RSA NETWITNESS® SUITE

Guide d'utilisation de NetWitness Respond

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

Processus NetWitness Respond

NetWitness Suite Respond collecte les alertes émises par plusieurs sources et permet de les regrouper de façon logique et de démarrer un workflow de réponse aux incidents pour identifier et corriger les problèmes de sécurité. NetWitness Suite Respond vous permet de configurer des règles qui agrègent des alertes en incidents. Les alertes sont normalisées par le système dans un format commun pour offrir aux utilisateurs une vue homogène des critères de règle indépendamment de la source de données. Vous pouvez élaborer des critères de requête basés sur les données d'alerte et effectuer des recherches dans les champs communs et propres aux sources de données.

Le moteur de règle vous permet de regrouper des alertes similaires dans un incident pour que le workflow de recherche et de correction puisse être partagé entre différentes alertes semblables. Vous pouvez créer des règles pour regrouper des alertes dans des incidents sur la base d'une valeur commune pour un ou deux attributs (par exemple, nom d'hôte de la source) ou si elles sont signalées dans une fenêtre limitée (par exemple, alertes distantes de quatre heures).

Si une alerte satisfait une règle, un incident est créé à l'aide des critères définis. Pour les nouvelles alertes, si un incident répondant aux critères a déjà été créé et qu'il n'est pas encore en cours, les nouvelles alertes continues à être ajoutées au même incident. S'il n'existe aucun incident pour la valeur groupée (par exemple, le nom d'hôte) ou la fenêtre, un nouvel incident est créé et l'alerte lui est ajoutée.

Vous pouvez avoir plusieurs règles d'agrégation. Les règles peuvent regrouper des alertes dans des incidents ou empêcher que des alertes correspondent à des règles. Les règles sont donc classées dans l'ordre décroissant et seule la première règle correspondant à une alerte entrante doit être utilisée pour inclure l'alerte en question dans un incident. Les incidents fournissent du contexte aux alertes et des outils pour enregistrer l'état de la procédure d'enquête, et permettent de suivre la progression des tâches associées.

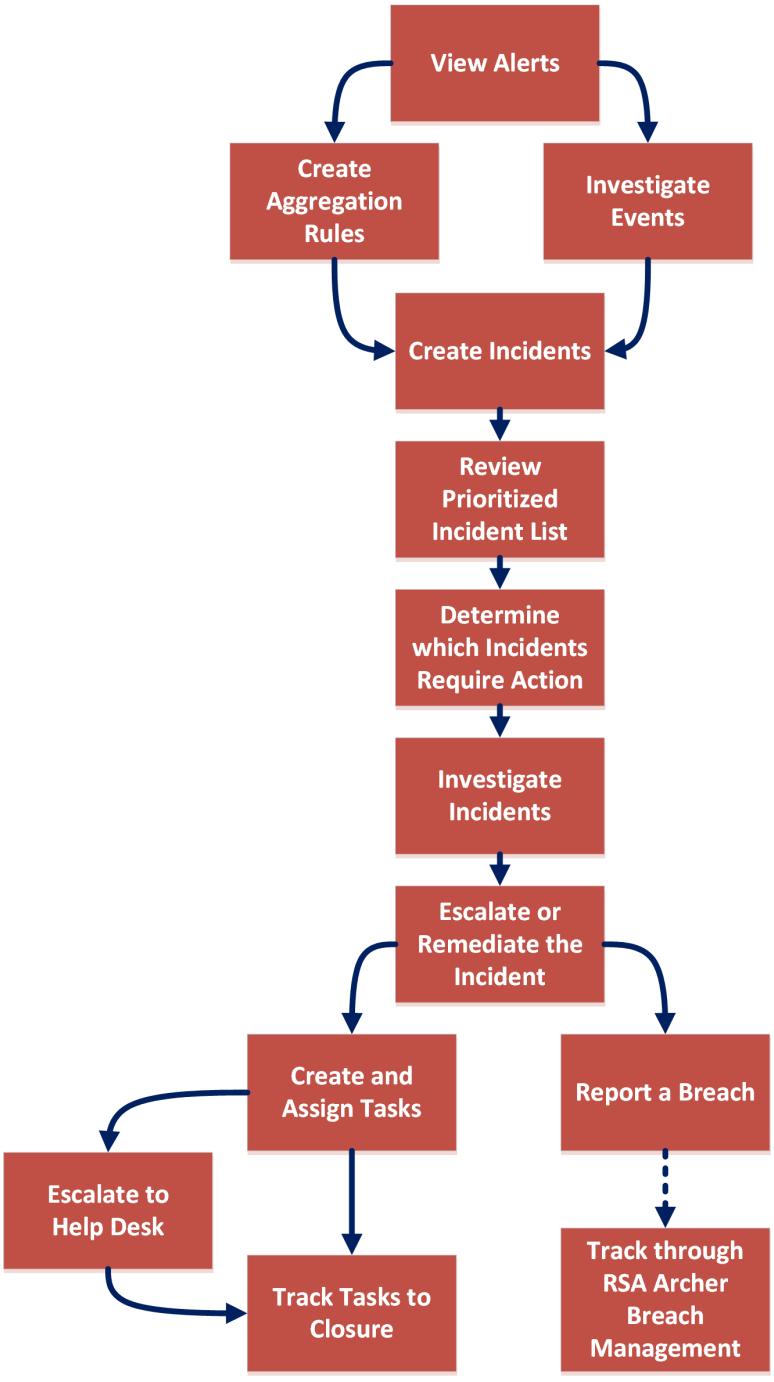
Les phases du processus NetWitness Respond sont les suivantes :

- Vérifier les alertes
- Créer des incidents
- Répondre aux incidents :
  - Passer en revue la liste des incidents hiérarchisés
  - Déterminer les incidents exigeant une action
  - Analyser des incidents
  - Faites remonter ou corriges l’incident (cela inclut la création et l’attribution de tâches, ainsi que le suivi des tâches jusqu'à la fermeture).

Vous avez également la possibilité de gérer les incidents dans NetWitness SecOps Manager au lieu de NetWitness Respond.

Workflow NetWitness Respond

La figure suivante illustre le processus général de workflow NetWitness Respond.



Réponse aux incidents

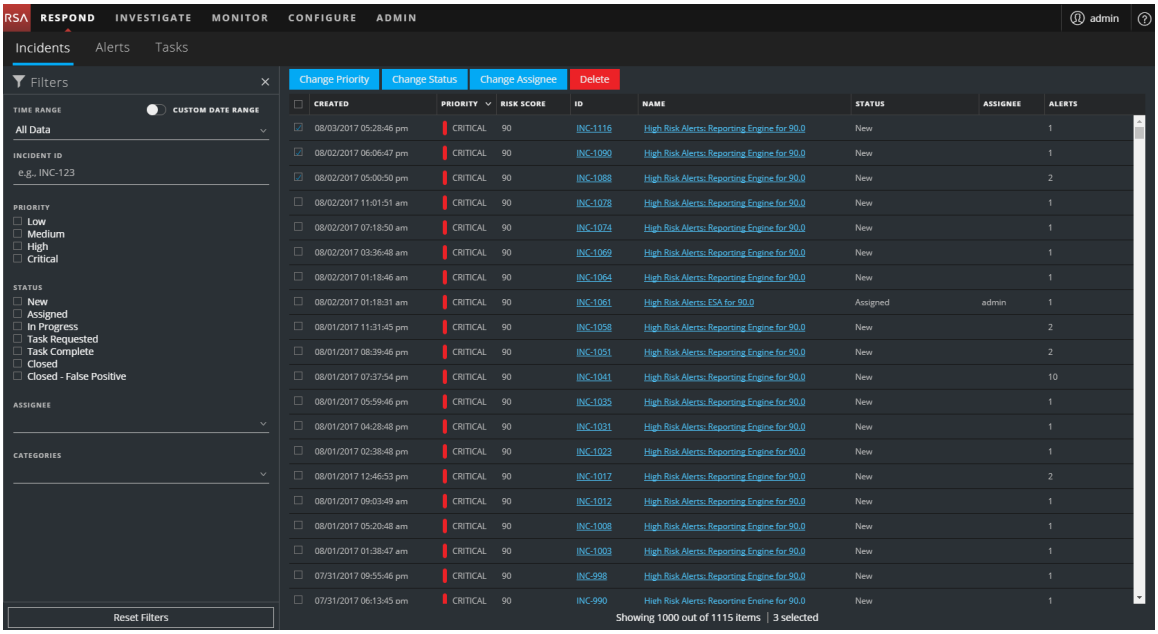
La vue **Répondre** est conçue pour vous aider à identifier rapidement les problèmes en cours sur votre réseau et à travailler avec d'autres analystes afin de les résoudre rapidement.

La vue Répondre présente aux Responsable de la réponse aux incidents une file d'attente d'incidents par ordre de gravité. Lorsque vous intégrez un incident à la file d'attente, vous recevez des données de support pertinentes pour vous aider à enquêter sur l'incident. Cela vous permet de déterminer la portée de l'incident et de le faire remonter ou bien de le corriger, le cas échéant.

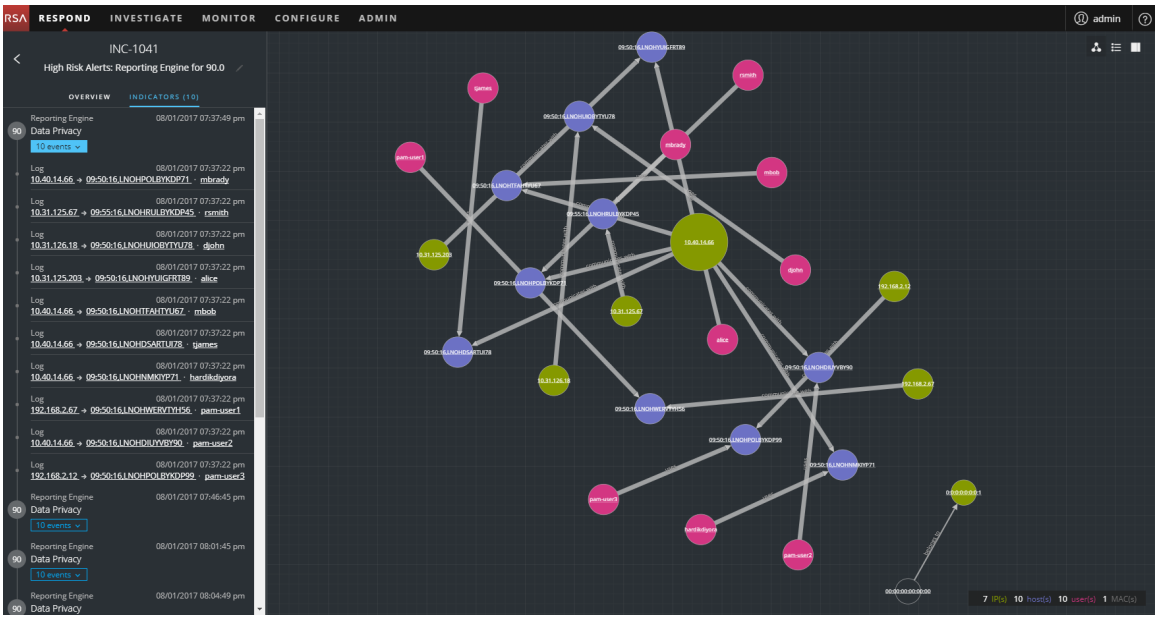
Dans la vue Répondre, vous pouvez afficher les Incidents, les Alertes et les Tâches :

- **Incidents** : Permet de répondre aux incidents et de les gérer du début à la fin.
- **Alertes** : Permet de gérer les alertes à partir de toutes les sources reçues par NetWitness Suite et de créer des incidents à partir des alertes sélectionnées.
- **Tâches** : Permet d'afficher et de gérer la liste complète de tâches créées pour tous les incidents.

Si vous accédez à Répondre > Incidents, vous pouvez afficher la vue Liste d'incidents et à partir de là, vous pouvez accéder à la vue Détails de l'incident pour un incident sélectionné. Voici les principales vues qui vous permettent de répondre aux incidents. La figure suivante présente la liste des incidents de priorité dans la vue **Liste d'incidents**.



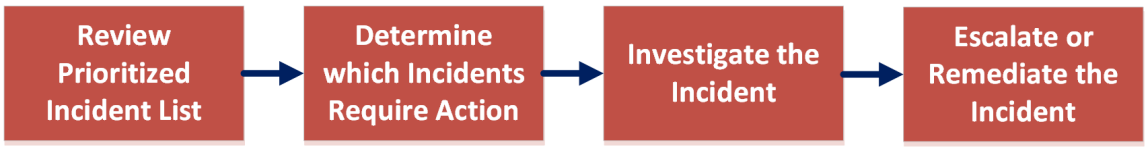
La figure suivante présente un exemple d'informations disponibles dans la vue **Détails de l'incident**.



La vue Répondre est conçue pour aider à évaluer des incidents, contextualiser ces données, collaborer avec d'autres analystes et pivoter vers une procédure d'enquête approfondie en fonction des besoins.

Workflow de réponse aux incidents

Ce workflow montre le processus de haut niveau que les Responsables de la réponse aux incidents utilisent pour répondre aux incidents dans NetWitness Suite.



Tout d'abord, vous passez en revue la liste d'incidents prioritaires, qui affiche des informations de base sur chaque incident, et vous déterminez les incidents qui exigent une action. Vous pouvez cliquer sur un lien dans un incident pour obtenir une vue plus claire de l'incident, avec des détails associés dans la vue Détails de l'incident. À partir de là, vous pouvez étudier davantage l'incident. Vous pouvez ensuite déterminer comment répondre à l'incident, en le faisant remonter ou en le corrigeant.

Voici les étapes de base pour répondre à un incident :

1. Passer en revue la liste des incidents hiérarchisés
2. Déterminer les incidents exigeant une action
3. Enquêter sur l'incident
4. Faire remonter ou corriger l'incident

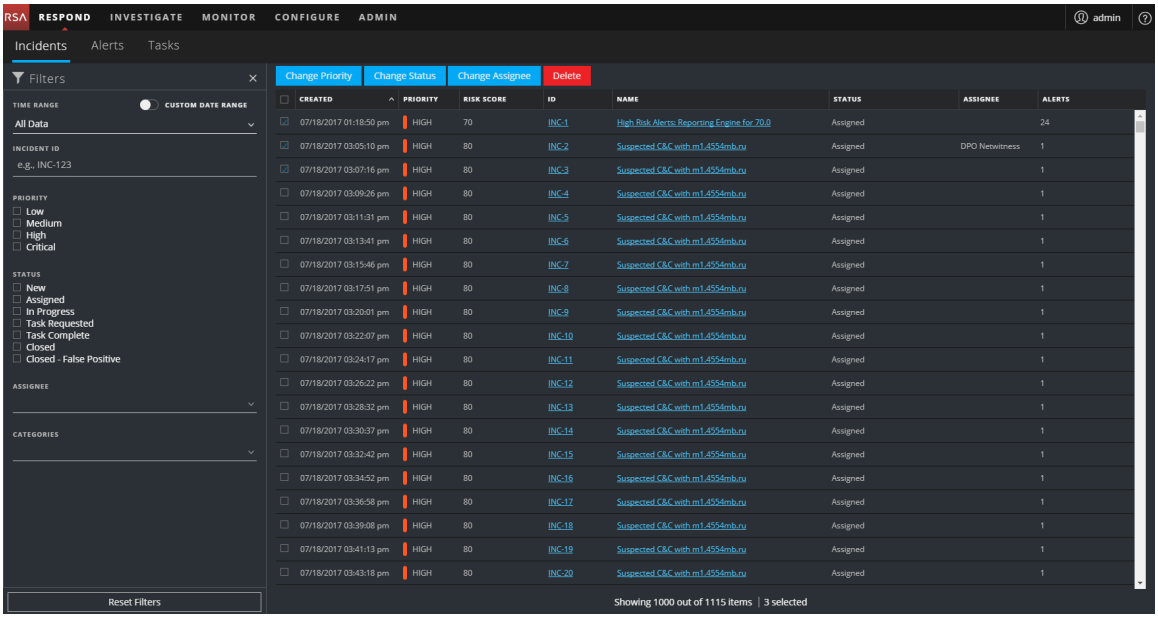
Passer en revue la liste des incidents hiérarchisés

Dans la vue Répondre, vous pouvez afficher les incidents prioritaires. La Liste Incidents affiche les incidents à la fois clôturés et actifs.

Afficher la liste des incidents

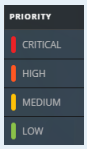
Une fois connectés à NetWitness Suite, la plupart des Responsables de la réponse aux incidents ont accès à la vue Répondre, qui est définie sur la vue par défaut. Si votre vue initiale est différente, vous pouvez naviguer jusqu'à la vue Répondre.

1. Connectez-vous à NetWitness Suite.
   La vue Répondre affiche la liste des incidents, également appelée Vue Liste des incidents.



2. Si vous ne voyez pas la liste d'incidents dans la vue Répondre, accédez à **RÉPONDRE > Incidents**.
3. Faites défiler la liste des incidents, qui affiche des informations de base sur chaque incident, comme décrit dans le tableau suivant.

Colonne	Description
DATE DE CRÉATION	Affiche la date de création de l'incident.

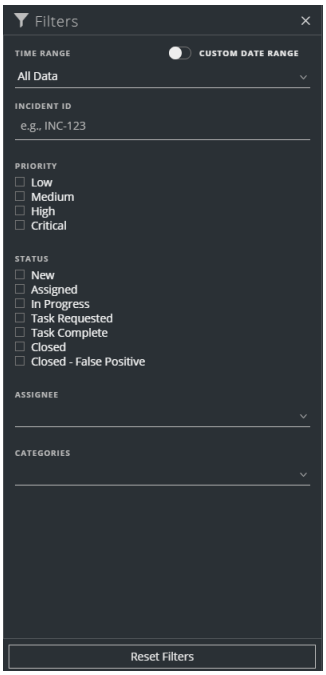
Colonne	Description
PRIORITÉ	Affiche la priorité de l'incident. La priorité peut être critique, élevée, moyenne ou faible. La Priorité est désignée par un code couleur où le rouge indique un incident **critique**, l'orange un incident à risque **élevé**, le jaune un incident à risque **moyen** et le vert un incident à **faible** risque. Par exemple : 
SCORE DE RISQUE	Affiche le score de risque de l'incident. Le score de risque indique le risque de l'incident, calculé via un algorithme et compris entre 0 et 100. 100 désigne le score de risque le plus élevé.
ID	Indique le numéro d'un incident créé automatiquement. Un numéro unique que vous pouvez utiliser pour effectuer le suivi de l'incident est attribué à chaque incident.
NOM	Affiche le nom de l'incident. Le nom de l'incident est dérivé de la règle utilisée pour déclencher l'incident. Cliquez sur le lien pour accéder à la vue Détails sur l'incident sélectionné.
ÉTAT	Affiche l'état de l'incident. L'état peut être : **Nouveau**, **Attribué**, **En cours**, **Tâche demandée**, **Tâche terminée**, **Clôturé** et **Clôturé - Faux positif**.
PERSONNE AFFECTÉE	Affiche le membre de l'équipe actuellement attribué à l'incident.
ALERTES	Affiche le nombre d'alertes associées à l'incident. Un incident peut inclure de nombreuses alertes. Un grand nombre d'alertes peut signifier que vous êtes confronté à une attaque à grande échelle.

Au bas de la liste, vous voyez le nombre d'incidents sur la page en cours, le nombre total d'incidents et le nombre sélectionné. Par exemple : **Affichage 1 000 éléments sur 1 115 | 3 sélectionnés**. Le nombre maximal d'incidents que vous pouvez afficher en même temps est 1 000.

Filtrer la liste des incidents

Le nombre d'incidents dans la Liste d'incidents peut être très volumineux, ce qui complexifie la recherche de tâches particulières. Le filtre vous permet de spécifier les incidents que vous souhaitez afficher. Vous pouvez également choisir la période d'apparition de ces incidents. Par exemple, vous pouvez afficher tous les incidents critiques et nouveaux qui ont été créés au cours de la dernière heure.

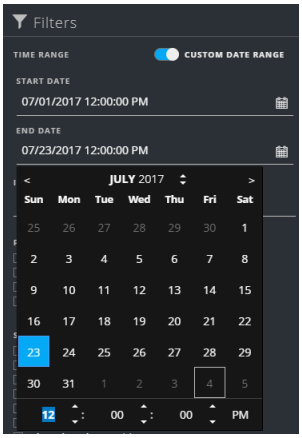
1. Vérifiez que le panneau Filtres apparaît à gauche de la liste des incidents. Si vous ne voyez pas le panneau Filtres, dans la barre d'outils de la vue Liste des incidents, cliquez sur afin d'ouvrir le panneau Filtres.



2. Dans le panneau Filtres, sélectionnez une ou plusieurs options pour filtrer la liste des incidents :

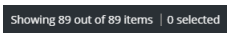
   - **PLAGE TEMPORELLE** : Vous pouvez sélectionner une période spécifique dans la liste déroulante Période. La période est basée sur la date de création des incidents. Par exemple, si vous sélectionnez Dernière heure, vous verrez les incidents qui ont été créés au cours des 60 dernières minutes.
   - **PLAGE DE DATES PERSONNALISÉE** : Vous pouvez spécifier une plage de dates spécifique au lieu de sélectionner une option de période. Pour ce faire, cliquez sur le cercle blanc devant Plage de dates personnalisée pour afficher les champs Date de début

et Date de fin. Sélectionnez les dates et heures dans le calendrier.



