez sur **Déployer**.




- Dans l'assistant de déploiement, sous **Services**, sélectionnez votre service Log Decoder.
- Cliquez sur **Déployer** pour déployer le fichier de configuration Envision vers le Log Decoder.

Pour vérifier que le fichier de configuration Envision a été mis à jour correctement :

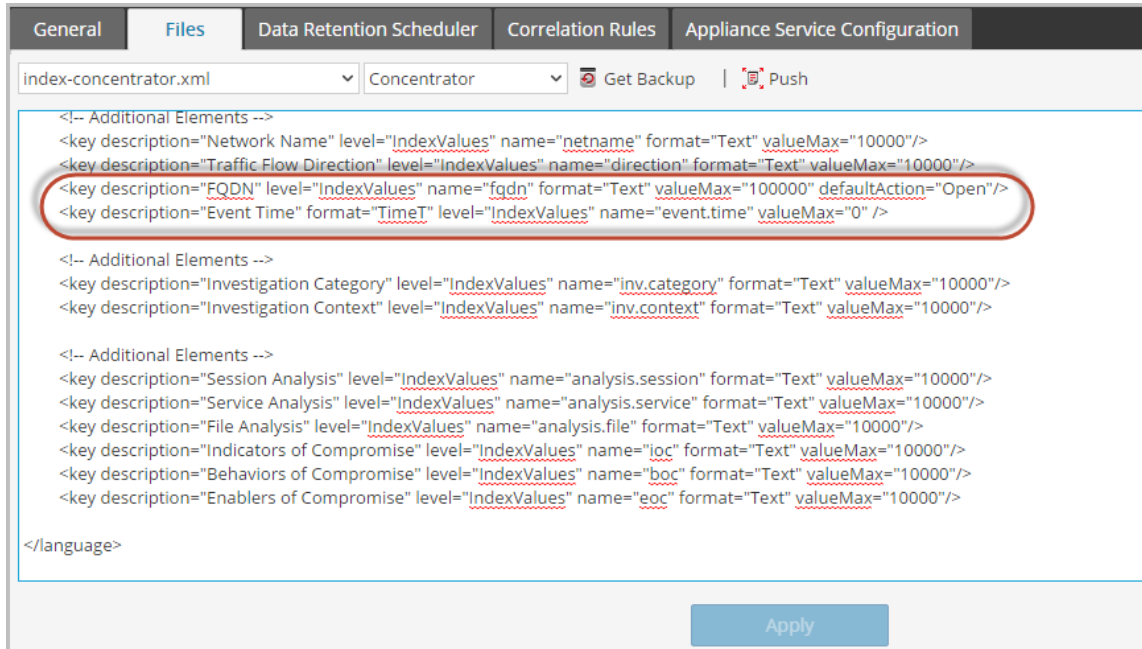
- Accédez à **ADMIN > Services**, sélectionnez le service Log Decoder, puis l'onglet  > **Vue > Config > Fichiers**.
Le fichier **table-map.xml** est visible. Ce fichier est modifié lorsque vous mettez à jour le fichier de configuration Envision.
- Recherchez le terme *event.time*. Le champ doit désormais afficher *"event.time" flags = "None"*. Cela signifie que la métadonnée event.time est désormais incluse dans le mappage. De même, l'indicateur de nom de domaine complet doit être défini sur « None ».

Pour vérifier que les index du fichier index-concentrator.xml ont été mis à jour :

Vous devez vérifier que le fichier **index-concentrator.xml** comprend la métadonnée event.time et celle de nom de domaine complet.

1. Accédez à **ADMIN > Services**, sélectionnez votre service Concentrator, puis sélectionnez  > **Vue > Config.**
2. Sous l'onglet Fichiers, recherchez le fichier **index-concentrator.xml**.
3. Vérifiez que l'entrée suivante existe dans le fichier index-concentrator.xml. Si ce n'est pas le cas, vous devez vérifier que votre Concentrator a été mis à niveau vers la version correcte :

```
<key description="FQDN" level="IndexValues" name="fqdn" format="Text" valueMax="100000" defaultAction="Open"/><key description="Event Time" format="TimeT" level="IndexValues" name="event.time" valueMax="0" />
```