- **ID D'INCIDENT** : Saisissez l'ID d'incident pour un incident que vous souhaitez rechercher, par exemple INC-1050.
- **PRIORITÉ** : Sélectionnez les priorités que vous souhaitez afficher.
- **ÉTAT** : Sélectionnez un ou plusieurs états d'incident. Par exemple, sélectionnez Clôturé - Faux positif pour afficher uniquement les incidents à l'état faux positif, c'est-à-dire qui ont été initialement identifiés comme suspects et qui ont ensuite été identifiés comme sûrs.
- **PERSONNE AFFECTÉE** : Sélectionnez la ou les personnes affectées aux incidents que vous souhaitez afficher. Par exemple, si vous souhaitez uniquement afficher les incidents attribués à Cale ou à Stanley, sélectionnez Cale et Stanley dans la liste déroulante Personne affectée. Si vous souhaitez afficher les incidents, quelle que soit la personne affectée, n'effectuez pas de sélection dans la liste Personne affectée.
- **CATÉGORIES** : Dans la liste déroulante, sélectionnez une ou plusieurs catégories. Par exemple, si vous souhaitez uniquement afficher les incidents classés avec les catégories Porte dérobée ou Abus de privilège, sélectionnez Porte dérobée et Abus de privilège.

La liste des incidents affiche une liste d'incidents qui répondent à vos critères de sélection. Vous pouvez voir le nombre d'incidents dans votre liste filtrée en bas de la liste des incidents.



3. Cliquez sur ✕ pour fermer le panneau Filtres et revenir à la vue Liste d'incidents, qui affiche maintenant vos incidents filtrés.

Supprimer mes filtres de la vue Liste des incidents

NetWitness Suite mémorise vos sélections de filtre dans la vie Liste des incidents. Vous pouvez supprimer vos sélections de filtre lorsque vous n'en avez plus besoin. Par exemple, si vous ne voyez pas le nombre d'incidents que vous devriez voir ou si vous souhaitez afficher tous les incidents dans la liste d'incidents, vous pouvez réinitialiser les filtres.

1. Dans la barre d'outils Vue de la Liste des incidents, cliquez sur .
   Le panneau filtres s'affiche à gauche de la liste des incidents.
2. Au bas du panneau Filtres, cliquez sur **Réinitialiser les filtres**.

Afficher mes incidents

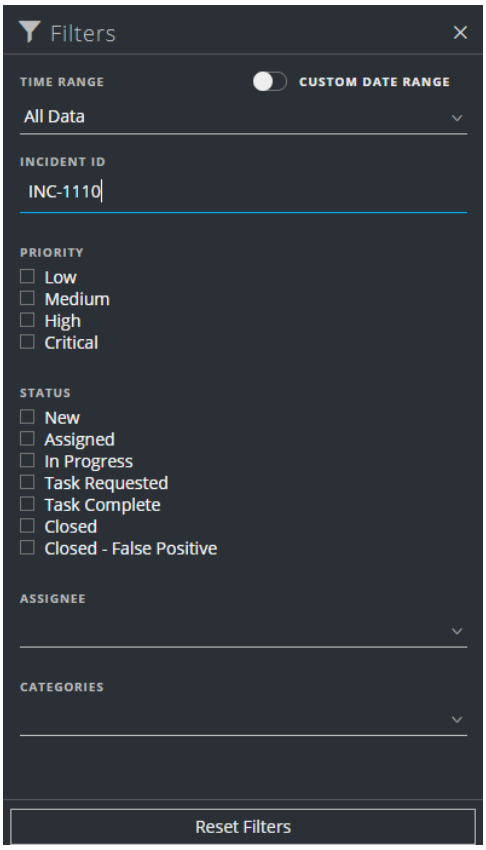
Vous pouvez afficher vos incidents en filtrant les incidents par votre nom d'utilisateur.

1. Si vous ne voyez pas le panneau Filtrer, dans la barre d'outils de la vue Liste des incidents, cliquez sur .
2. Dans le panneau Filtre, sous PERSONNE AFFECTÉE, sélectionnez votre nom d'utilisateur dans la liste déroulante.
   La liste d'incidents présente les incidents qui vous sont attribués.

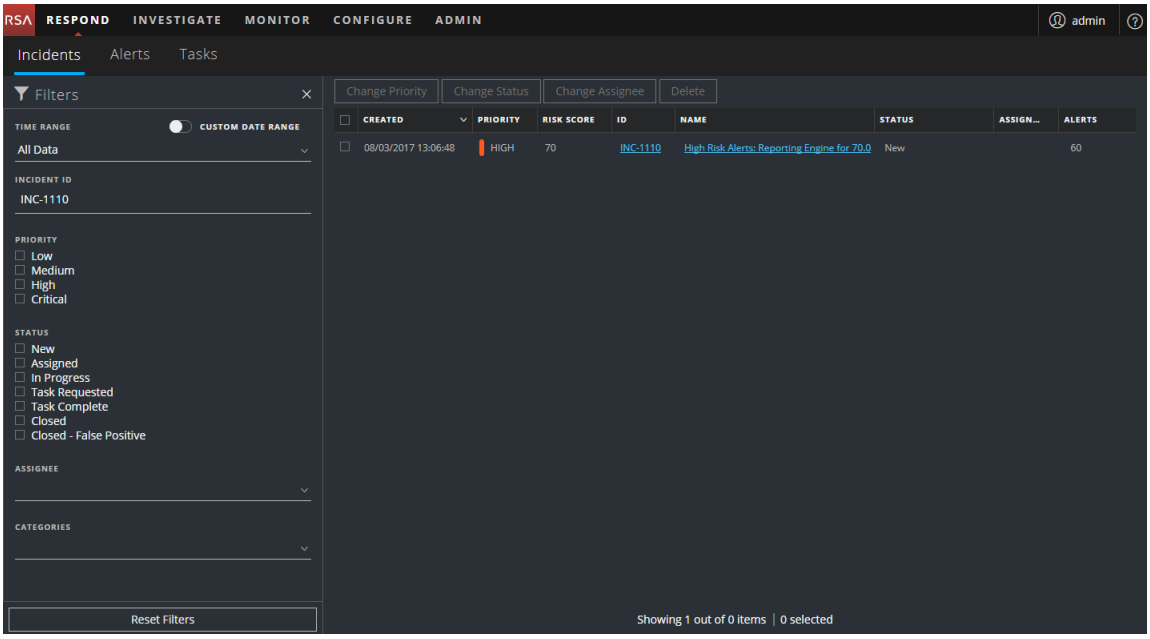
Trouver un incident

Si vous connaissez l'ID de l'incident, vous pouvez localiser rapidement un incident à l'aide du filtre. Par exemple, vous pouvez localiser un incident spécifique parmi des milliers de tâches.

1. Accédez à **RÉPONDRE > Incidents**.
   .Le panneau Filtres apparaît à gauche de la liste des incidents. Si vous ne voyez pas le panneau Filtres, dans la barre d'outils de la vue Liste des incidents, cliquez sur afin d'ouvrir le panneau Filtres.

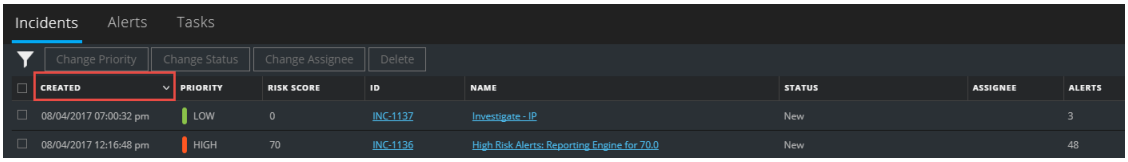


2. Dans le champ ID D'INCIDENT, saisissez l'ID D'INCIDENT pour un incident que vous souhaitez localiser, par exemple INC-1110.
   L'incident spécifié s'affiche dans la liste de vos incidents. Si vous ne voyez pas les résultats, essayez de réinitialiser vos filtres.



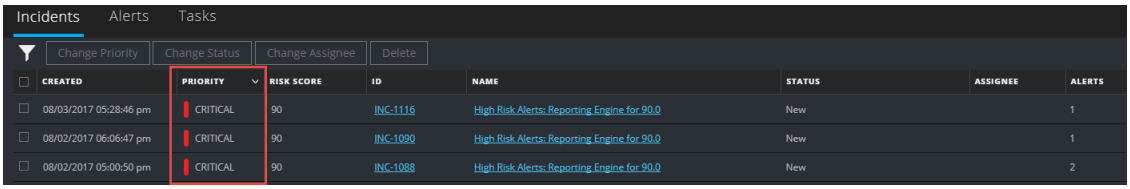
Trier la liste des incidents

Le tri par défaut de la liste des incidents se fait par Date de création, dans l'ordre décroissant (les plus récents en haut).

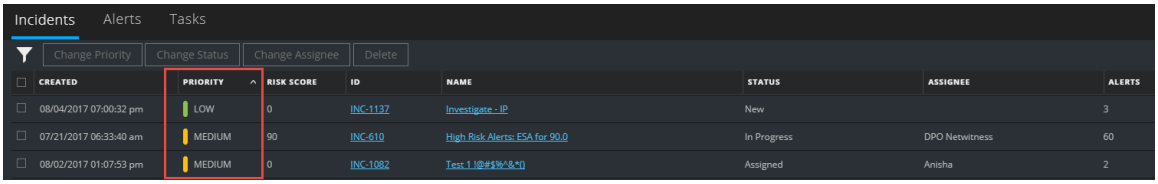


Vous pouvez modifier l'ordre de tri de la liste d'incidents en cliquant sur une colonne dans la liste.

Par exemple, pour définir la priorité des incidents, vous pouvez trier l'affichage dans la colonne Priorité. Pour ce faire, passez le pointeur sur la colonne Priorité, puis cliquez sur la flèche vers le bas . La liste des incidents est triée par priorité décroissante (priorité la plus élevée en haut), comme illustré sur la figure suivante.



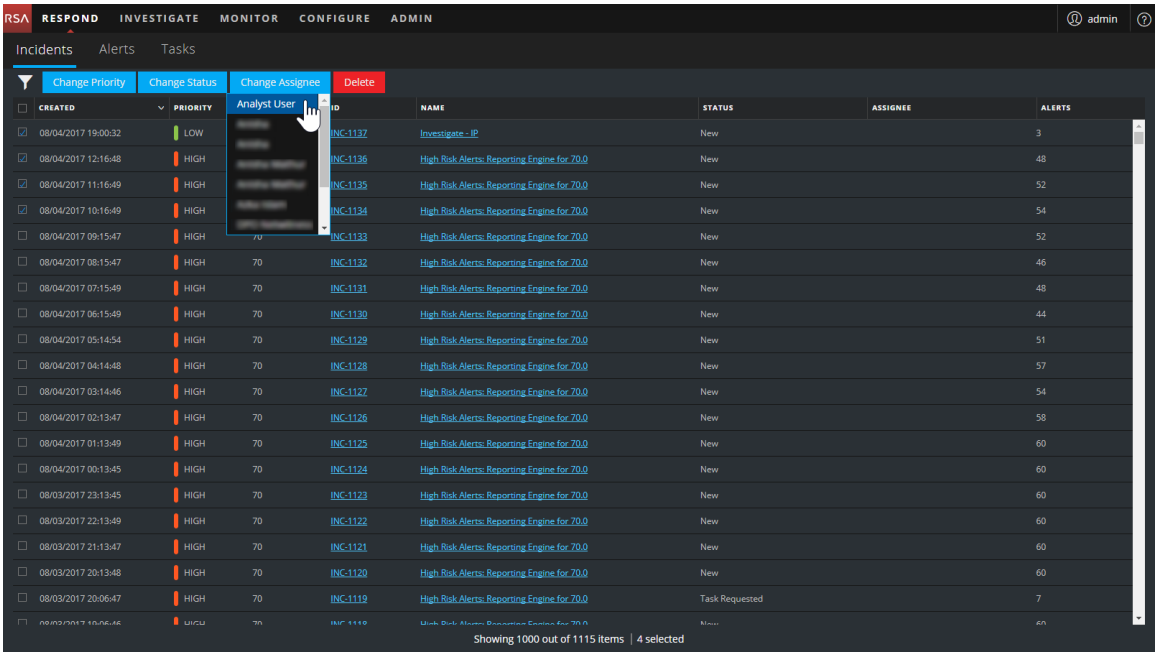
Pour trier par priorité croissante (priorité la plus faible en haut), cliquez sur la flèche vers le haut comme le montre la figure suivante.



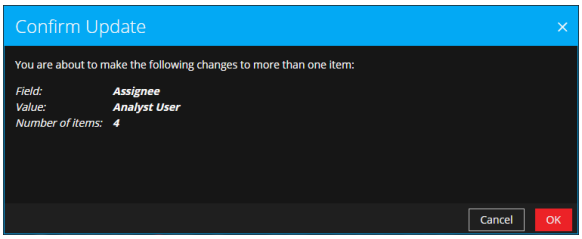
Attribuer les incidents à moi-même

1. Dans la vue Liste des incidents, sélectionnez un ou plusieurs incidents qui vous voulez attribuer à vous-même.

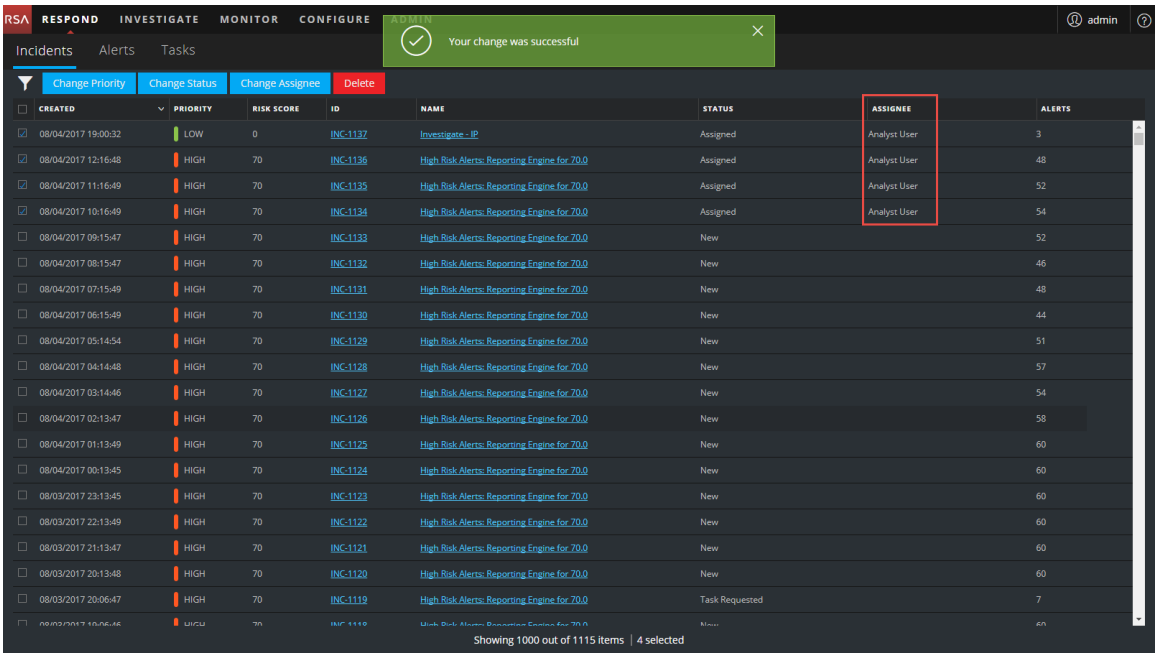
2. Cliquez sur **Modifier la personne affectée** et sélectionnez un utilisateur dans la liste déroulante.



3. Si vous sélectionnez plus d'un incident, dans la boîte de dialogue **Confirmer la mise à jour**, cliquez sur OK.

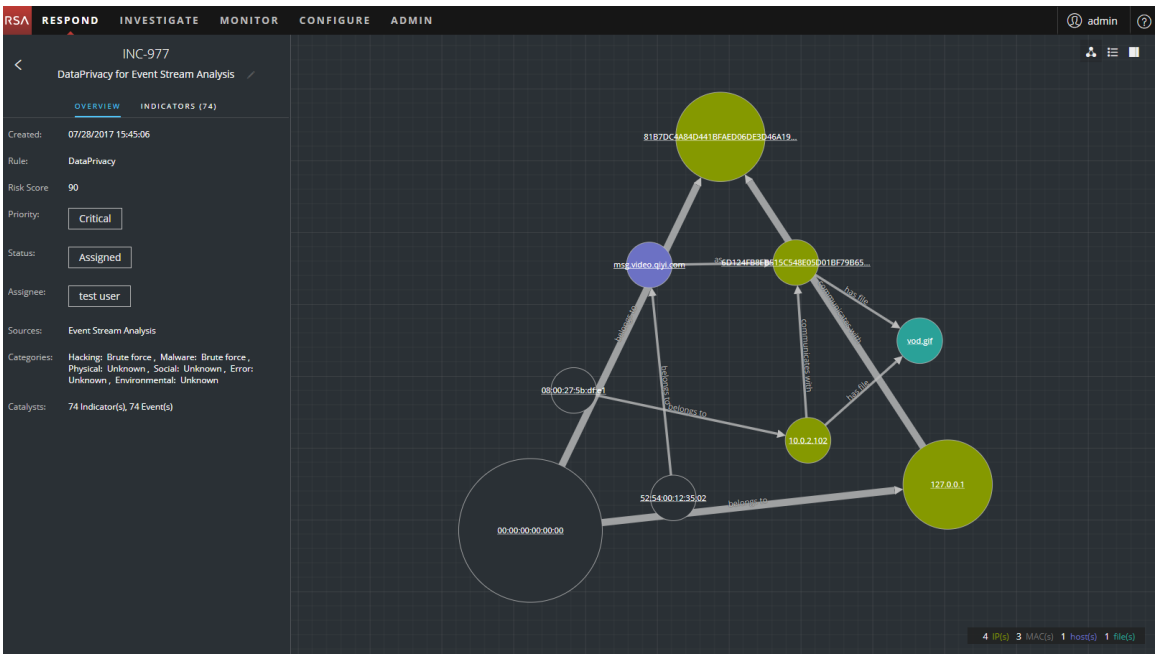


Vous verrez une notification de modification réussie.



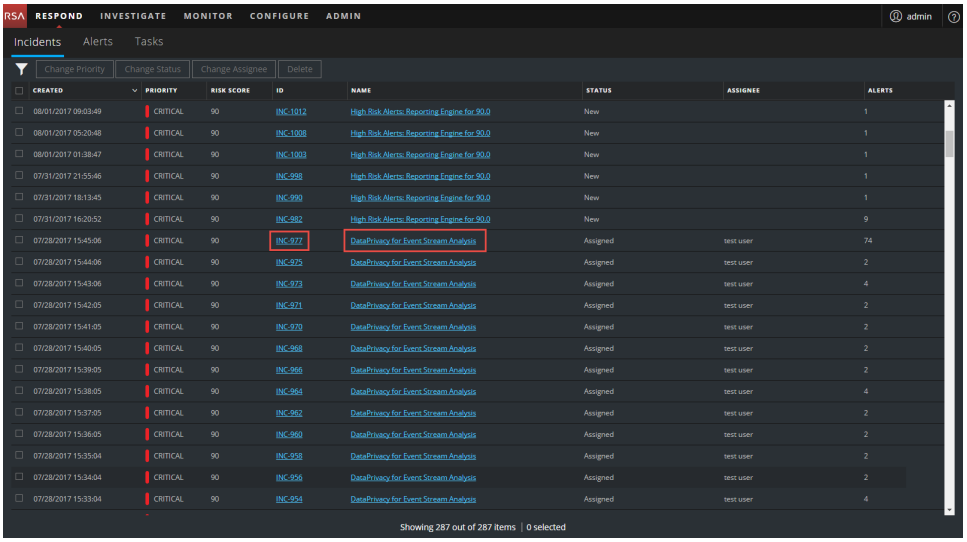
Déterminer les incidents exigeant une action

Une fois que vous avez obtenu des informations générales sur l'incident dans la vue Liste des incidents, vous pouvez accéder à la vue Détails de l'incident pour plus d'informations afin de déterminer l'action requise.

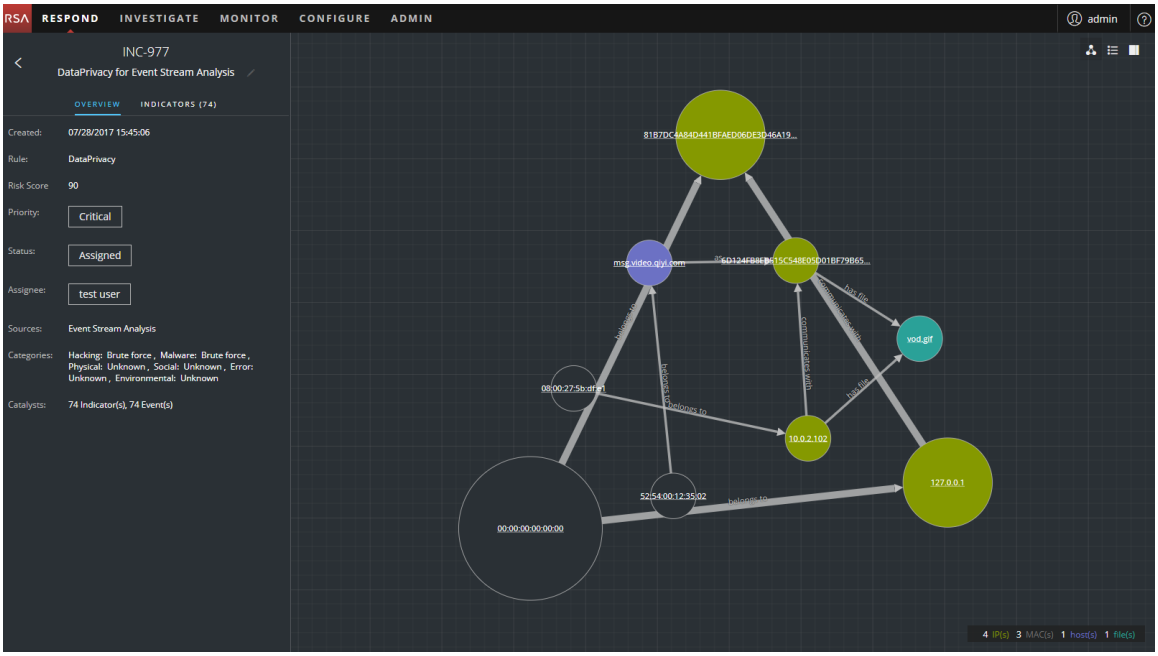


Afficher les détails sur l'incident

Pour afficher les détails d'un incident, dans la vue Liste des incidents, choisissez un incident à afficher et cliquez sur le lien dans la colonne ID ou NOM de cet incident.



La vue Détails de l'incident pour l'incident sélectionné s'affiche avec le panneau Présentation et le Graphique de nœud.

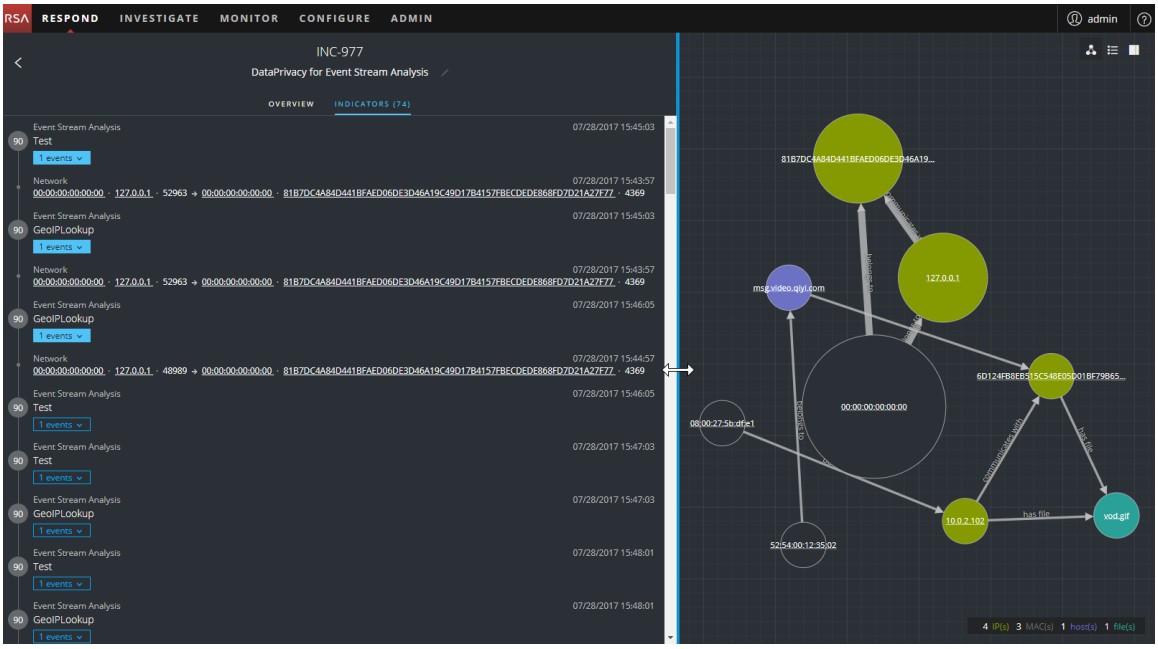


La vue Détails de l'incident inclut les panneaux suivants :

- **PRÉSENTATION** : Le panneau Présentation de l'incident contient des informations de synthèse générales sur l'incident, telles que la note, la priorité, les alertes et l'état. Vous avez la possibilité de modifier la priorité, l'état et la personne affectée pour l'incident.
- **INDICATEURS** : Le panneau Indicateurs contient une liste chronologique des indicateurs. ***Les indicateurs*** sont des alertes, comme une alerte ESA ou une alerte NetWitness Endpoint. Cette liste vous aide à connecter les indicateurs et les données importantes. Par exemple, une adresse IP est connectée à une commande, et une alerte ESA de communication peut également avoir déclenché une alerte NetWitness Endpoint ou d'autres activités suspectes.
- **Graphique de nœud** : Le graphique de nœud est un graphique interactif qui illustre les relations entre les entités impliquées dans l'incident. Une *entité* est un composant spécifié de méta, comme l'adresse IP, l'adresse MAC, l'utilisateur, l'hôte, le domaine, le nom de fichier ou le hachage de fichier.
- **Événements** : Le panneau Événements, également connu sous le nom de Tableau des événements, répertorie les événements associés à l'incident. Il indique également les informations de source et de destination de l'événement, ainsi que des informations supplémentaires en fonction du type d'événement. Vous pouvez cliquer sur un événement dans la liste pour afficher les données détaillées pour cet événement.

- **JOURNAL** : Le panneau Journal permet d'accéder au Journal de l'incident sélectionné, ce qui vous permet de communiquer et de collaborer avec d'autres analystes. Vous pouvez valider les notes dans un journal, ajouter des balises Étape Investigation (Reconnaissance, Remise, Exploitation, Installation, Commande et contrôle), et afficher l'historique de l'activité sur votre incident.
- **TÂCHES** : Le panneau Tâches affiche toutes les tâches qui ont été créées pour l'incident. Vous pouvez également créer des tâches supplémentaires à cet endroit.
- **ASSOCIÉ** : Le panneau Indicateurs associés vous permet d'effectuer une recherche dans la base de données des alertes NetWitness Suite pour trouver les alertes liées à cet incident. Vous pouvez également ajouter des alertes associées à l'incident.

Pour afficher plus d'informations dans le volet de gauche sans défilement, vous pouvez vous placez le pointeur sur le bord droit et faire glisser la ligne pour redimensionner le panneau, comme illustré dans la figure suivante :

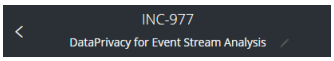


Afficher les informations récapitulatives de base sur l'incident

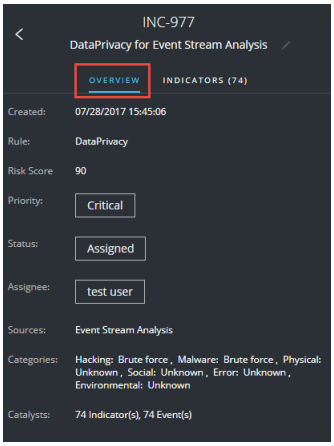
Vous pouvez afficher des informations récapitulatives de base relatives à un incident dans le panneau Présentation.

Au-dessus du Panneau de présentation, vous pouvez voir les informations suivantes :

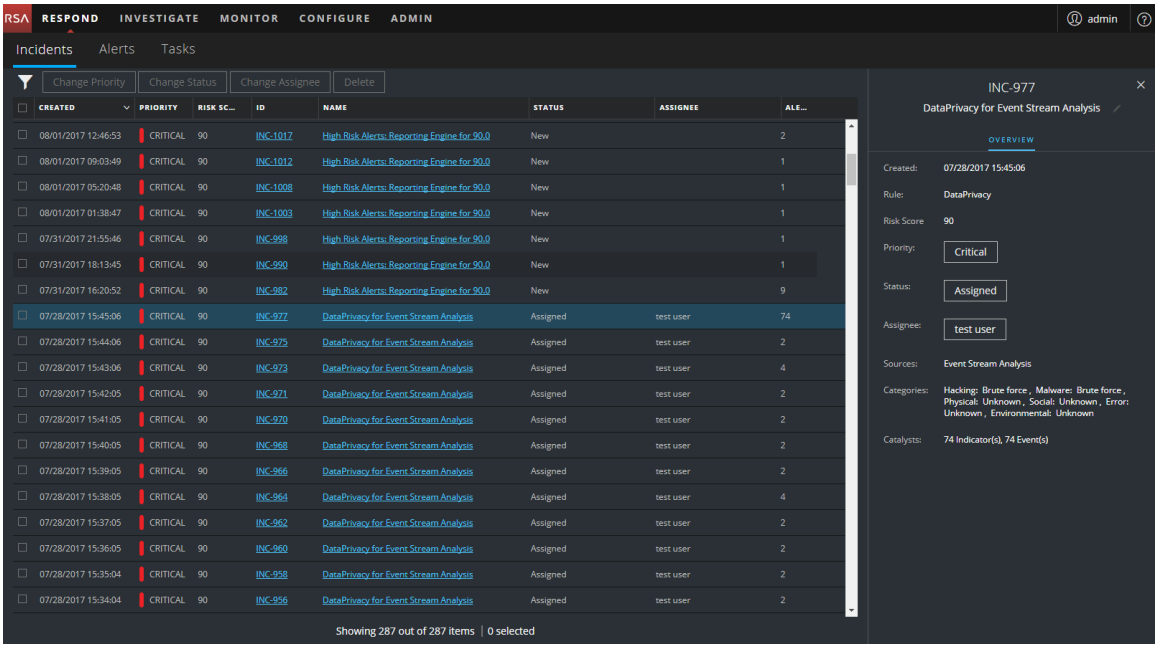
- **ID d'incident** : il s'agit d'un ID unique créé automatiquement et attribué à l'incident.
- **Nom** : le nom de l'incident est dérivé de la règle utilisée pour déclencher l'incident.



Pour afficher le volet Présentation à partir de la vue Détails de l'incident, sélectionnez **Présentation** dans le volet de gauche.



Pour afficher le panneau Présentation à partir de la vue Liste d'incidents, cliquez sur un incident dans la liste. Le panneau Présentation s'affiche sur la droite.



Le panneau Présentation contient des informations récapitulatives de base sur l'incident sélectionné :

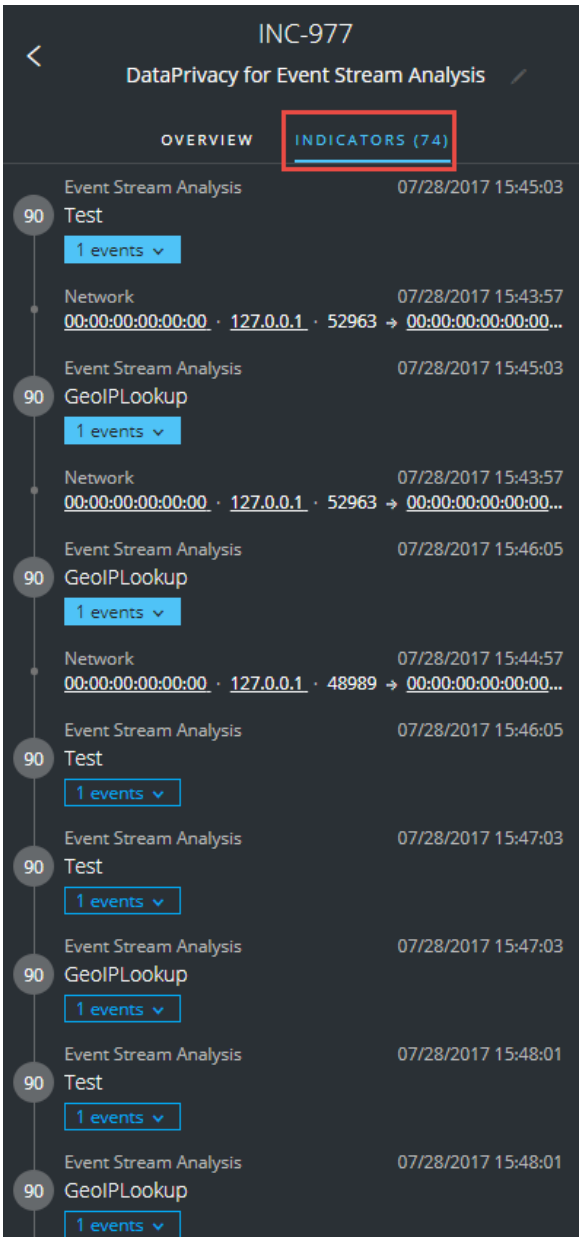
- **Créé** : affiche la date et l'heure de création de l'incident.
- **Règle / Par** : Affiche le nom de la règle qui a créé l'incident ou le nom de la personne qui a créé l'incident.
- **Valeur de risque** : indique le risque de l'incident, calculé via un algorithme et compris entre 0 et 100. 100 est le score de risque le plus élevé.
- **Priority** : affiche la priorité de l'incident. La priorité peut être critique, élevée, moyenne ou faible.
- **État** : affiche l'état de l'incident. L'état peut être Nouveau, Attribué, En cours, Tâche demandée, Tâche terminée, Fermé et Fermé - Faux positif. Après avoir créé une tâche, l'état devient Tâche demandée.
- **Personne affectée**: affiche le membre de l'équipe actuellement attribué à l'incident.
- **Sources** : indique les sources de données utilisées pour localiser l'activité suspecte.
- **Catégories** : affiche les catégories des événements d'incident.
- **Catalysts** : affiche le nombre d'indicateurs qui a donné lieu à l'incident.

Afficher les indicateurs et les enrichissements

Remarque : *les indicateurs* sont des alertes, comme une alerte ESA ou une alerte NetWitness Endpoint.

Vous trouverez les indicateurs, les événements et les enrichissements dans le panneau Indicateurs. Le panneau Indicateurs est une liste chronologique d'indicateurs qui vous aide à trouver des enrichissements et des événements liés à l'indicateur de déclenchement. Par exemple, un indicateur peut être une alerte de commande et contrôle, une alerte NetWitness Endpoint, une alerte de domaines suspects (C2) ou une alerte à partir d'une règle Event Stream Analysis (ESA). Le panneau Indicateurs vous aide à agréger et organiser ces indicateurs à partir de différents systèmes afin que vous puissiez voir comment elles sont associées et vous aident à développer une chronologie d'une attaque donnée.

Pour afficher le panneau Indicateurs, dans le volet gauche de la vue Détails de l'incident, sélectionnez **INDICATEURS**.



Les indicateurs sont des alertes, comme une alerte ESA ou une alerte NetWitness Endpoint. Cette liste vous aide à connecter les indicateurs et les données importantes. Par exemple, des indicateurs peuvent affichent les données trouvées par vos règles. Dans le panneau Indicateurs, la valeur de risque d'un indicateur s'affiche dans un cercle de couleur unie.

Les informations de sources de données sont présentées sous les noms des indicateurs. Vous pouvez également voir la date de création et l'heure de l'indicateur, ainsi que le nombre d'événements dans l'indicateur. Lorsque des données sont disponibles, vous pouvez voir le nombre d'enrichissements. Vous pouvez cliquer sur les boutons d'événement et d'enrichissement pour afficher les détails.

Afficher et étudier les événements

Vous pouvez afficher et étudier les événements associés à l'incident dans le panneau Événements. Il présente des informations sur les événements, comme l'heure de l'événement, l'adresse IP source, l'adresse IP de destination, l'adresse IP du détecteur, l'utilisateur source, l'utilisateur de destination et les informations de fichier sur les événements. La quantité d'informations répertoriées varie selon le type d'événement.

Il existe deux types d'événements :

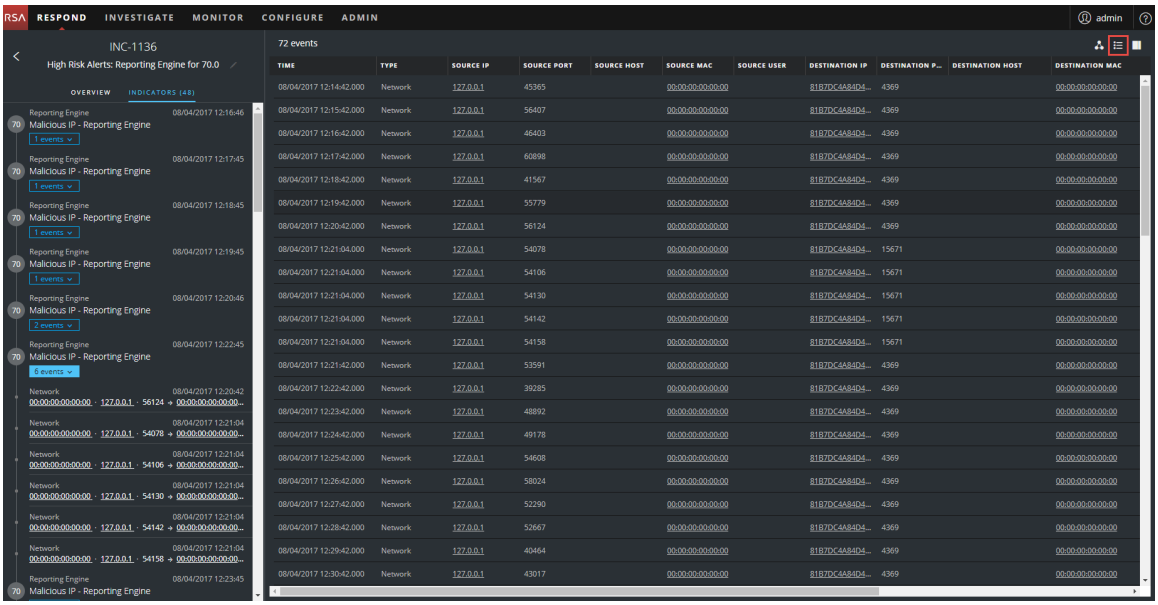
- Une transaction entre deux machines (une source et une destination)
- Une anomalie détectée sur une seule machine (un détecteur)

Certains événements ne disposent que d'un détecteur. Par exemple, NetWitness Endpoint détecte des malware sur votre machine. D'autres événements posséderont une source et une destination. Par exemple, les données de paquets affichent une communication entre votre ordinateur et une commande et le domaine de contrôle (C2).

Vous pouvez effectuer une recherche verticale dans un événement pour obtenir des données détaillées à son sujet.

Pour afficher et étudier les événements :

1. Pour afficher le panneau Événements, dans la barre d'outils de la vue Détails de l'incident, cliquez sur .



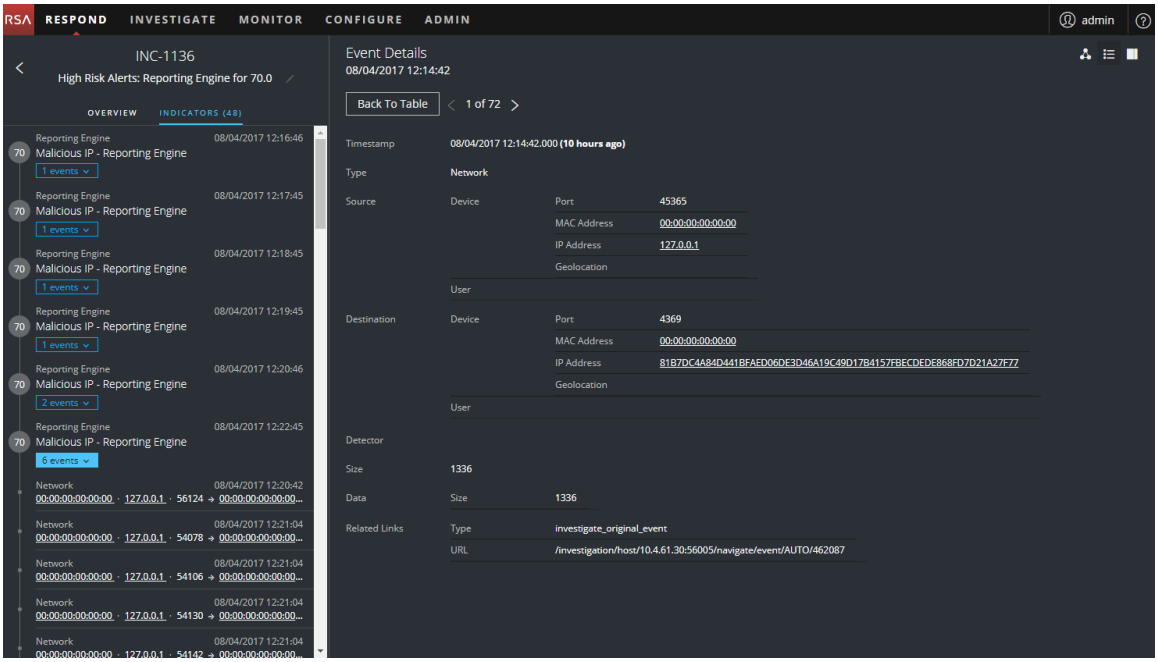
Le panneau Événements présente la liste des informations sur chaque événement, comme indiqué dans le tableau suivant.

Colonne	Description
TEMPS	Affiche l'heure à laquelle l'événement s'est produit.
TYPE	Affiche le type d'alerte, comme Log et Réseau.
IP SOURCE	Affiche l'adresse IP source s'il y a eu une transaction entre les deux machines.
PORT SOURCE	Indique le port de la source de la transaction. Les ports source et de destination peuvent être sur la même adresse IP.
HÔTE SOURCE	Affiche l'hôte source dans lequel l'événement a eu lieu.
MAC SOURCE	Affiche l'adresse MAC de la machine source.
UTILISATEUR SOURCE	Affiche l'utilisateur de la machine source.

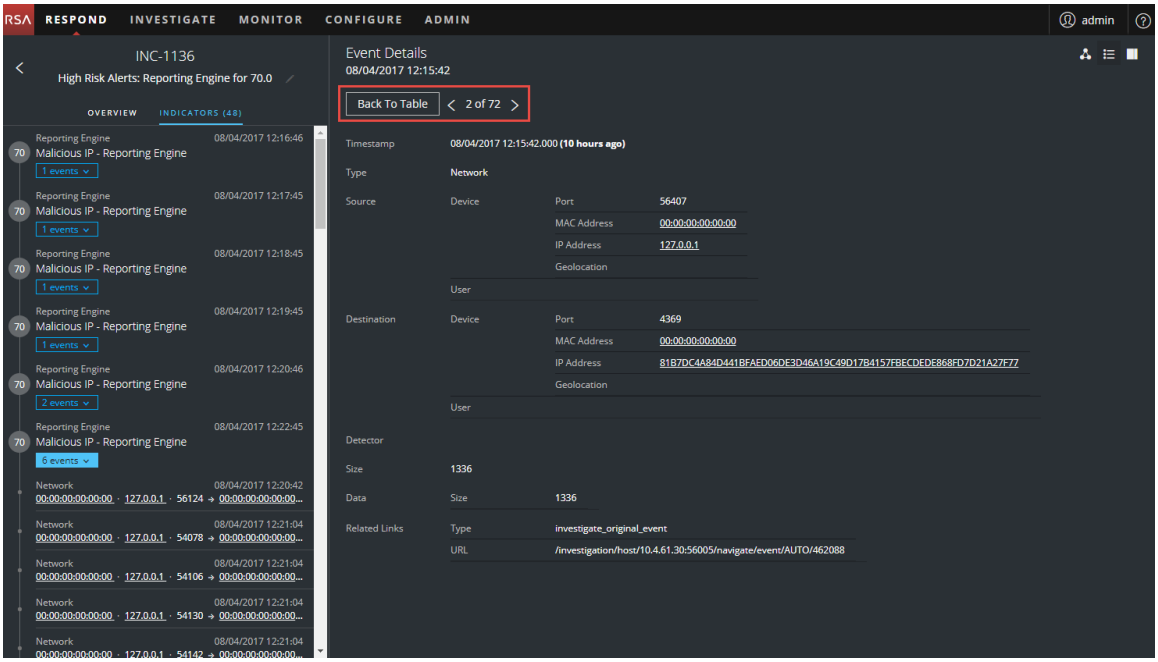
Colonne	Description
IP de destination	Affiche l'adresse IP de destination s'il y a eu une transaction entre les deux machines.
Port de destination	Indique le port de la destination de la transaction. Les ports source et de destination peuvent être sur la même adresse IP.
HÔTE DE DESTINATION	Affiche l'hôte de destination dans lequel l'événement a eu lieu.
ADRESSE MAC DE DESTINATION	Affiche l'adresse MAC de la machine de destination.
UTILISATEUR DE DESTINATION	Affiche l'utilisateur de la machine de destination.
IP DÉTECTEUR	Affiche l'adresse IP de la machine dans laquelle une anomalie a été détectée.
NOM DE FICHIER	Affiche le nom du fichier si un fichier est impliqué dans l'événement.
HACHAGE DE FICHIER	Présente un hachage du contenu du fichier.