The screenshot shows the configuration interface for the 'index-concentrator.xml' file. The 'Files' tab is selected, and the XML content is displayed. The entry for 'FQDN' is highlighted with a red circle, indicating the required configuration.

```
<!-- Additional Elements -->
<key description="Network Name" level="IndexValues" name="netname" format="Text" valueMax="10000"/>
<key description="Traffic Flow Direction" level="IndexValues" name="direction" format="Text" valueMax="10000"/>
<key description="FQDN" level="IndexValues" name="fqdn" format="Text" valueMax="100000" defaultAction="Open"/>
<key description="Event Time" format="TimeT" level="IndexValues" name="event.time" valueMax="0" />

<!-- Additional Elements -->
<key description="Investigation Category" level="IndexValues" name="inv.category" format="Text" valueMax="10000"/>
<key description="Investigation Context" level="IndexValues" name="inv.context" format="Text" valueMax="10000"/>

<!-- Additional Elements -->
<key description="Session Analysis" level="IndexValues" name="analysis.session" format="Text" valueMax="10000"/>
<key description="Service Analysis" level="IndexValues" name="analysis.service" format="Text" valueMax="10000"/>
<key description="File Analysis" level="IndexValues" name="analysis.file" format="Text" valueMax="10000"/>
<key description="Indicators of Compromise" level="IndexValues" name="ioc" format="Text" valueMax="10000"/>
<key description="Behaviors of Compromise" level="IndexValues" name="boc" format="Text" valueMax="10000"/>
<key description="Enablers of Compromise" level="IndexValues" name="eoc" format="Text" valueMax="10000"/>

</language>
```

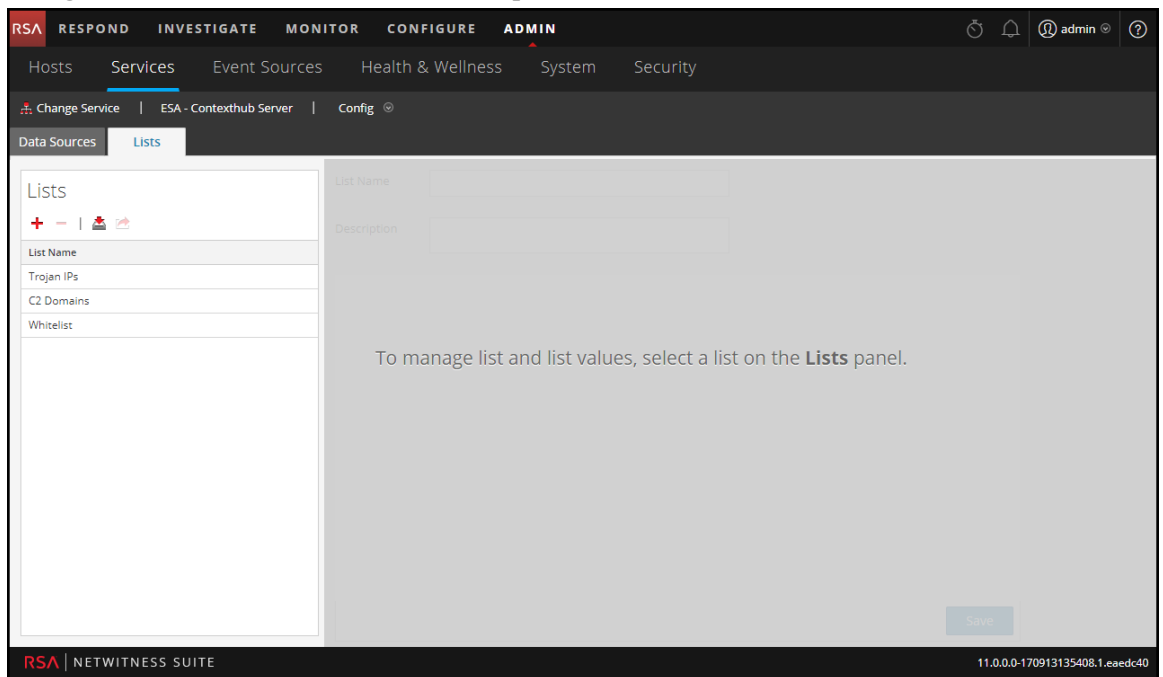
Étape 2 : Créer une liste blanche Domaines (facultatif)