S'il existe un seul événement dans la liste, vous verrez les détails de l'événement pour cet événement au lieu d'une liste.

2. Cliquez sur un événement dans la liste Événements pour afficher les détails Événement.
   Cet exemple montre les détails de l'événement pour le premier événement dans la liste.



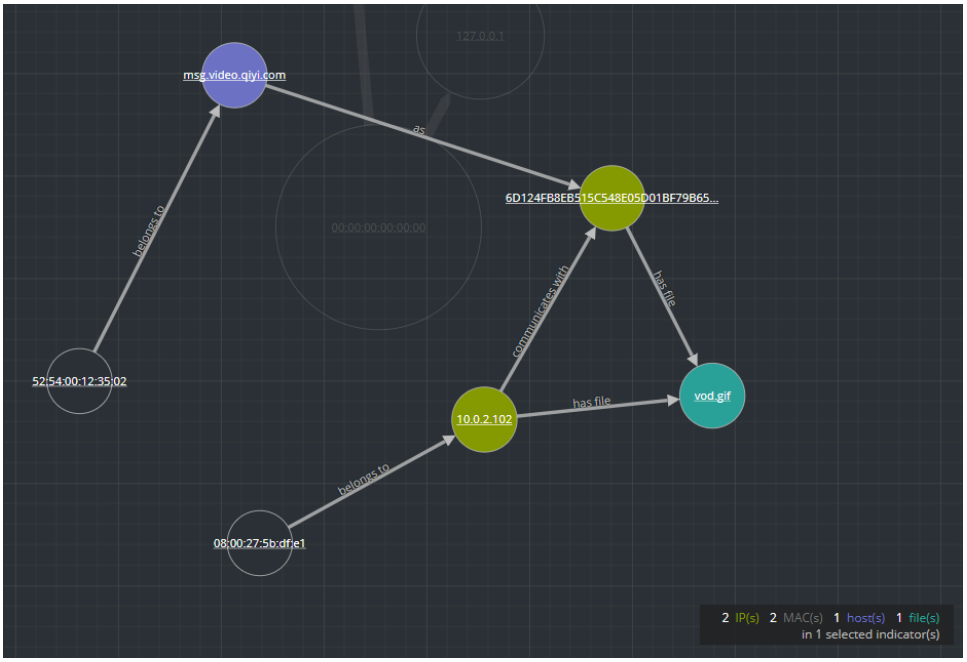
3. Utilisez la barre de Détails de navigation pour afficher les détails pour d'autres événements.
   Cet exemple montre le deuxième événement dans la liste.



Afficher et étudier les entités impliquées dans les événements

Une *entité* peut être une adresse IP, une adresse MAC, un utilisateur, un hôte, un domaine, un nom de fichier ou un hachage de fichier. Le graphique de nœud est un graphique interactif que vous pouvez déplacer pour mieux comprendre la façon dont les entités impliquées dans les événements sont reliées entre elles. Les graphiques de nœud ont un aspect différent selon le type d'événement, le nombre de machines impliquées, selon que les machines sont associées à des utilisateurs, et selon qu'il existe des fichiers associés à l'événement.

La figure suivante illustre un exemple de graphique de nœud avec six nœuds.



Si vous examinez attentivement le graphique de nœud, vous pouvez voir les cercles qui représentent des nœuds. Un graphique de nœud peut contenir un ou plusieurs des types de nœuds suivants :

- **Adresse IP** (si l'événement est une anomalie détectée, vous voyez une adresse IP du détecteur. Si l'événement est une transaction, vous voyez une adresse IP de destination et une adresse IP source.)
- **Adresse MAC** (vous pouvez voir une adresse MAC pour chaque type d'adresse IP).
- **Utilisateur** (si la machine est associée à un utilisateur, vous voyez un nœud d'utilisateur.)
- **Hôte**
- **Domaine**

- **Nom de fichier** (si l'événement implique des fichiers, vous pouvez voir un nom de fichier.)
- **Hachage de fichier** (si l'événement implique des fichiers, vous voyez un hachage de fichier.)

La légende en bas du graphique de nœud indique le nombre de nœuds de chaque type et le code couleur des nœuds.

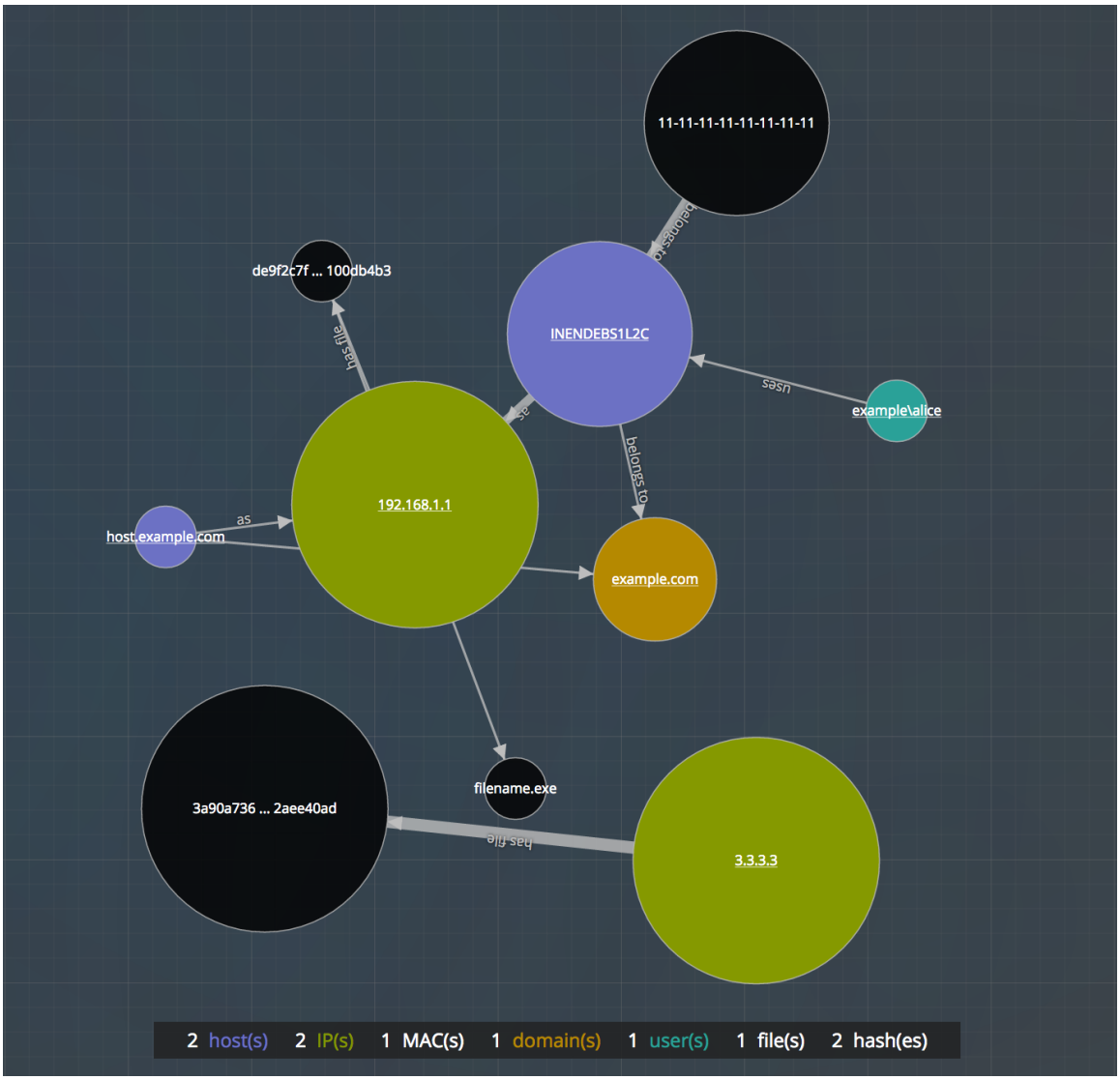
Vous pouvez cliquer sur n'importe quel nœud et le faire glisser pour le repositionner.

Les flèches entre les nœuds fournissent des informations supplémentaires sur les relations d'entité :

- **Communique avec** : une flèche entre un nœud de machine source (adresse IP ou adresse MAC) et un nœud de machine de destination nommé « communique avec » indique la direction de la communication.
- **En tant que** : une flèche entre les nœuds nommée « en tant que » fournit des informations complémentaires sur l'adresse IP vers laquelle la flèche pointe. Dans l'exemple ci-dessus, une flèche à partir du cercle du nœud hôte pointe vers un nœud de l'adresse IP hachée nommé « en tant que ». Cela indique que le nom sur le cercle de nœud d'hôte est le nom d'hôte de l'adresse IP et qu'il n'est pas une autre entité.
- **Contient le fichier** : une flèche entre un nœud de machine (adresse IP, adresse MAC ou hôte) et un nœud de hachage de fichier identifié par « contient » indique que l'adresse IP contient ce fichier.
- **Utilise** : une flèche entre un nœud d'utilisateur et un nœud de machine (adresse IP, adresse MAC ou hôte) nommée « utilise » indique la machine que l'utilisateur utilisait lors de l'événement.
- **Est nommé** : une flèche à partir d'un nœud de hachage de fichier vers un nœud de nom de fichier accompagné de « est nommé » indique que le hachage de fichier correspond à un fichier portant ce nom.
- **Appartient à** : une flèche entre deux nœuds identifiée par « appartient à » indique qu'ils appartiennent au même nœud. Par exemple, une flèche entre une adresse MAC et un hôte nommé « appartient à » indique qu'il s'agit de l'adresse MAC de l'hôte.

Des flèches avec une ligne de taille supérieure représentent plus de communication entre les nœuds. Des nœuds plus grands (cercles) indiquent davantage d'activité que les nœuds plus petits. Les nœuds de plus grande taille sont les entités les plus courantes mentionnées dans les événements.

L'exemple de graphique de nœud suivant contient dix nœuds.

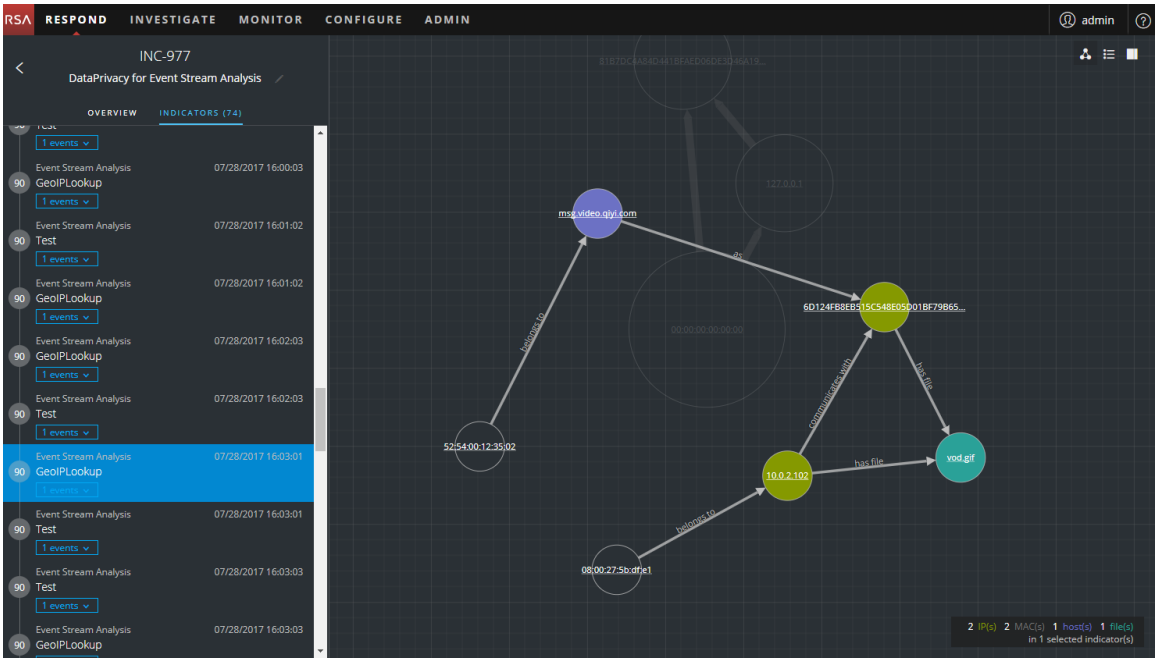


Dans cet exemple, notez que deux nœuds IP présentent une forte activité. Ils contiennent tous deux des fichiers, mais ne communiquent pas entre eux. L'adresse IP dans la partie supérieure (192.168.1.1) correspond à une machine avec deux noms d'hôte (hote.example.com et INENDEBS1L2C) dans le domaine example.com. L'adresse MAC de la machine est 11-11-11-11-11-11-11-11 et Alice l'utilise.

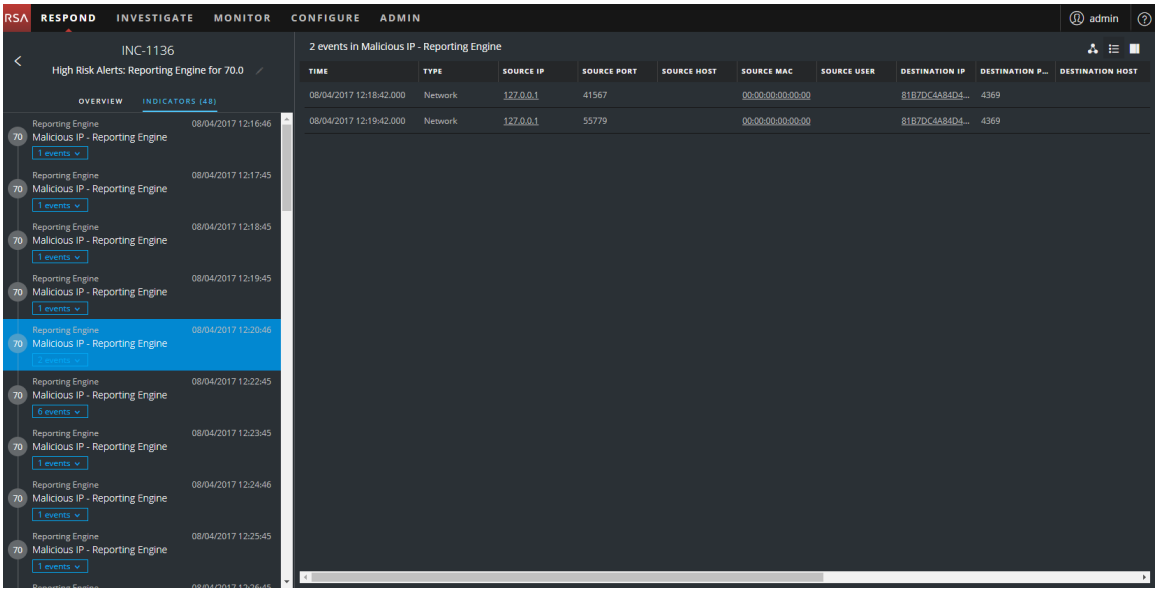
Filtrer les données dans la vue Détails de l'incident

Vous pouvez cliquer sur les indicateurs dans le panneau Indicateurs pour filtrer ce que vous pouvez voir dans le graphique de nœud et la Liste des événements.

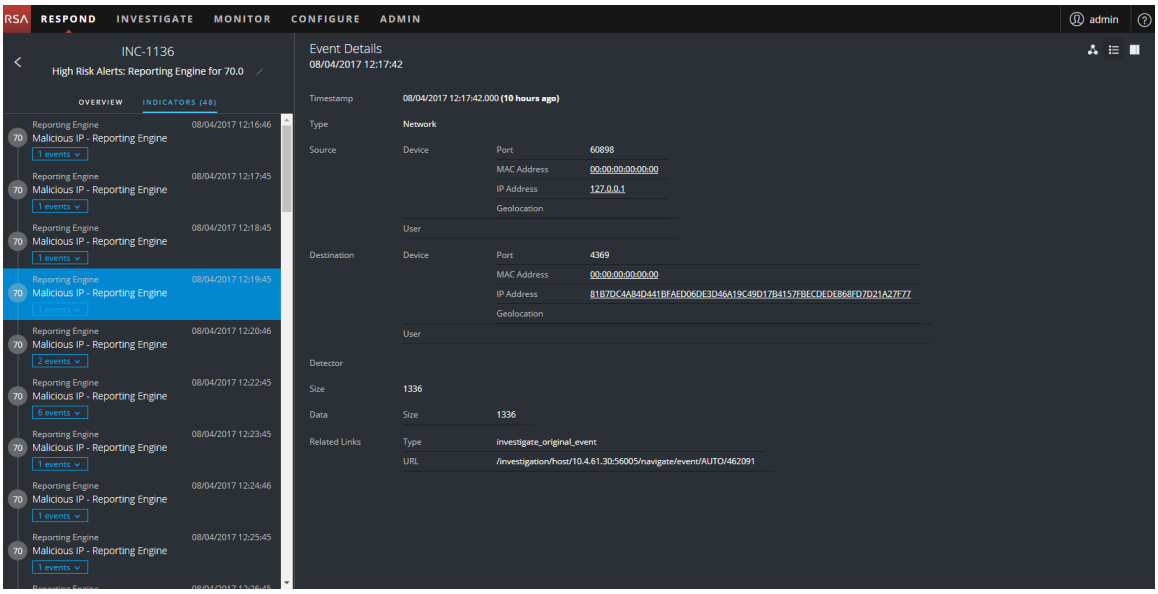
Si vous sélectionnez un indicateur pour filtrer le graphique de nœud, les données qui ne font pas partie de votre sélection sont grisées, mais elles restent toujours dans la vue comme indiqué dans la figure suivante.



Si vous sélectionnez un indicateur pour filtrer la liste des événements, seuls les événements de cet indicateur sont affichés dans la liste. La figure suivante montre un indicateur sélectionné qui contient deux événements. La Liste des événements filtrée présente ces deux événements.



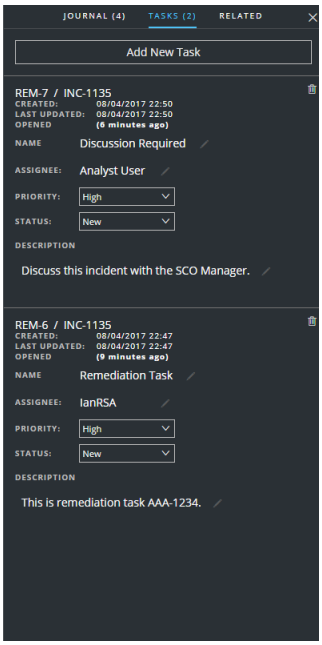
Si vous sélectionnez un indicateur pour filtrer la liste des événements et qu'il n'existe qu'un seul événement pour cet indicateur, vous pouvez voir les détails de l'événement pour cet événement, comme illustré dans la figure suivante.


RSA
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
INC-1136
High Risk Alerts: Reporting Engine for 70.0
OVERVIEW
INDICATORS (48)
Reporting Engine
Malicious IP - Reporting Engine
08/04/2017 12:16:46
1 events
08/04/2017 12:17:45
08/04/2017 12:18:45
08/04/2017 12:19:45
08/04/2017 12:20:46
2 events
08/04/2017 12:22:45
6 events
08/04/2017 12:23:45
08/04/2017 12:24:46
08/04/2017 12:25:45
Event Details
08/04/2017 12:17:42
Timestamp
08/04/2017 12:17:42.000 (10 hours ago)
Type
Network
Source
Device
Port
60898
MAC Address
00:00:00:00:00:00
IP Address
127.0.0.1
Geolocation
User
Destination
Device
Port
4369
MAC Address
00:00:00:00:00:00
IP Address
81B7DC4A84D441BFAED06DE3D46A19C49D17B4157FBECDEDE868FD7D21A27F77
Geolocation
User
Detector
Size
1336
Data
Size
1336
Related Links
Type
investigate_original_event
URL
/investigation/host/10.4.61.30:56005/navigate/event/AUTO/462091

Afficher les tâches associées à un incident

Les intervenants de menaces et d'autres analystes peuvent créer des tâches pour un incident et suivre ces tâches jusqu'à l'achèvement. Cela peut être très utile, par exemple, lorsque vous avez besoin d'actions sur les incidents de la part d'équipes en dehors de vos opérations de sécurité. Vous pouvez afficher les tâches associées à un incident dans la vue Détails de l'incident.

1. Accédez à **RÉPONDRE > Incidents** et recherchez l'incident que vous souhaitez afficher dans la Liste des incidents.
2. Cliquez sur le lien dans le champ **ID** ou **NOM** de l'incident pour accéder à la vue Détails de l'incident.
3. Dans la barre d'outils de la vue Détails de l'incident, cliquez sur ▣.
   Le panneau Journal s'ouvre.
4. Cliquez sur l'onglet **TÂCHES**.
   Le panneau Tâches affiche toutes les tâches pour l'incident.

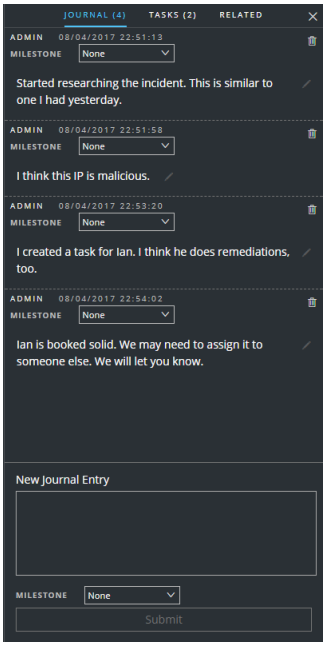


Pour plus d'informations sur les tâches, reportez-vous à la section Vue Liste des tâches, Afficher toutes les tâches d'incident et Créer une tâche.

Afficher les notes sur l'incident

Le Journal des incidents vous permet d'afficher l'historique d'activité sur votre incident. Vous pouvez afficher les entrées de journal d'autres analystes et communiquer et collaborer avec eux.

1. Accédez à **RÉPONDRE > Incidents** et recherchez l'incident que vous souhaitez afficher dans la Liste des incidents.
2. Cliquez sur le lien dans le champ **ID** ou **NOM** de l'incident pour accéder à la vue Détails de l'incident.
3. Dans la barre d'outils de la vue Détails de l'incident, cliquez sur .
   Le panneau Journal affiche tous les entrées de journal de l'incident.



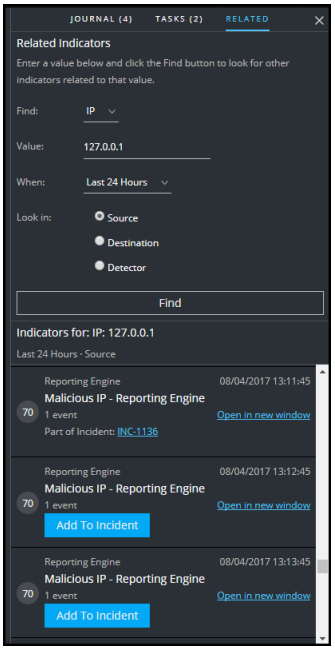
Rechercher des indicateurs associés

Les Indicateurs associés sont des alertes qui ne faisaient pas partie de l'incident sélectionné à l'origine, mais qui sont associés à l'incident. La relation peut être évidente ou non. Par exemple, les indicateurs associés peuvent impliquer une ou plusieurs entités de l'incident, mais ils peuvent également être associés en raison de certains renseignements en dehors de NetWitness Suite.

Dans le panneau Associé de la vue Détails de l'incident, vous pouvez rechercher une entité (par exemple, IP, MAC, Hôte, Domaine, Utilisateur, Nom de fichier ou Hachage) dans les autres alertes en dehors de l'incident actuel.

1. Accédez à **RÉPONDRE > Incidents** et recherchez l'incident que vous souhaitez afficher dans la Liste des incidents.
2. Cliquez sur le lien dans le champ **ID** ou **NOM** de l'incident pour accéder à la vue Détails de l'incident.
3. Dans la barre d'outils de la vue Détails de l'incident, cliquez sur .
   Le panneau Journal s'ouvre sur la droite.

4. Cliquez sur l'onglet **ASSOCIÉS**.



5. Dans le panneau **Indicateurs associés**, saisissez vos critères de recherche :

   - **Rechercher** : sélectionnez l'entité que vous souhaitez trouver dans les alertes. Par exemple, IP.
   - **Valeur** : saisissez la valeur de l'entité. Par exemple, saisissez l'adresse IP réelle de l'entité.
   - **Quand** : sélectionnez une plage de temps pour rechercher les alertes. Par exemple, Dernières 24 heures.
   - **Rechercher dans** : Spécifiez le type de l'entité à rechercher :
     Source - La machine source dans une transaction entre deux machines.
     Destination - La machine de destination dans une transaction entre deux machines.
     Détecteur - Une machine unique dans laquelle une anomalie a été détectée.
     Domaine - Cette option est disponible lorsque vous sélectionnez Domaine dans le champ Rechercher.

     Par exemple, sélectionnez la Source pour rechercher des alertes où une adresse IP particulière est traitée en tant qu'appareil source. Vous pouvez effectuer des recherches séparées pour chaque type d'appareil : Source, Destination et Détecteur.

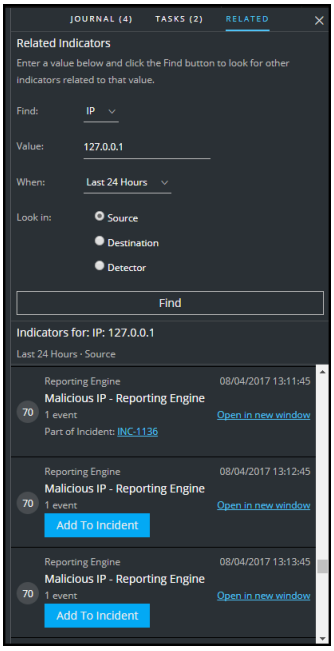
6. Cliquez sur **Rechercher**.
   Une liste des indicateurs associés (alertes) s'affiche sous le bouton **Rechercher** dans la section **Indicateurs pour**. Si une alerte ne fait pas partie d'un autre incident, vous pouvez

cliquer sur le bouton **Ajouter à l'incident** pour ajouter l'indicateur associé (alerte) à l'incident actuel. Reportez-vous à la section Ajouter des indicateurs associés à l'incident ci-dessous.

Ajouter des indicateurs associés à l'incident

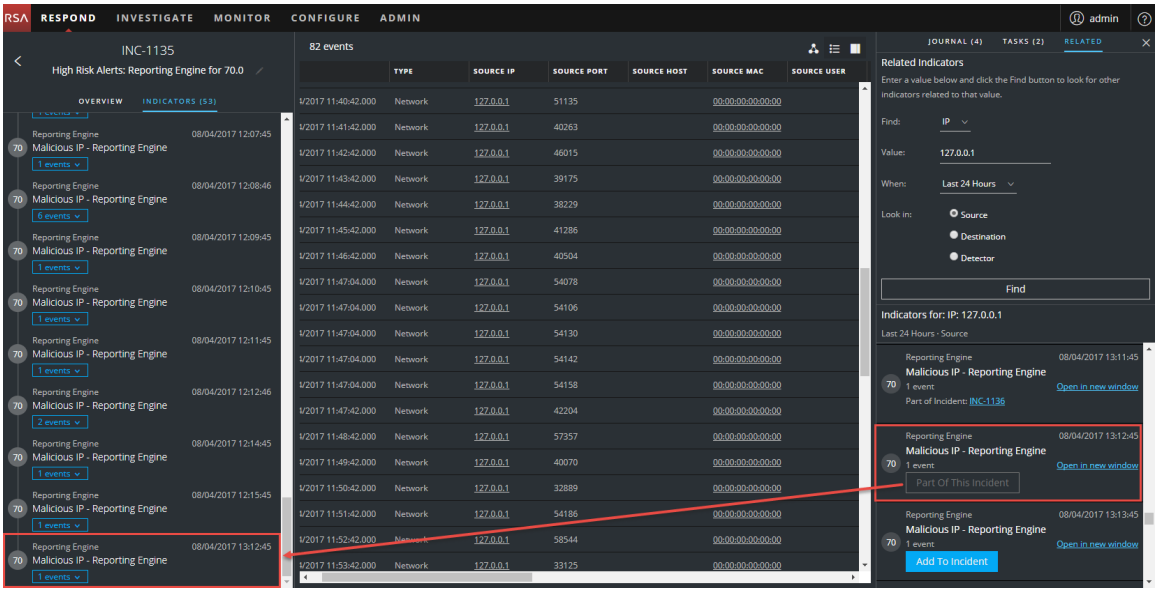
Vous pouvez ajouter des indicateurs associés (alertes) à l'incident actuel à partir du panneau Indicateurs associés. Un indicateur qui ne fait pas déjà partie d'un incident ne peut pas faire partie d'un autre incident. Dans les résultats de recherche, si une alerte ne fait pas déjà partie d'un incident, elle possède un bouton **Ajouter à l'incident**.

1. Dans le panneau **ASSOCIÉS** (Indicateurs associés), effectuez une recherche pour trouver les indicateurs associés. Reportez-vous à la section Rechercher des indicateurs associés ci-dessus.



2. Passez en revue les alertes dans les résultats de recherche. La section **Indicateurs pour** (sous le bouton Rechercher) affiche les indicateurs associés (alertes).
3. Pour examiner les détails d'une alerte avant de l'ajouter en tant qu'indicateur associé à l'incident, vous pouvez cliquer sur le lien **Ouvrir dans une nouvelle fenêtre** pour afficher les détails de l'alerte pour cet indicateur.
4. Pour chaque alerte que vous souhaitez ajouter à l'incident en tant qu'indicateur associé, cliquez sur le bouton **Ajouter à l'incident**.
   L'indicateur associé sélectionné s'ajoute dans le panneau Indicateurs sur la gauche. Le

bouton dans le panneau Indicateurs associés sur la droite affiche à présent **Partie de cet incident**.



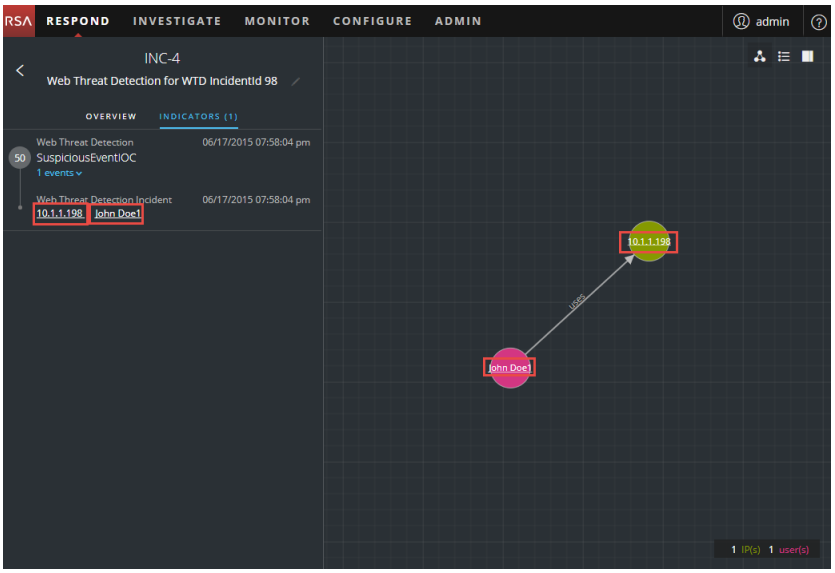
Enquêter sur l’incident

Pour enquêter davantage sur un incident dans la vue Détails de l’incident, vous trouverez des liens vers des informations contextuelles supplémentaires sur l’incident, si elles sont disponibles. Ce contexte supplémentaire peut vous aider à comprendre les contextes technique et métier supplémentaires sur une entité spécifique dans l’incident. Il peut également fournir des informations supplémentaires que vous pouvez étudier pour comprendre toute la portée de l’incident.

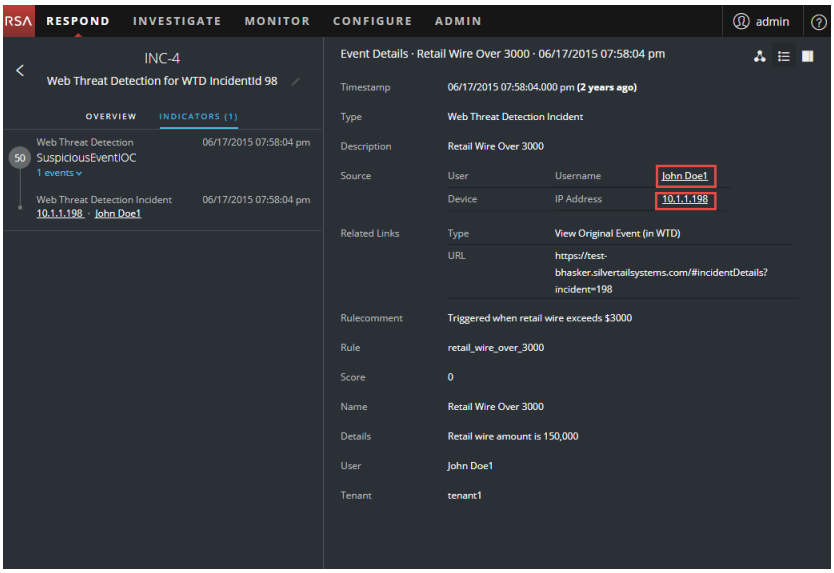
Afficher les informations contextuelles

Dans le panneau Indicateurs, panneau Liste d’événements, panneau Détails de l’événement ou Graphique de nœud, vous pouvez voir les entités soulignées. Si une entité est soulignée, NetWitness Suite renseigne les informations relatives à ce type d’entité dans le service Context Hub. Des informations supplémentaires relatives à cette entité peuvent être disponibles dans le service Context Hub.

La figure suivante illustre les entités soulignées dans le panneau Indicateurs et le Graphique de nœud.



La figure suivante illustre les entités soulignées dans le panneau Détails de l’événement.

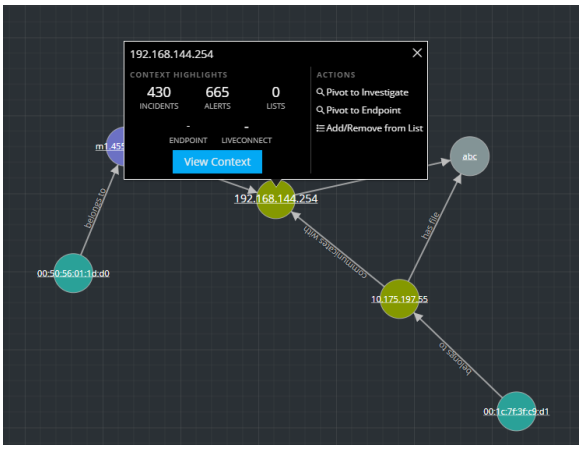


Le service Context Hub est préconfiguré avec les champs méta mappés aux entités. NetWitness Respond et Enquêter utilisent ces mappages par défaut pour la recherche contextuelle. Pour plus d'informations sur l'ajout de clés méta, consultez « Configurer les paramètres pour une source de données » dans le *Guide de configuration de Context Hub*.

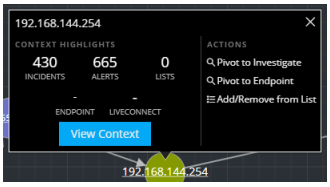
Attention : Pour que la recherche contextuelle fonctionne correctement dans les vues Répondre et Enquêter, RSA vous recommande, lorsque vous mappez des clés méta dans l'onglet **ADMIN > SYSTÈME > Procédures d'enquête > Recherche contextuelle**, d'ajouter uniquement les clés méta aux mappages de clé méta, et non aux champs dans MongoDB. Par exemple, ip.address est une clé méta et ip_address n'est pas une clé méta (il s'agit d'un champ dans MongoDB).

Pour afficher les informations contextuelles :

1. Dans le panneau Indicateurs, Liste d'événements, Détails de l'événement ou Graphique de nœud, survolez une entité soulignée.
   Une info-bulle contextuelle s'affiche avec un bref résumé du type de données contextuelles disponible pour l'entité sélectionnée.



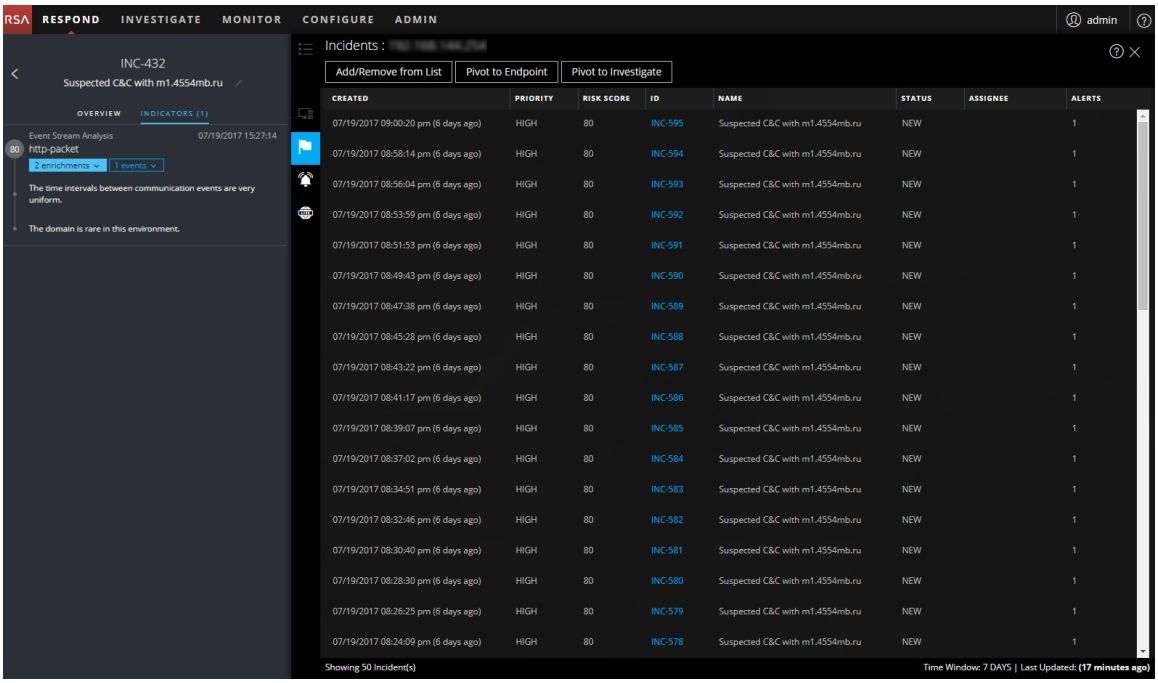
L’info-bulle contextuelle comporte deux sections : Points forts du contexte et actions.



Les informations contenues dans la section **Points forts du contexte** vous aident à déterminer les actions que vous devez entreprendre. Elles peuvent afficher des données connexes pour les Incidents, les Alertes, les Listes, le Point de terminaison et Live Connect. En fonction de vos données, vous pourrez peut-être cliquer sur ces éléments pour plus d’informations. L’exemple ci-dessus montre 430 incidents connexes, 665 alertes, 0 liste et aucune information dans NetWitness Endpoint ou Live Connect mentionnant l’entité de l’adresse IP, 192.168.144.254.

La section **Actions** répertorie les actions disponibles. Dans l’exemple ci-dessus, les options Pivoter vers la fonction Enquêter, Pivot vers le point de terminaison, et Ajouter à la liste/Supprimer de la liste sont disponibles. Pour plus d’informations, reportez-vous à la section Pivoter vers la fonction Enquêter, Pivoter vers le point de terminaison NetWitness et Ajouter une entité à une liste blanche.

2. Pour obtenir plus de détails sur l’entité sélectionnée, cliquez sur le bouton **Afficher le contexte**.
   Le panneau Recherche contextuelle s’ouvre et affiche toutes les informations relatives à l’entité.
   L’exemple suivant présente des informations contextuelles pour une adresse IP source sélectionnée. Elle répertorie tous les incidents qui mentionnent l’adresse IP.



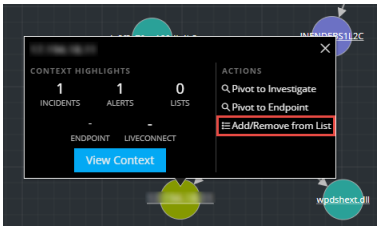
Pour comprendre les différentes vues dans le panneau Recherche Context Hub, reportez-vous à la section

Panneau Recherche contextuelle - Vue Répondre .

Ajouter une entité à une liste blanche

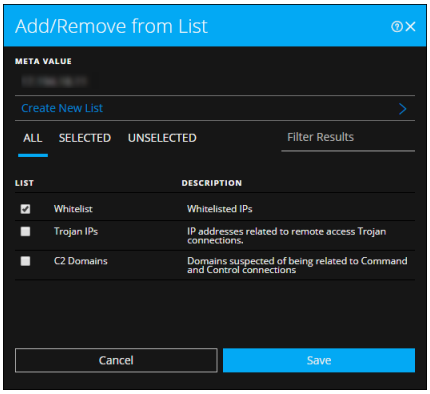
Vous pouvez ajouter n'importe quelle entité soulignée à une liste, comme une liste blanche ou noire, à partir d'une info-bulle de contexte. Par exemple, pour réduire les faux positifs, vous pouvez ajouter à la liste blanche un domaine souligné pour l'exclure des entités associées.

1. Dans le panneau Indicateurs, Liste d'événements, Détails de l'événement ou Graphique de nœud, survolez l'entité soulignée que vous souhaitez ajouter à une liste Context Hub.
   Une info-bulle contextuelle s'affiche et présente les actions disponibles.



2. Dans la section **ACTIONS** de l'info-bulle, cliquez sur **Ajouter à la liste/Supprimer de la liste**.

La boîte de dialogue Ajouter à la liste/Supprimer de la liste affiche les listes disponibles.



3. Sélectionnez une ou plusieurs listes, puis cliquez sur **Enregistrer**.
   L'entité s'affiche dans les listes sélectionnées.
   Boîte de dialogue Ajouter à la liste/Supprimer de la liste fournit des informations supplémentaires.