Cette procédure est appliquée lors de l'utilisation de la fonction de détection automatisée des menaces afin de garantir que certains domaines ne déclenchent pas d'indice de menace. Parfois, un domaine auquel vous accédez régulièrement peut déclencher un score de détection automatisée des menaces. Par exemple, un service météorologique peut avoir un comportement de beaconing similaire à celui d'une communication de commande et contrôle et déclencher alors un indice négatif non garanti. Dans ce cas, il s'agit d'un faux positif. Pour empêcher le déclenchement d'un faux positif avec un domaine spécifique, vous pouvez ajouter ce domaine à une liste blanche. La plupart des domaines n'ont pas besoin d'être ajoutés à une liste blanche, car la solution n'émet d'alertes que pour les comportements très suspects. Les domaines que vous pouvez ajouter à une liste blanche sont des services automatisés valides qui possèdent peu de connexions hôtes.

Remarque : Pour les migrations à partir de la version 10.6.x, si votre liste blanche précédente de détection automatisée des menaces (domaines sur liste blanche) s'affiche sous l'onglet Listes, vous pouvez la renommer **domains_whitelist** pour l'utiliser avec les modules de domaines suspects.

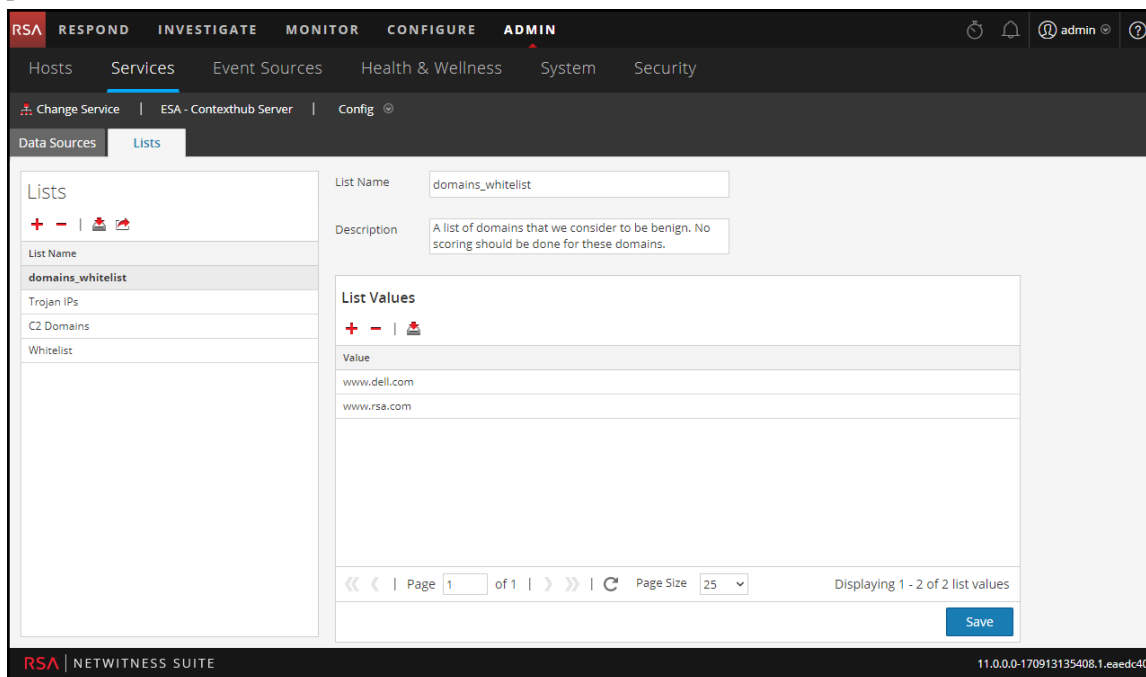
1. Créer une liste blanche de domaines dans Context Hub nommée **domains_whitelist**:
 - a. Accédez à **ADMIN > Services**, sélectionnez le service Context Hub Server, puis **Vue > Config > Listes**.

L'onglet Listes affiche les listes actuelles présentes dans le service Context Hub.






- b. Dans le panneau Listes, cliquez sur **+** pour ajouter une liste. Dans le champ **Nom de la liste**, saisissez **domains_whitelist**. Vous devez utiliser ce nom pour que le module

puisse identifier la liste.



2. Ajoutez manuellement des domaines à la liste ou importez un fichier .CSV contenant une liste de domaines.

Vous pouvez saisir des domaines complets, ou vous pouvez utiliser un caractère générique pour inclure tous les sous-domaines d'un domaine donné. Par exemple, vous pouvez saisir *.gov pour ajouter à la liste blanche toutes les adresses IP de l'administration. Toutefois, vous ne pouvez pas utiliser d'autres fonctions de regex, par exemple [a-z]*.gov. En effet, si vous utilisez *.gov, la chaîne entière, par exemple www.irs.gov, est remplacée.

 - a. Pour ajouter des domaines manuellement, dans la section **Valeurs de la liste**, cliquez sur  pour ajouter des domaines.
 - b. Pour supprimer un domaine, sélectionnez-le et cliquez sur .
 - c. Pour importer un fichier .CSV, dans la section **Valeurs de la liste**, cliquez sur  et, dans la boîte de dialogue **Importer les valeurs de la liste**, accédez au fichier .CSV. Choisissez parmi les séparateurs suivants : Virgule, Saut de ligne et Retour chariot en fonction du séparateur que vous avez choisi pour séparer les valeurs. Cliquez sur **Télécharger**.
3. Cliquez sur **Enregistrer**.

La liste **domains_whitelist** s'affiche dans le panneau Listes. Les analystes peuvent ajouter des éléments à cette liste dans la vue Répondre et d'autres parties de la procédure

d'enquête. Le *Guide de configuration de Context Hub* fournit des informations supplémentaires.

Étape 3 : Configurer le service de recherche Whois

Consultez la rubrique « Configurer le service de recherche Whois » dans le *Guide de configuration ESA*.

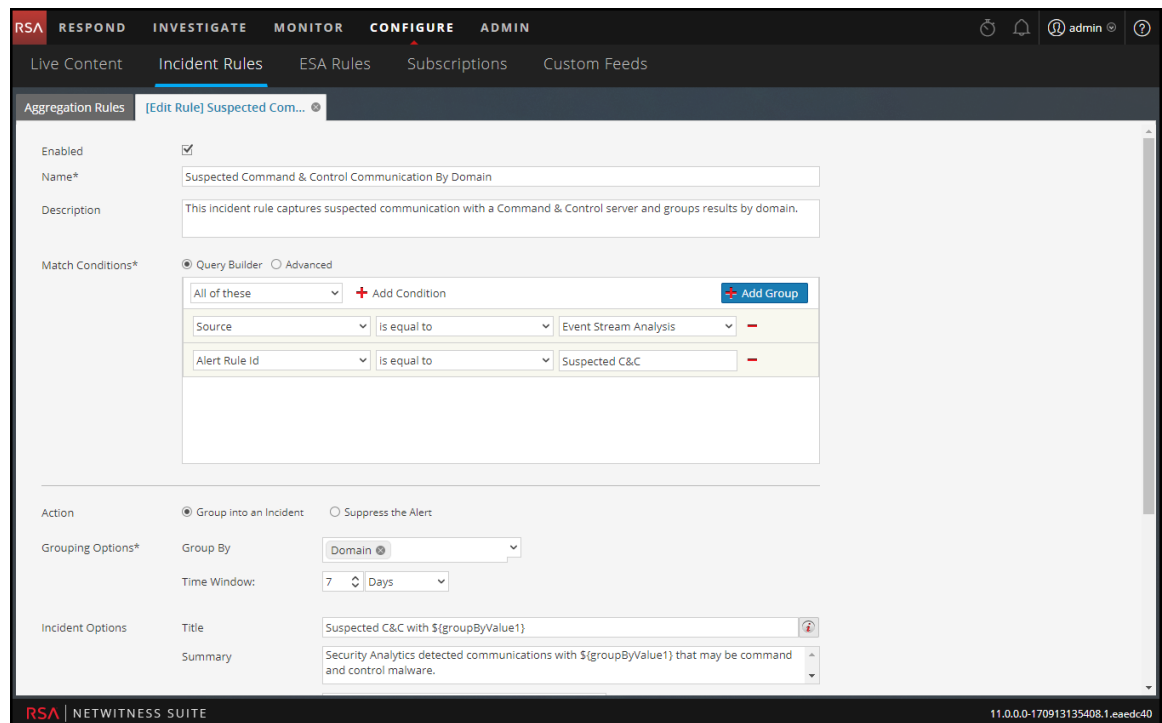
Étape 4 : Mapper des sources de données à des modules ESA Analytics

Consultez la rubrique « Mappage des sources de données ESA aux modules Analytics » dans le *Guide de configuration ESA*.