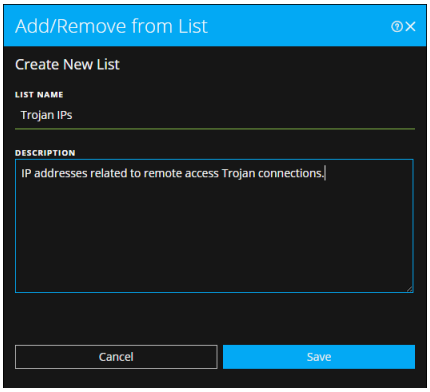
Créer une liste

Vous pouvez créer des listes dans Context Hub à partir de la vue Répondre. En plus d'utiliser des listes dans des entités de liste blanche et de liste noire, vous pouvez utiliser des listes pour surveiller des entités présentant un comportement anormal. Par exemple, pour améliorer la visibilité d'une adresse IP suspecte et du domaine faisant l'objet d'une enquête, vous pouvez les inclure dans deux listes distinctes. La première liste peut concerner les domaines suspectés d'être liés aux connexions de commande et contrôle, et une autre liste peut concerner les adresses IP liées aux connexions de chevaux de Troie autorisant un accès à distance. Vous pouvez ensuite identifier les indicateurs de compromis à l'aide de ces listes.

Pour créer une liste dans Context Hub :

1. Dans le panneau Indicateurs, Liste d'événements, Détails de l'événement ou Graphique de nœud, survolez l'entité soulignée que vous souhaitez ajouter à une liste Context Hub.
   Une info-bulle contextuelle s'affiche et présente les actions disponibles.
2. Dans la section **ACTIONS** de l'info-bulle, cliquez sur **Ajouter à la liste/Supprimer de la liste**.

3. Dans la boîte de dialogue Ajouter à la liste/Supprimer de la liste, cliquez sur **Créer une nouvelle liste**.



4. Saisissez une valeur **Nom de la liste** unique pour obtenir la liste. Le nom de la liste n'est pas sensible à la casse.
5. (Facultatif) Saisissez une **DESCRIPTION** pour la liste.
   Les analystes disposant des autorisations adéquates peuvent également exporter des listes au format CSV à envoyer à d'autres analystes pour un suivi et une analyse approfondis. Le *Guide de configuration de Context Hub* fournit des informations supplémentaires.

Pivoter vers le point de terminaison NetWitness

Si l'application de client Thick NetWitness Endpoint est installée, vous pouvez la démarrer via l'info-bulle de contexte. À partir de là, vous pouvez mener davantage l'enquête sur une adresse IP suspecte, un hôte ou une adresse MAC.

1. Dans le panneau Indicateurs, Liste d'événements, Détails de l'événement ou Graphique de nœud, survolez une entité soulignée pour accéder à une info-bulle contextuelle.
2. Dans la section **ACTIONS** de l'info-bulle, sélectionnez **Pivoter vers le point de terminaison**.
   L'application NetWitness Endpoint s'ouvre en dehors de votre navigateur Web.

Pour plus d'informations, consultez le *NetWitness EndpointGuide d'utilisation*.

Pivoter vers la fonction Enquêter

Pour une procédure d'enquête plus approfondie de l'incident, vous pouvez accéder à la vue Procédure d'enquête.

1. Dans le panneau Indicateurs, Liste d'événements, Détails de l'événement ou Graphique de nœud, survolez une entité soulignée pour accéder à une info-bulle contextuelle.

2. Dans la section **ACTIONS** de l'info-bulle, sélectionnez **Pivoter vers la fonction Enquêter**. Enquêter - vue Naviguer s'ouvre, ce qui vous permet d'effectuer une procédure d'enquête plus approfondie.

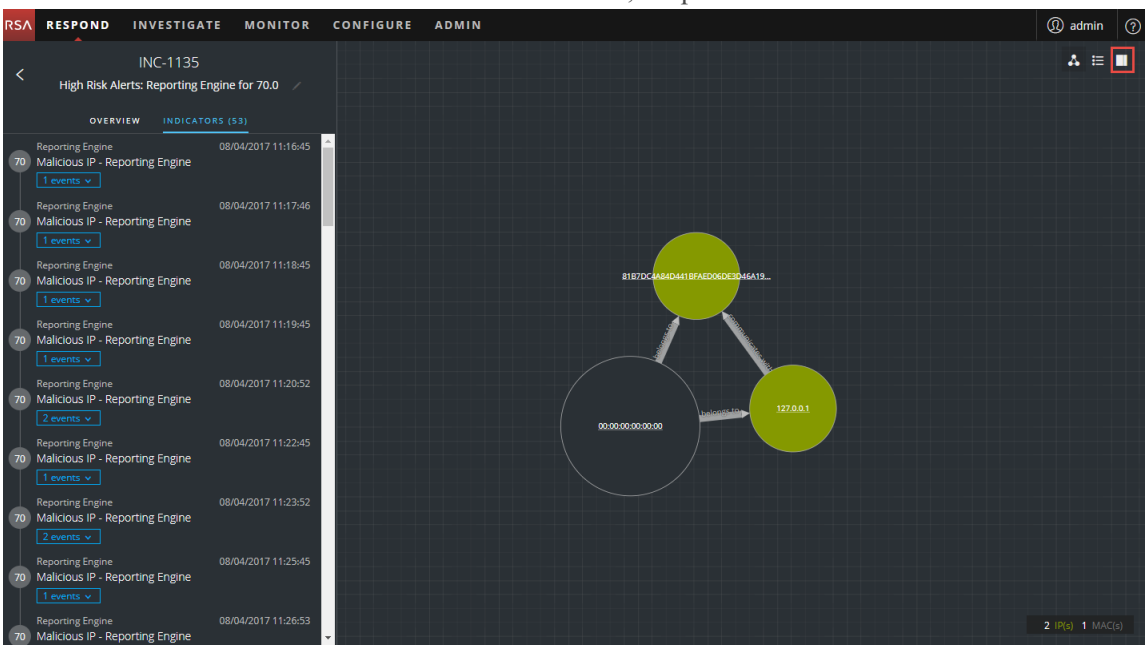
Pour plus d'informations, consultez le *Guide d'utilisation Investigation et Malware Analysis*.

Documenter les étapes suivies en dehors de NetWitness

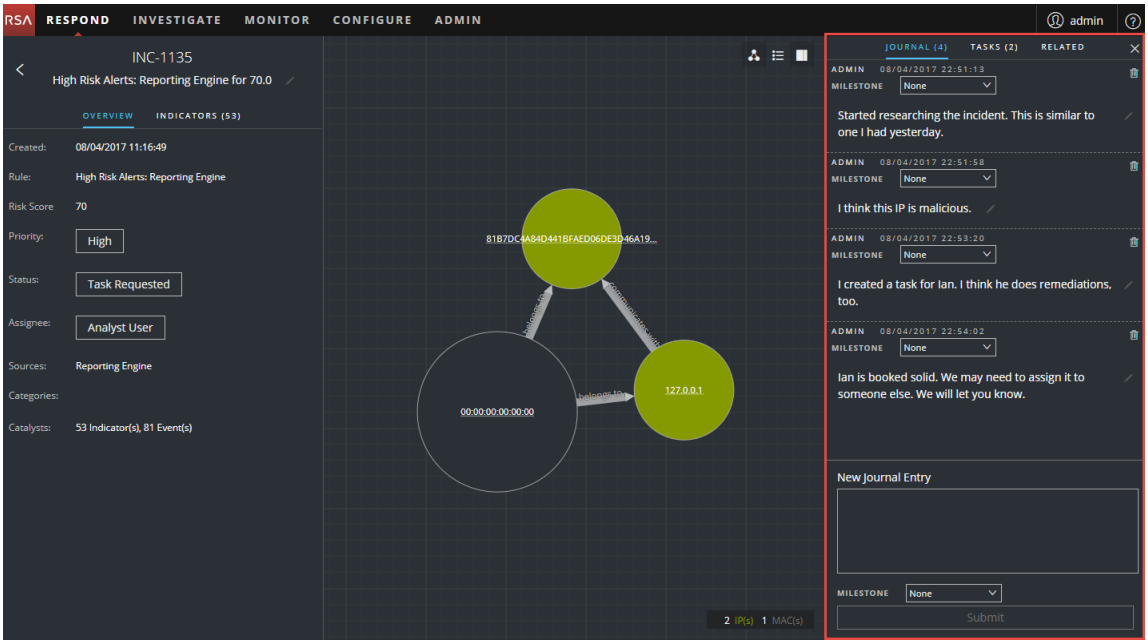
Le journal affiche les commentaires ajoutés par les analystes et vous permet de collaborer avec vos homologues. Vous pouvez valider les notes dans un journal, ajouter des balises Étape Investigation (Reconnaissance, Remise, Exploitation, Installation, Commande et contrôle), et afficher l'historique de l'activité sur votre incident.

Afficher les entrées de journal pour un incident

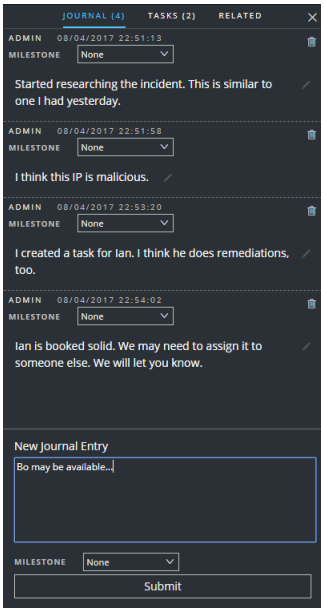
Dans la barre d'outils de la vue Détails de l'incident, cliquez sur ▣ .



Le Journal s'affiche sur le côté droit de la vue Détails de l'incident.



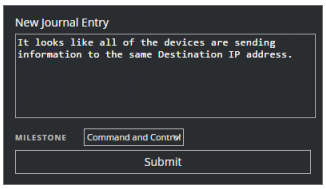
Le Journal présente l'historique de l'activité sur un incident. Pour chaque entrée de journal, l'auteur et l'heure de l'entrée sont affichés.



Ajouter une remarque

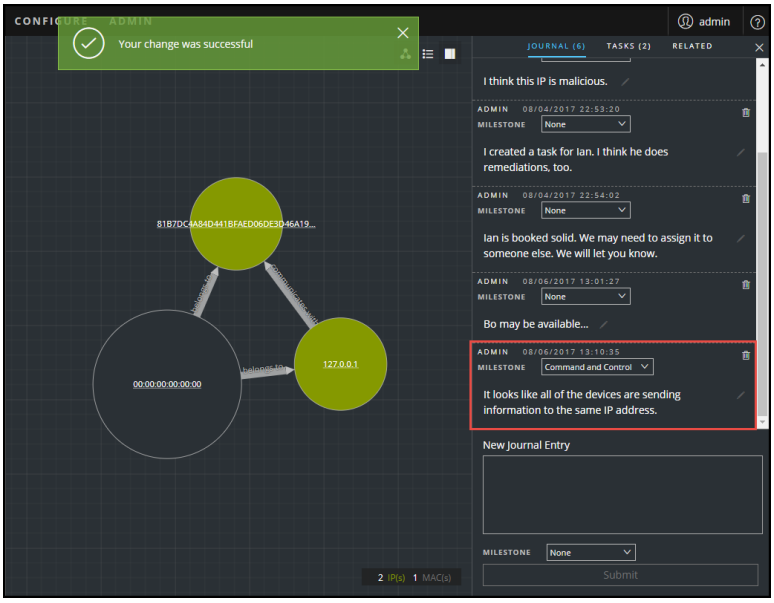
En règle générale, vous devez ajouter une remarque pour permettre à un autre analyste de comprendre l'incident, ou ajouter une remarque pour la suite afin que vos étapes de procédure d'enquête soient documentées.

1. Au bas du panneau Journal, saisissez votre remarque dans la zone **Nouvelle entrée de journal**.



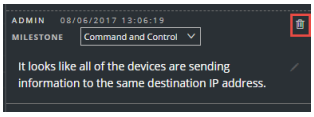
2. (Facultatif) Sélectionnez une Étape Investigation dans la liste déroulante (Reconnaissance, Livraison, Exploitation, Installation, Commande et contrôle, Action sur l'objectif, Contention, Éradication et Clôture).

3. Une fois la rédaction de votre remarque terminée, cliquez sur **Envoyer**.
   Votre nouvelle entrée de journal s'affiche dans le Journal.



Supprimer une remarque

1. Dans le panneau Journal, localisez l'entrée de journal que vous souhaitez supprimer.
2. Cliquez sur l'icône Corbeille (supprimer) en regard de l'entrée de journal.



3. Dans la fenêtre de confirmation qui s'affiche, cliquez sur **OK** pour confirmer que vous souhaitez supprimer l'entrée de journal. Cette action ne peut pas être annulée.

Faire remonter ou corriger l'incident

Il peut être utile d'affecter des incidents à un autre analyste ou de modifier l'état et la priorité d'un incident lorsque vous collectez plus d'informations à son sujet. C'est utile si, par exemple, vous mettez à niveau la priorité d'un incident de **moyenne** à **haute** après avoir déterminé que l'incident constitue une violation majeure.

Mettre à jour un incident

Vous pouvez mettre à jour un incident à partir de plusieurs emplacements. Vous pouvez modifier la priorité, l'état ou la personne affectée à partir de la vue Liste des incidents et de la vue Détails de l'incident. Par exemple, si vous êtes un analyste, vous pouvez vous attribuer un dossier à partir de la vue Liste des incidents si vous voyez qu'il est associé à un autre dossier sur lequel vous travaillez. Si vous êtes un responsable SOC ou un administrateur, vous pouvez afficher les incidents non affectés dans la vue Liste des incidents et attribuer les incidents à mesure qu'ils sont disponibles. Les responsables SOC et les administrateurs peuvent effectuer des mises à jour en bloc de la priorité, de l'état ou de la personne affectée au lieu de les mettre à jour un incident à la fois.

Depuis la vue Détails, vous pouvez remplacer l'état par « En cours » une fois que vous commencez à travailler sur un incident, puis le mettre à jour à « Clôturé » ou « Clôturé - Faux positif » après avoir résolu le problème. Vous pouvez aussi modifier la priorité de l'incident à « Moyenne » ou « Élevée » au fur et à mesure que vous déterminez les détails du dossier.

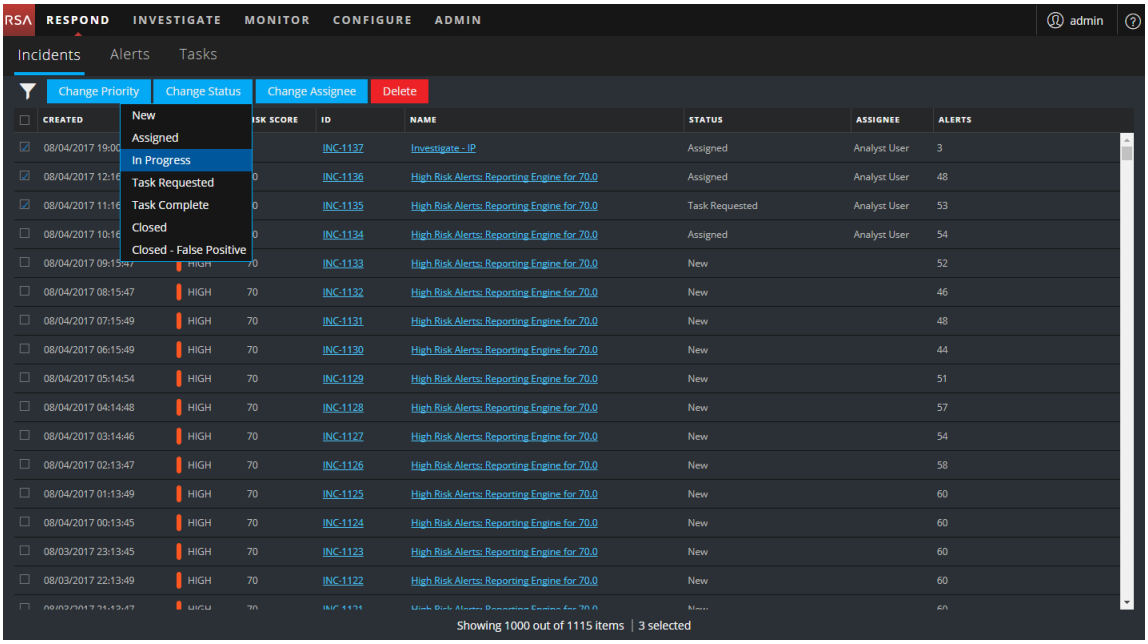
Modifier l'état des incidents

Lorsqu'un incident s'affiche d'abord dans la liste des incidents, il possède l'état initial Nouveau. Vous pouvez mettre à jour l'état à mesure que vous terminez votre travail sur l'incident. Les états suivants sont disponibles :

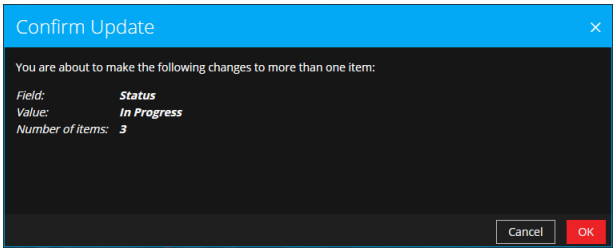
- Nouveau
- Affecté
- En cours
- Tâche demandée
- Tâche terminée
- Closed
- Clôturé - Faux positif

Pour mettre à jour l'état de plusieurs incidents :

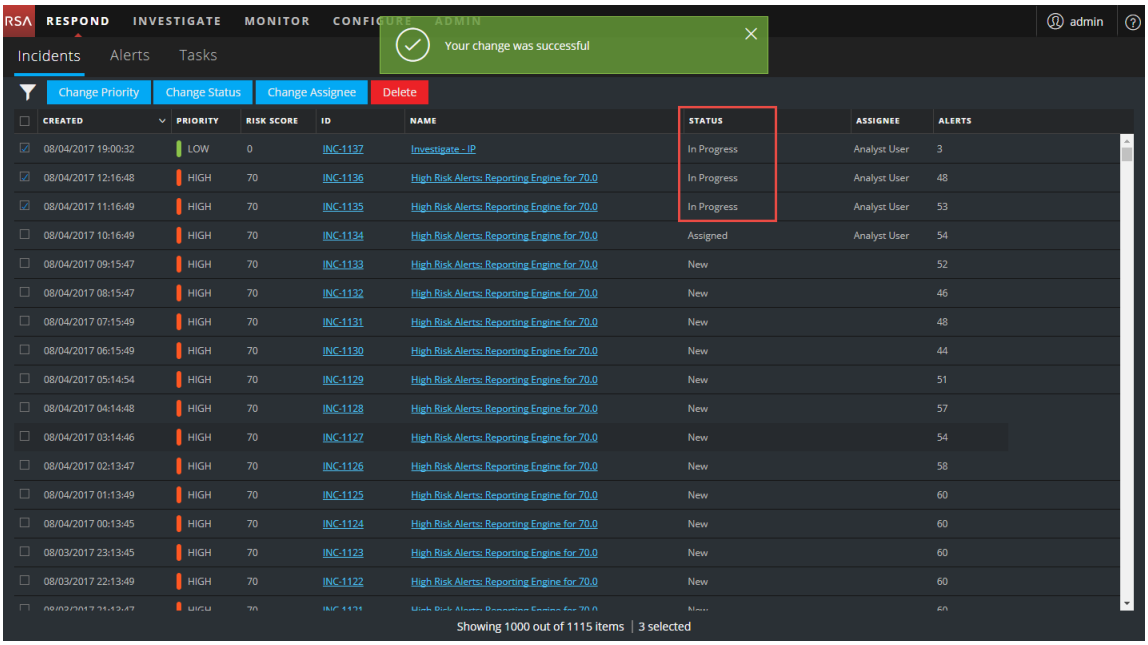
1. Dans la vue Liste d'incidents, sélectionnez un ou plusieurs incidents que vous souhaitez modifier. Pour sélectionner tous les incidents sur la page, activez la case dans la ligne d'en-tête de la liste d'incidents. Le nombre d'incidents sélectionné affiche le pied de page de la liste des incidents.
2. Cliquez sur **Modifier l'état** et sélectionnez un état dans la liste déroulante. Dans cet exemple, l'état actuel est Attribué, mais l'analyste souhaiterait le remplacer par En cours pour les incidents sélectionnés.



3. Si vous sélectionnez plus d'un incident, dans la boîte de dialogue **Confirmer la mise à jour**, cliquez sur **OK**.

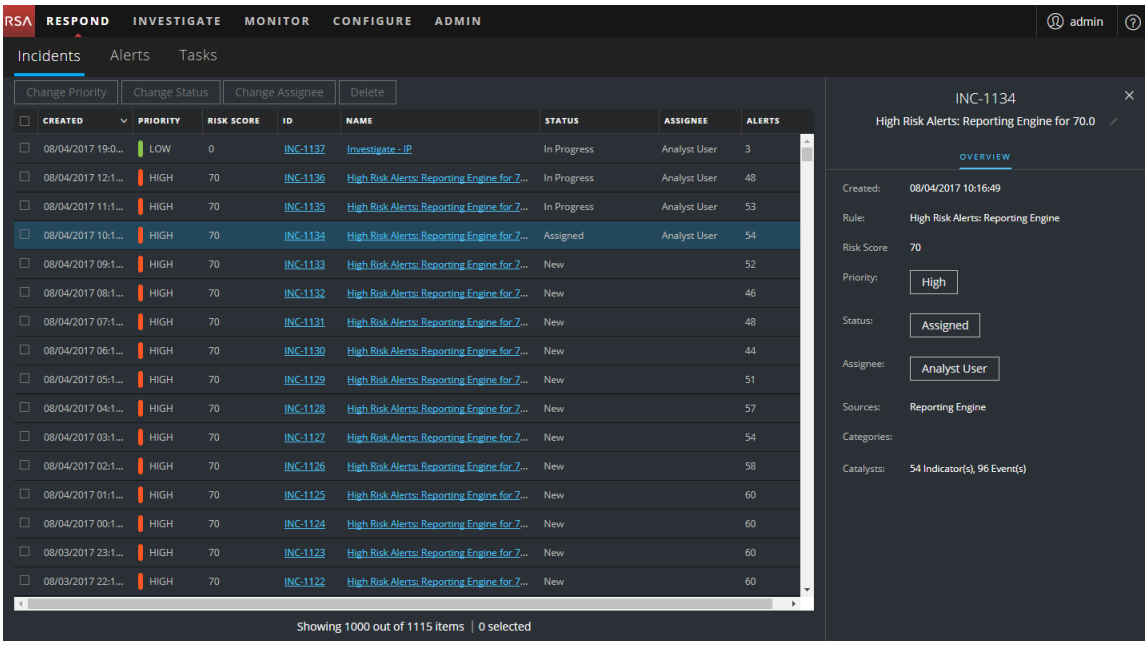


Vous verrez une notification de modification réussie. Dans cet exemple, l'état des incidents mis à jour affiche désormais En cours.