Étape 5 : Vérifier que la règle **Commande et contrôle suspect par domaine** est activée et surveiller la règle

Vérifiez la règle **Commande et contrôle suspect par domaine** dans les règles de l'incident.

1. Accédez à **CONFIGURER > Règles de l'incident > Règles d'agrégation**.
2. Sélectionnez la règle **Communication de commande et contrôle suspect par domaine**, et double-cliquez dessus pour l'ouvrir.



3. Vérifiez que **Activé** est sélectionné.

Une fois que la règle est activée, elle est repérée par un bouton **Activé** vert.

Résultat

Une fois que vous avez déployé le mappage du module ESA Analytics de domaines suspects pour la fonction de détection automatisée des menaces, votre service ESA commence à effectuer l'analytique sur le trafic HTTP. Vous pouvez afficher des informations détaillées sur chaque incident dans la vue Répondre.

Étape 6 : Vérifier que l'incident est regroupé par C&C suspect

Pour regrouper des incidents correctement dans la vue Répondre, définissez la condition Regrouper par sur *Domaine*.

1. Accédez à **CONFIGURER > Règles de l'incident > Règles d'agrégation**.
2. Sélectionnez la règle **Communication de commande et contrôle suspect par domaine**, et double-cliquez dessus pour l'ouvrir.
3. Vérifiez que le champ **Regrouper par** est défini sur *Domaine*.

Cette option permet de regrouper les alertes et de créer des incidents pour « C&C suspect ».

Étapes suivantes

Surveiller la vue Répondre pour voir si la règle se déclenche. Le *Guide d'utilisation de NetWitness Respond* fournit des informations supplémentaires.

Dépannage de la détection automatisée des menaces avec NetWitness Suite

NetWitness Suite La détection automatisée des menaces est un moteur d'analyse qui examine vos données HTTP. Il permet également d'utiliser d'autres composants, comme les services Whois et Context Hub, qui peuvent ajouter de la complexité à votre installation. Cette rubrique fournit des suggestions vous permettant de trouver des solutions si le déploiement de votre détection automatisée des menaces ne fournit pas les résultats escomptés.

Problèmes possibles

Problème	Causes possibles	Solutions
De nombreuses alertes s'affichent à l'écran (fausses alertes).	Plusieurs	Une cause possible est que le service de recherche Whois échoue ou est mal configuré. La recherche Whois est utile pour déterminer si une URL est valide, et si la connexion échoue ou n'est pas correctement configurée, ce qui entraîne de fausses alertes. Consultez la section « Configurer le service de recherche Whois » dans le <i>Guide de configuration ESA</i> .
		Vous devrez peut-être créer une liste blanche des URL. Parfois, le comportement légitime d'une URL déclenche une alerte. Une façon d'éviter ce problème est d'ajouter l'URL à la liste blanche. Consultez la section « Ajouter une entité à une liste blanche » dans le <i>NetWitness Respond Guide d'utilisation</i> .

Problème	Causes possibles	Solutions
Je ne vois aucune alerte.	L'hôte ESA nécessite une période de préparation lorsque vous déployez un mappage de module ESA Analytics pour la détection automatisée des menaces.	Lorsque vous déployez un mappage de module ESA Analytics pour la détection automatisée des menaces, il existe une période de préparation durant laquelle aucune alerte ne s'affiche à l'écran. Chaque type de module dispose d'une période de préparation par défaut et vous devez attendre jusqu'à la fin de cette période. Pour plus d'informations, consultez la section « Mappage des sources de données ESA aux modules Analytics » dans le <i>Guide de configuration ESA</i> .
Je rencontre des problèmes de performance (utilisation accrue des ressources ou baisse du débit).	Plusieurs	Si vous rencontrez des problèmes de performance sur un hôte ESA qui exécute la détection automatisée des menaces (ESA Analytics) et les règles ESA, suivez les étapes de dépannage relatives aux règles. Pour en savoir plus sur ces étapes de dépannage, accédez à la section « Dépanner le service ESA » dans le <i>Guide des alertes basées sur ESA</i> .