Pour modifier l'état d'un seul incident dans le panneau Présentation :

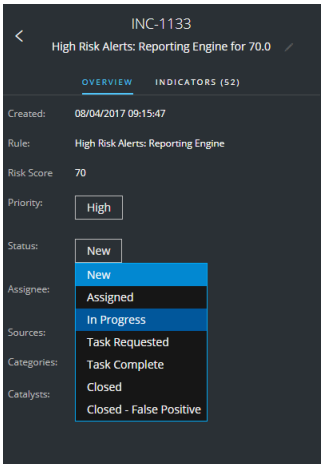
1. Pour ouvrir le panneau Présentation, effectuez l'une des opérations suivantes :
   - Dans la vue Liste d'incidents, cliquez sur un incident qui a besoin d'une mise à jour de l'état.



- Dans la vue Détails de l'incident, cliquez sur l'onglet **PRÉSENTATION**.

Dans le panneau Présentation, le bouton État affiche l'état actuel de l'incident.

2. Cliquez sur le bouton **État** et sélectionnez un état dans la liste déroulante.



Vous verrez une notification de modification réussie.

Modifier la priorité de l'incident

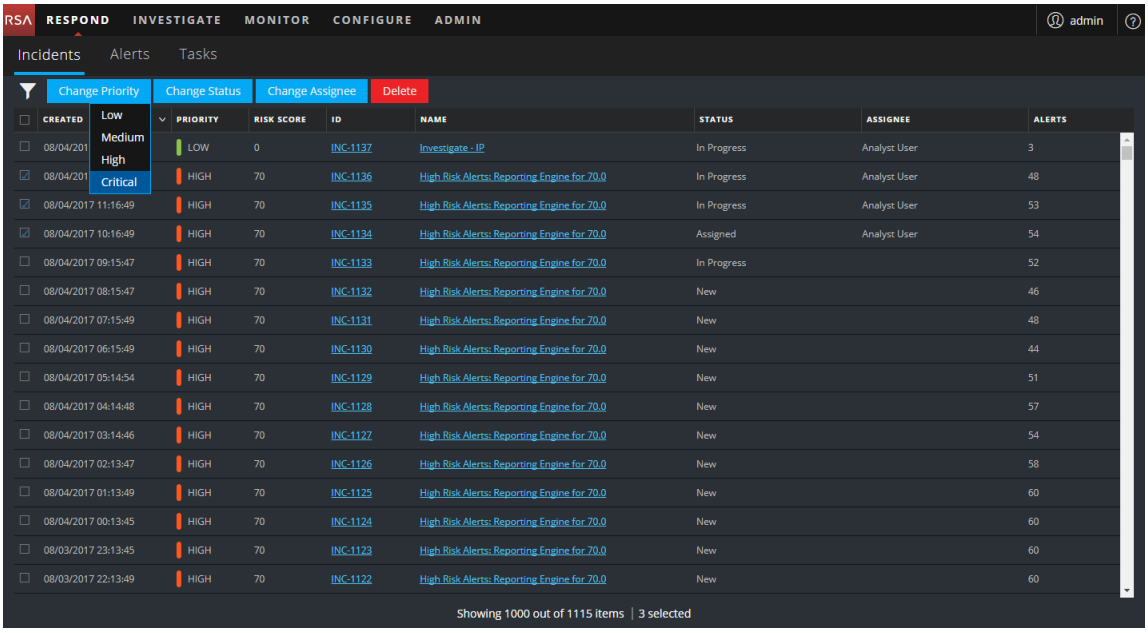
La liste des incidents est triée par priorité par défaut. Vous pouvez mettre à jour la priorité tandis que vous examinez les détails de l'incident. Les priorités suivantes sont disponibles :

- Critique
- Élevée
- Medium
- Low

Remarque : Vous ne pouvez pas modifier la priorité d'un incident clos.

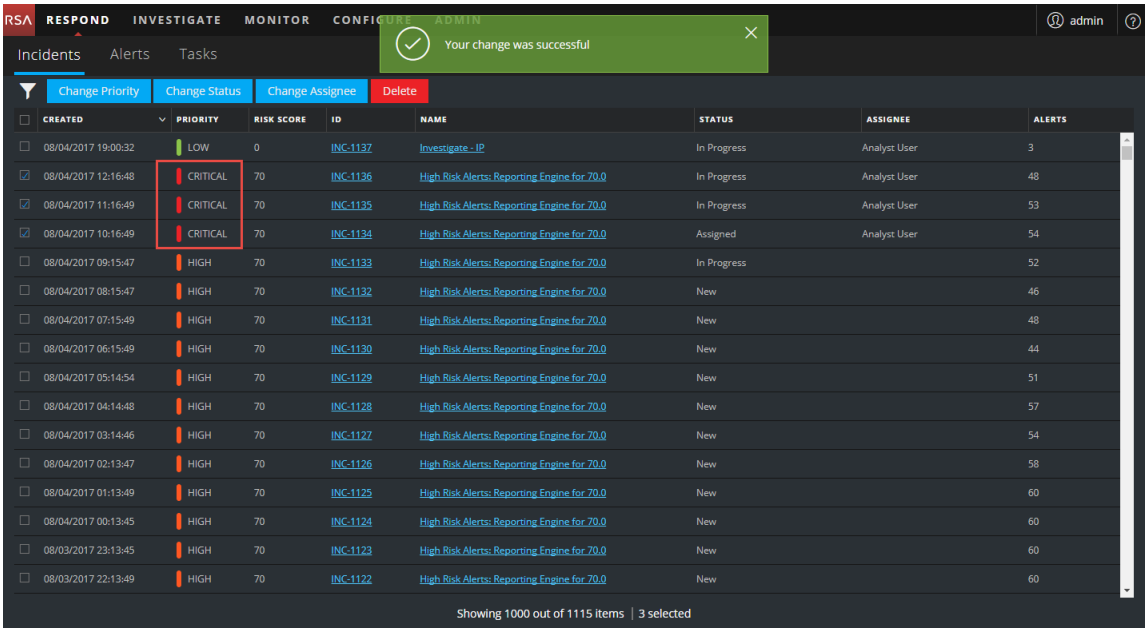
Pour mettre à jour la priorité de plusieurs incidents :

1. Dans la vue Liste d'incidents, sélectionnez un ou plusieurs incidents que vous souhaitez modifier. Pour sélectionner tous les incidents sur la page, activez la case dans la ligne d'en-tête de la liste d'incidents. Le nombre d'incidents sélectionné affiche le pied de page de la liste des incidents.
2. Cliquez sur **Modifier la priorité**, sélectionnez une priorité dans la liste déroulante. Dans cet exemple, la priorité actuelle est Élevé, mais l'analyste souhaiterait le remplacer par Critique pour les incidents sélectionnés.



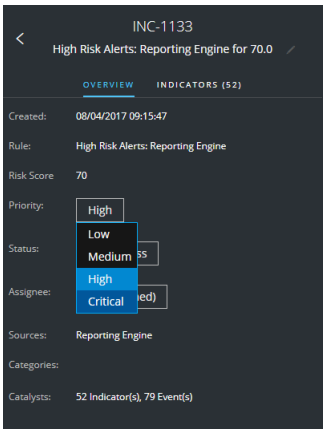
3. Si vous sélectionnez plus d'un incident, dans la boîte de dialogue **Confirmer la mise à jour**, cliquez sur **OK**.
   Vous verrez une notification de modification réussie. Dans cet exemple, l'état des incidents

mis à jour affiche désormais Critique.



Pour modifier la priorité d'un seul incident dans le panneau Présentation

1. Pour ouvrir le panneau Présentation, effectuez l'une des opérations suivantes :
   - Dans la vue Liste d'incidents, cliquez sur un incident qui a besoin d'une mise à jour de la priorité.
   - Dans la vue Détails de l'incident, cliquez sur l'onglet **PRÉSENTATION**.
     Dans le panneau Présentation, le bouton Priorité affiche la priorité actuelle de l'incident.
2. Cliquez sur le bouton **Priorité** et sélectionnez un état dans la liste déroulante.



Vous verrez une notification de modification réussie. Le bouton Priorité change pour afficher la nouvelle priorité d'incident.

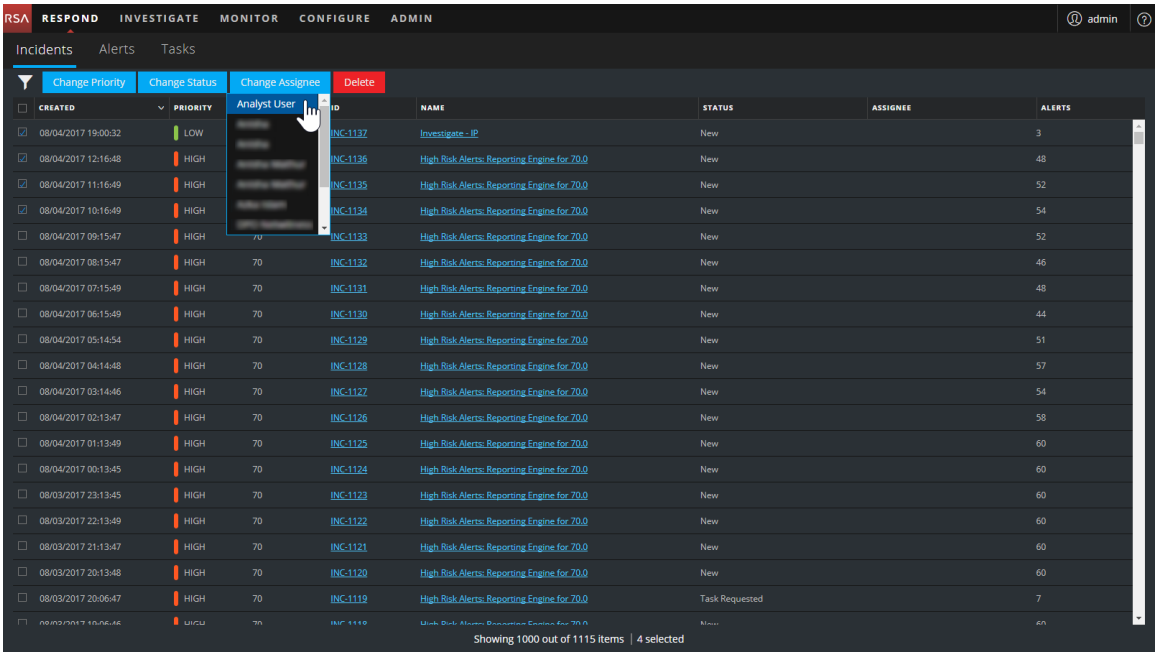
Attribuer les incidents à d'autres analystes

Vous pouvez attribuer des incidents à d'autres analystes de la même manière que vous affectez des incidents à vous-même. Les responsables SOC et les administrateurs peuvent attribuer plusieurs incidents à un utilisateur en même temps.

Remarque : Vous ne pouvez pas modifier la personne affectée d'un incident clos.

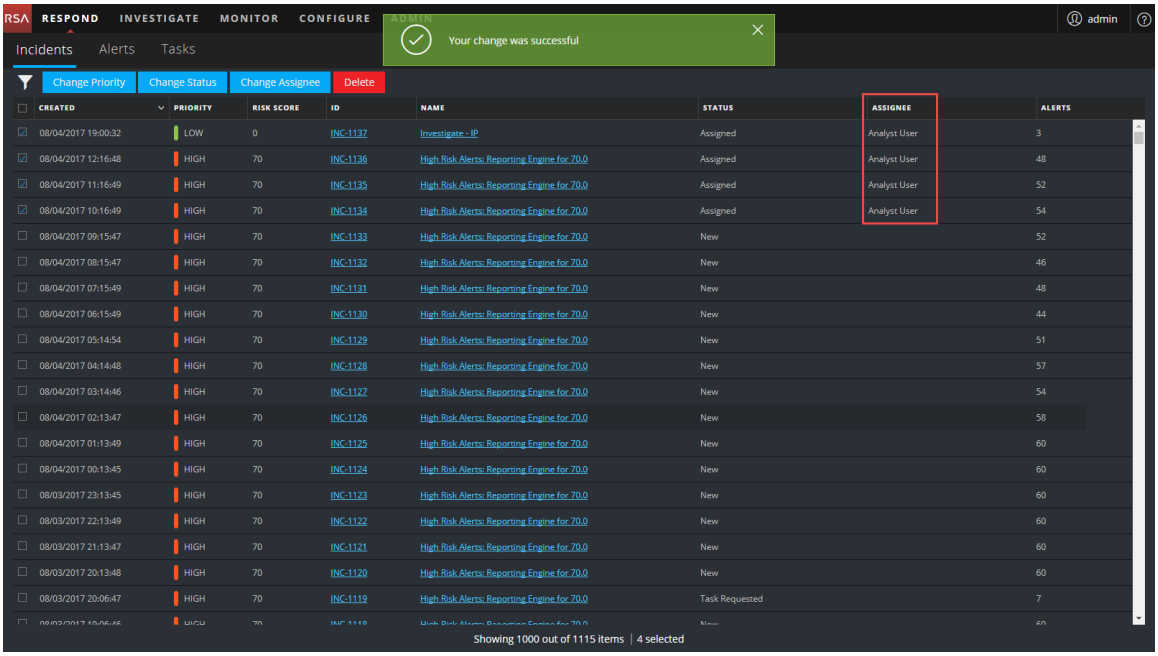
Pour affecter plusieurs incidents à un utilisateur :

1. Dans la vue Liste d'incidents, sélectionnez les incidents que vous souhaitez affecter à un utilisateur. Pour sélectionner tous les incidents sur la page, activez la case dans la ligne d'en-tête de la liste d'incidents. Le nombre d'incidents sélectionné affiche le pied de page de la liste des incidents.
2. Cliquez sur **Modifier la personne affectée** et sélectionnez un utilisateur dans la liste déroulante. Dans cet exemple, les incidents sont non attribués, mais ils doivent être attribués à un analyste.



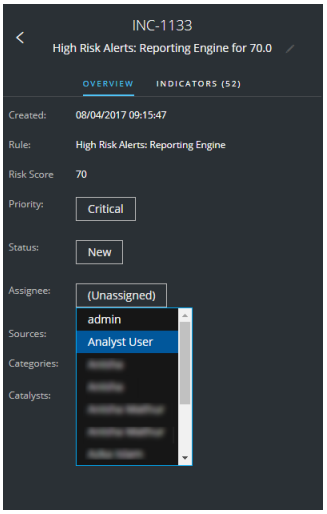
3. Si vous sélectionnez plus d'un incident, dans la boîte de dialogue **Confirmer la mise à jour**, cliquez sur **OK**.
   Vous verrez une notification de modification réussie. La personne affectée devient

l'utilisateur sélectionné.



Pour attribuer un utilisateur à un incident à partir du panneau Présentation :

1. Pour ouvrir le panneau Présentation, effectuez l'une des opérations suivantes :
   - Dans la vue Liste d'incidents, cliquez sur un incident qui a besoin d'une mise à jour de la priorité.
   - Dans la vue Détails de l'incident, cliquez sur l'onglet **PRÉSENTATION**.
     Dans le panneau Présentation, le bouton Priorité affiche la priorité actuelle de l'incident.
     Dans l'exemple suivant, le bouton Personne affectée possède l'état actuel Non attribué.

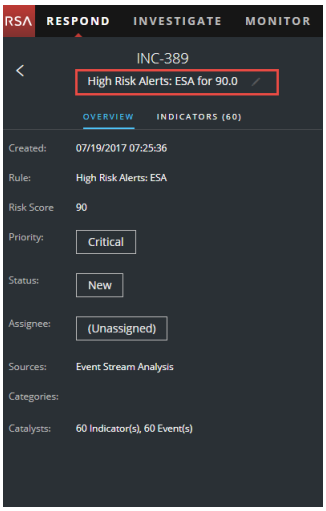


2. Cliquez sur le bouton **Personne affectée** et sélectionnez un utilisateur dans la liste déroulante.
   Vous verrez une notification de modification réussie. Le bouton Personne affectée change pour afficher l'utilisateur affecté.

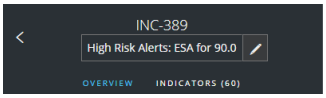
Renommer un incident

Vous pouvez renommer un incident depuis le panneau Présentation dans la vue Liste d'incidents et la vue Détails de l'incident. Par exemple, vous pouvez renommer un incident pour fournir des précisions sur le problème, en particulier si plusieurs incidents ont le même nom.

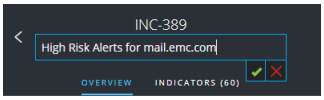
1. Accédez à **RÉPONDRE > Incidents**.
2. Pour ouvrir le panneau Présentation, effectuez l'une des opérations suivantes :
   - Dans la vue Liste d'incidents, cliquez sur un incident dont le nom doit être modifié.
     Le panneau Présentation s'ouvre.
   - Dans la vue Détails de l'incident, accédez au panneau **PRÉSENTATION**.
     Dans l'en-tête au-dessus du panneau Présentation, vous voyez l'ID d'incident et le nom de l'incident.



3. Cliquez sur le nom de l'incident dans l'en-tête pour ouvrir un éditeur de texte.



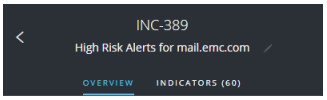
4. Saisissez un nouveau nom pour l'incident dans l'éditeur de texte, puis cliquez sur la case à cocher pour confirmer la modification.



Par exemple, vous pouvez remplacer « Alertes à risque élevé : ESA pour 90.0 » par « Alertes pour mail.emc.com » pour plus de clarté.

Vous verrez une notification de modification réussie.

Le champ Nom de l'incident présente le nouveau nom.

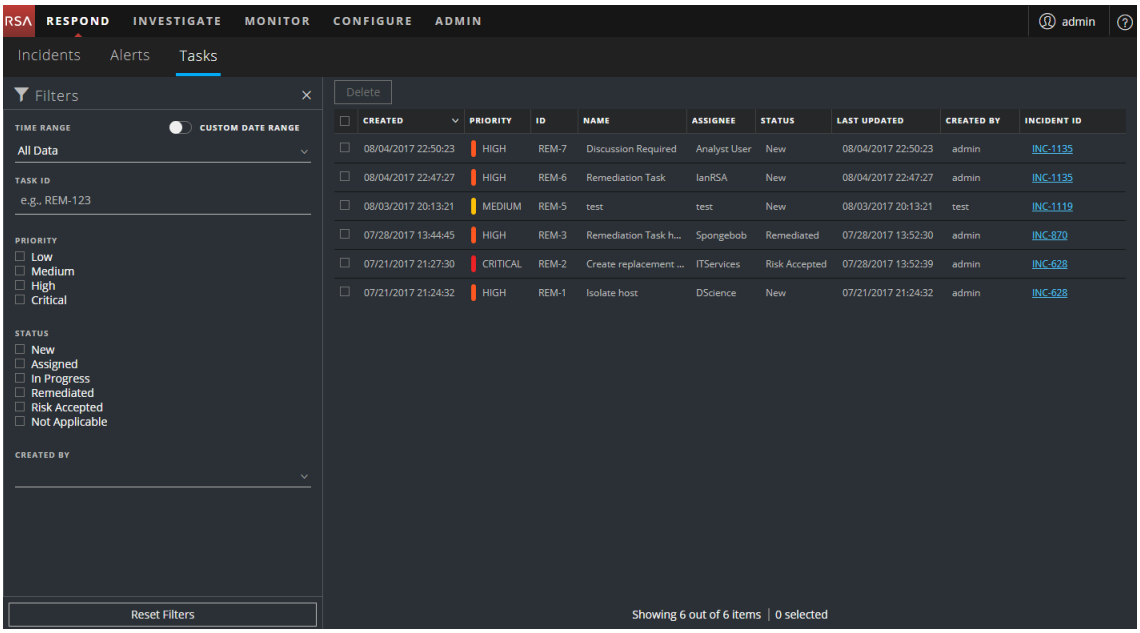


Afficher toutes les tâches d'incident

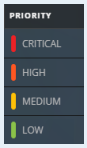
Lorsque le travail supplémentaire est requis pour un incident, vous pouvez créer des tâches pour l'incident et suivre la progression de ces tâches. Cela est utile, par exemple, lorsque le travail en cours d'exécution est extérieur aux opérations de sécurité ou lorsque vous faites une demande pour une nouvelle image d'ordinateur. Dans la vue Liste de tâches, vous pouvez gérer et suivre les tâches^jusqu'à sa fermeture.

1. Accédez à **RÉPONDRE > Tâches**.

La vue Liste de tâches affiche la liste de toutes les tâches d'incidents.



2. Faites défiler la liste de tâches, qui affiche des informations de base sur chaque tâche, comme décrit dans le tableau suivant.

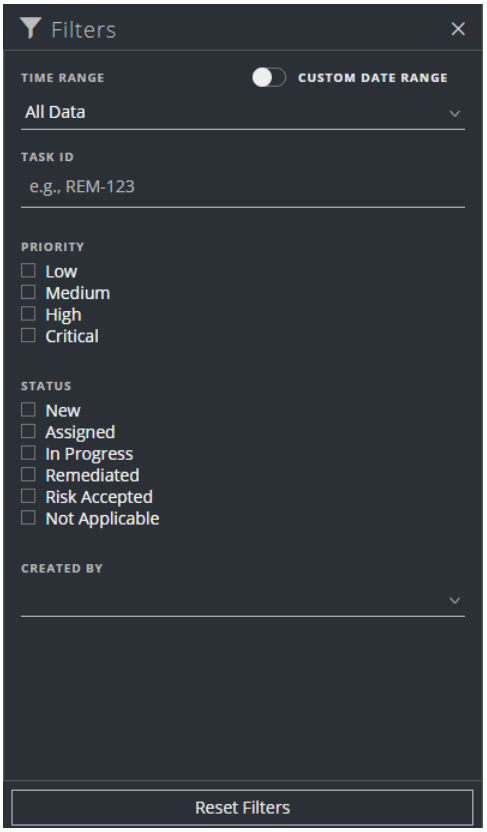
Colonne	Description
DATE DE CRÉATION	Affiche la date de création de la tâche.
PRIORITÉ	Affiche la priorité attribuée à la tâche. La priorité peut être l'une des suivantes : Critique, Élevé, Moyen ou Faible. La priorité est également indiquée à l'aide d'un code couleur, où rouge indique **Critique**, orange représente un risque **Élevé**, jaune indique un risque **Moyen** et vert représente un risque **Faible**, comme illustré dans la figure suivante : 
ID	Affiche l'ID de tâche.
NOM	Affiche le nom de la tâche.
PERSONNE AFFECTÉE	Affiche le nom de l'utilisateur auquel la tâche est attribuée.
ÉTAT	Affiche l'état de la tâche : Nouveau, Attribué, En cours, Corrigé, Risque accepté et Sans objet.
DATE DE DERNIÈRE MISE À JOUR	Affiche la date et l'heure auxquelles la tâche a été mise à jour pour la dernière fois.
CRÉÉ PAR	Affiche l'utilisateur qui a créé la tâche.
ID d'incident	Affiche l'ID d'incident pour lequel la tâche a été créée. Cliquez sur cet ID pour afficher les détails de l'incident.

Au bas de la liste, vous voyez le nombre de tâches sur la page en cours, le nombre total de tâches et le nombre de tâches sélectionné. Par exemple : **Affichage de 6 éléments sur 6 | 2 sélectionnés**.

Filtrer la liste des tâches

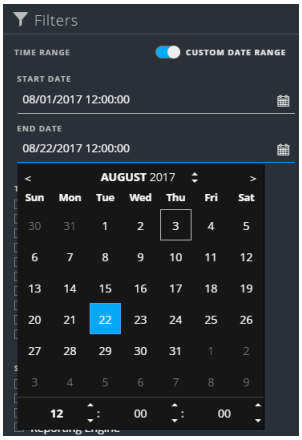
Le nombre de tâches dans la Liste des tâches peut être très volumineux, ce qui complexifie la recherche de tâches particulières. Le filtre vous permet de spécifier les tâches que vous souhaitez afficher, comme les tâches créées dans les 7 derniers jours. Vous pouvez également rechercher une tâche spécifique.

1. Accédez à **RÉPONDRE > Tâches**.
   Le panneau Filtres s'affiche à gauche de la liste des tâches. Si vous ne voyez pas le panneau Filtres, dans la barre d'outils de la vue Liste des tâches, cliquez sur afin d'ouvrir le panneau Filtres.



2. Dans le panneau Filtres, sélectionnez une ou plusieurs options pour filtrer la liste des incidents :

- **PLAGE TEMPORELLE** : Vous pouvez sélectionner une période spécifique dans la liste déroulante Période. La période est basée sur la date de création des tâches. Par exemple, si vous sélectionnez Dernière heure, vous verrez les tâches qui ont été créées au cours des 60 dernières minutes.
- **PLAGE DE DATES PERSONNALISÉE** : Vous pouvez spécifier une plage de dates spécifique au lieu de sélectionner une option de période. Pour ce faire, cliquez sur le cercle blanc devant PLAGE DE DATES PERSONNALISÉE pour afficher les champs Date de début et Date de fin. Sélectionnez les dates et heures dans le calendrier.



- **ID DE TÂCHE** : Saisissez l'ID de tâche pour une tâche que vous souhaitez localiser, par exemple REM-123.
- **PRIORITÉ** : Sélectionnez les priorités que vous souhaitez afficher.
- **ÉTAT** : Sélectionnez un ou plusieurs états d'incident. Par exemple, sélectionnez Corrigé pour afficher les tâches de mesure corrective terminées.
- **CRÉÉ PAR** : Sélectionnez l'utilisateur qui a créé les tâches que vous souhaitez afficher. Par exemple, si vous souhaitez afficher les tâches créées par Edwardo uniquement, sélectionnez Edwardo dans la liste déroulante CRÉÉ PAR. Si vous souhaitez afficher les tâches quelle que soit la personne qui a créé la tâche, n'effectuez aucune sélection sous CRÉÉ PAR.

La liste des tâches affiche une liste de tâches qui répondent à vos critères de sélection. Vous pouvez voir le nombre d'éléments dans votre liste filtrée en bas de la liste des tâches.
Par exemple : **Affichage de 6 éléments sur 6**

3. Si vous souhaitez fermer le panneau Filtres, cliquez sur **X**. Vos filtres restent en place jusqu'à ce que vous les supprimiez.

Supprimer Mes filtres de la liste des tâches

NetWitness Suite mémorise vos sélections de filtre dans la liste de tâches. Vous pouvez supprimer vos sélections de filtre lorsque vous n'en avez plus besoin. Par exemple, si vous ne voyez pas le nombre de tâches que vous devriez voir ou si vous souhaitez afficher toutes les tâches dans la liste des tâches, vous pouvez réinitialiser les filtres.

1. Accédez à **RÉPONDRE > Tâches**.

   Le panneau Filtres s'affiche à gauche de la liste des tâches. Si vous ne voyez pas le panneau Filtres, dans la barre d'outils de la vue Liste des tâches, cliquez sur afin d'ouvrir le panneau Filtres.

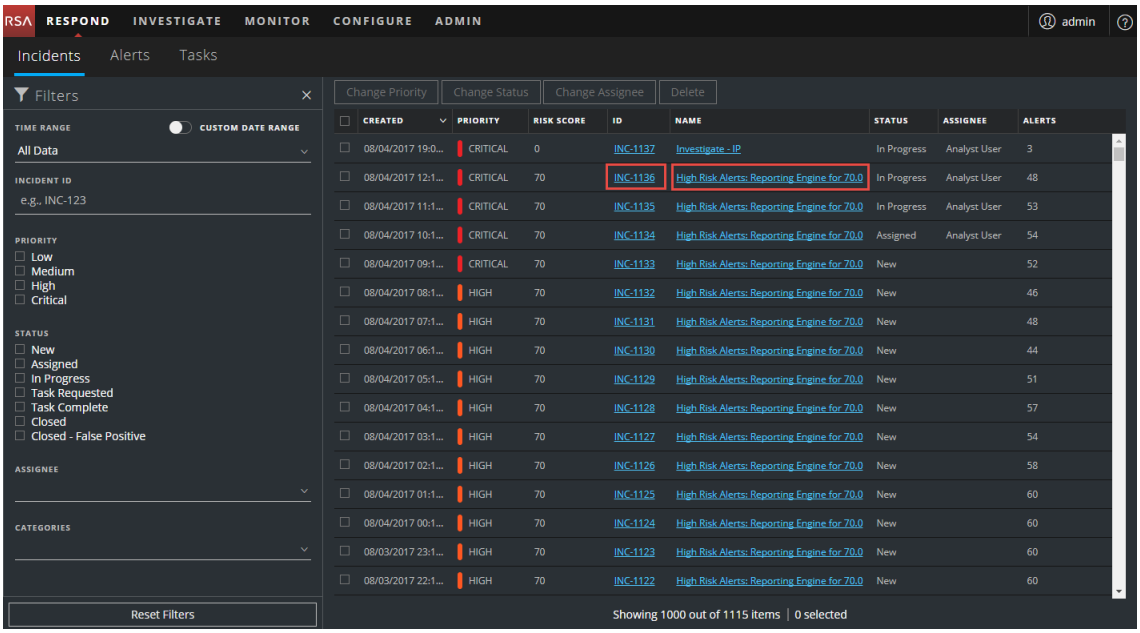
2. Au bas du panneau Filtres, cliquez sur **Réinitialiser les filtres**.

Créer une tâche

Après avoir analysé un incident et avoir reçu plus d'informations, vous pouvez créer une tâche, l'attribuer à un utilisateur et la suivre jusqu'à sa clôture. Vous pouvez créer des tâches à partir de la vue Détails de l'incident.

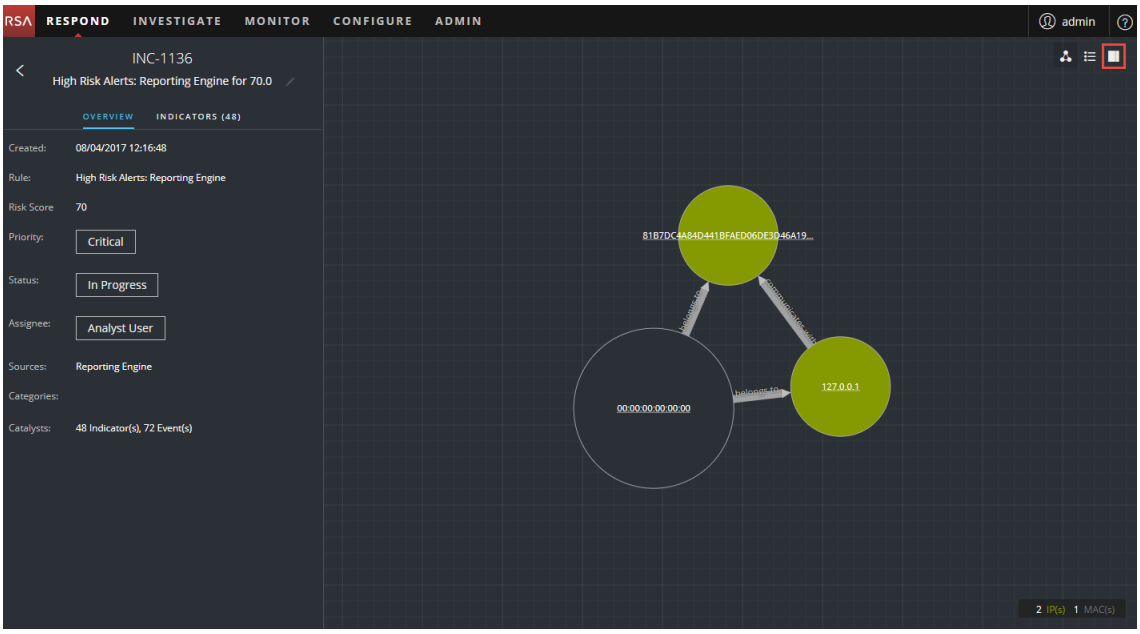
1. Accédez à **RÉPONDRE > Incidents**.

   La vue Liste d'incidents affiche la liste de tous les incidents.



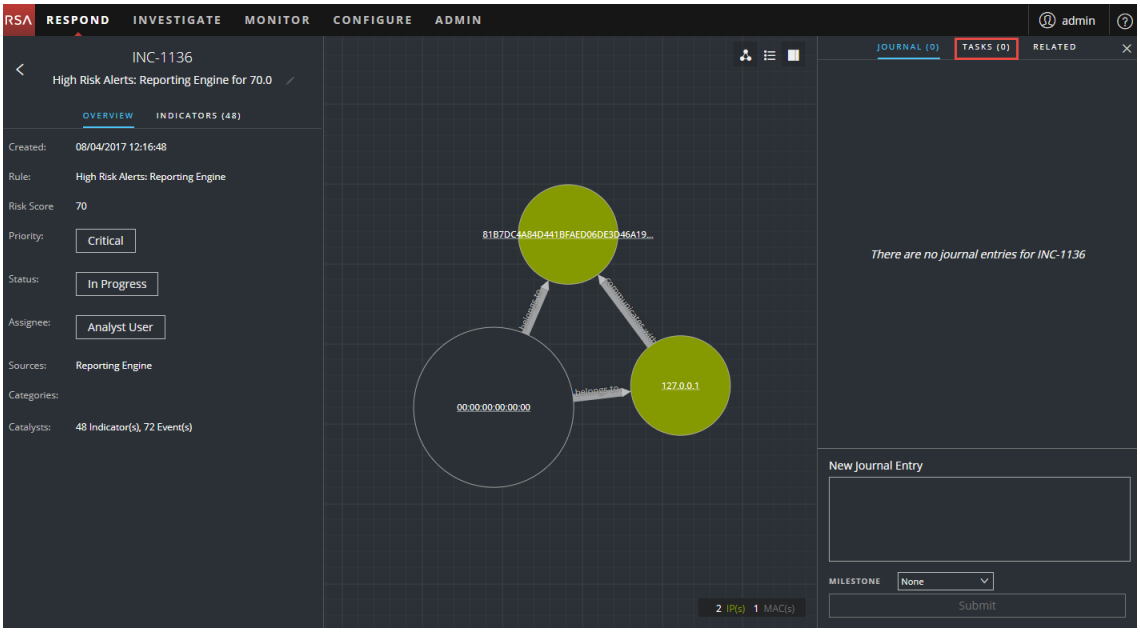
2. Localisez l'incident qui a besoin d'une tâche, puis cliquez sur le lien dans le champ **ID** ou **NOM**.

   La vue Détails de l'incident s'ouvre.

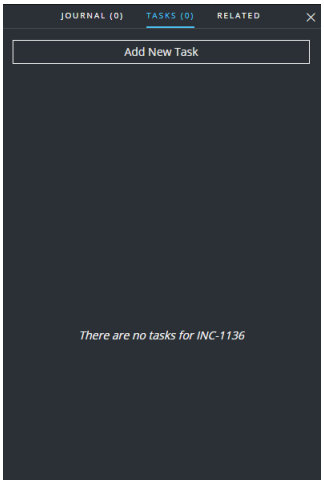


3. Dans la barre d'outils en haut à droite de la vue Détails de l'incident, sélectionnez ▣.

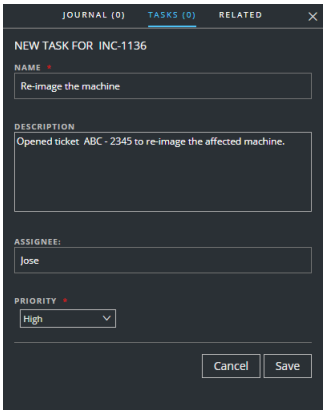
   Le panneau Journal s'ouvre.



4. Sélectionnez l'onglet **TÂCHES**.



5. Dans le panneau Tâches, cliquez sur **Ajouter une nouvelle tâche.**
   Vous verrez les champs Nouvelle tâche.



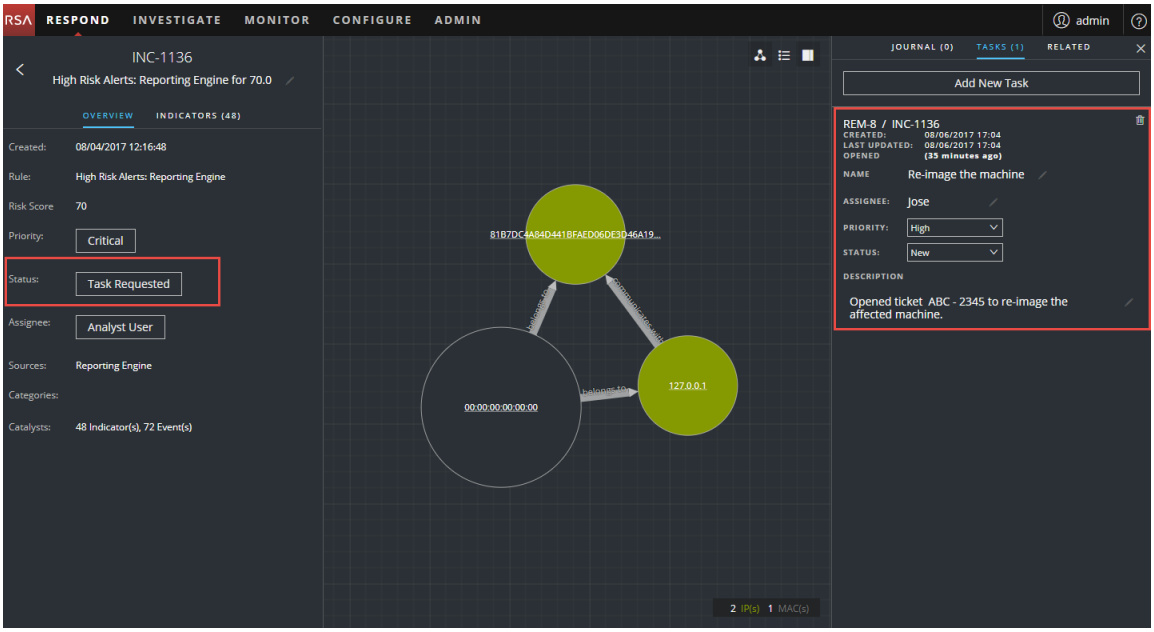
   Si l'incident est dans un état clôturé (Clôturé ou Clôturé - Faux positif), le bouton Ajouter une nouvelle tâche est désactivé.

6. Fournissez les informations suivantes :

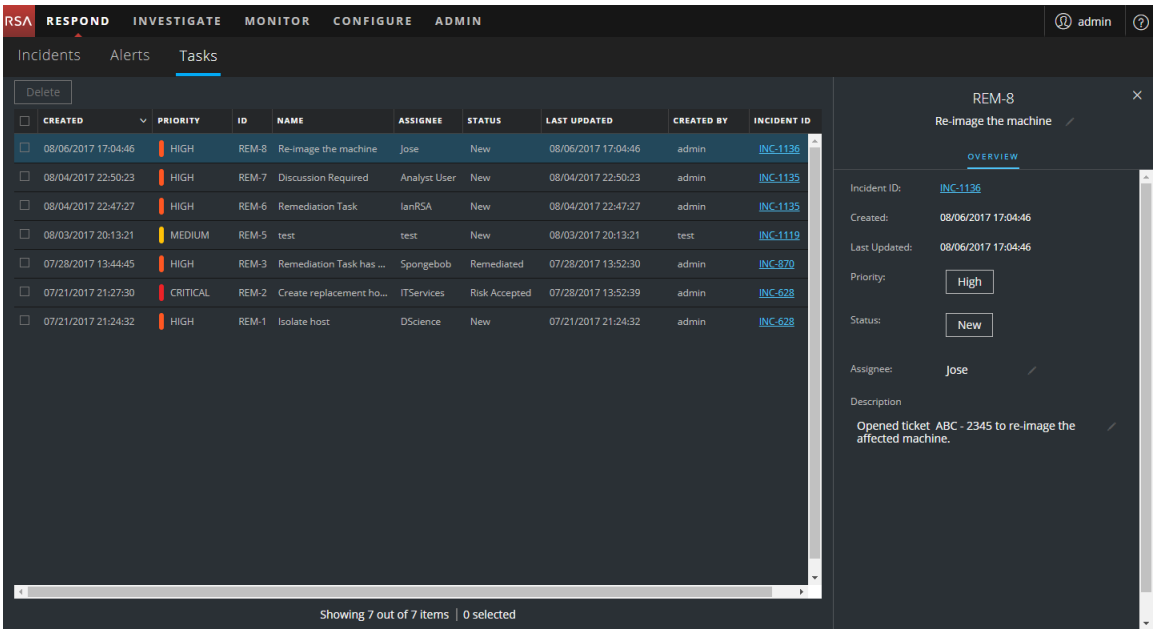
   - **Nom** - Nom de la tâche. Par exemple : Nouvelle image de la machine.
   - **Description** - (Facultatif) Saisissez les informations qui décrivent la tâche. Vous pouvez inclure des numéros de référence applicables.
   - **Personne affectée** - (Facultatif) Saisissez le nom d'utilisateur de l'utilisateur auquel la tâche doit être attribuée.
   - **Priorité** - Cliquez sur le bouton de priorité et sélectionnez une priorité pour la tâche dans la liste déroulante : Faible, Moyen, Élevé ou Critique.

7. Cliquez sur **Enregistrer**.
   Une confirmation indiquant que votre modification a réussi s'affiche. L'état de l'incident

devient **Tâche demandée**. La tâche s'affiche dans le panneau Tâches pour cet incident.



Elle apparaît également dans la liste Tâches (RÉPONDRE > Tâches), qui affiche une liste de toutes les tâches d'incident.

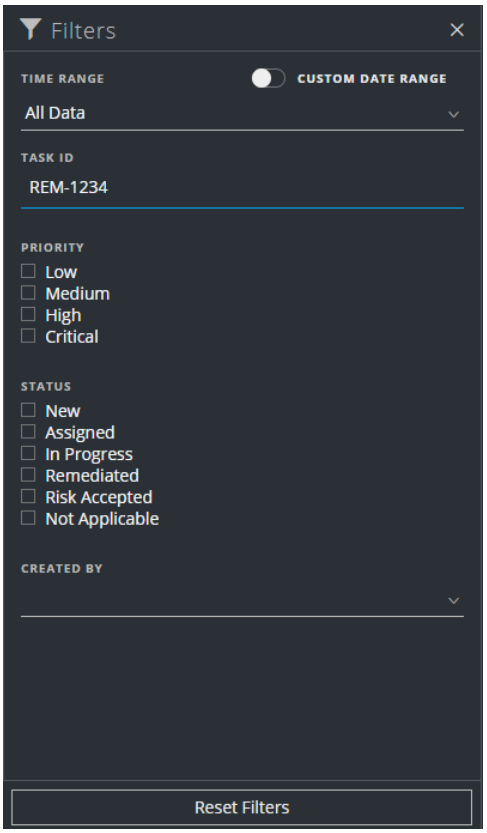


Remarque : Si l'état ne change pas, vous devez actualiser votre navigateur internet.

Recherche d'une tâche

Si vous connaissez l'ID de tâche, vous pouvez localiser rapidement une tâche à l'aide du filtre. Par exemple, vous pouvez rechercher une tâche spécifique parmi des milliers de tâches.

1. Accédez à **RÉPONDRE > Tâches**.
   Le panneau Filtres s'affiche à gauche de la liste des tâches. Si vous ne voyez pas le panneau Filtres, dans la barre d'outils de la vue Liste des tâches, cliquez sur afin d'ouvrir le panneau Filtres.



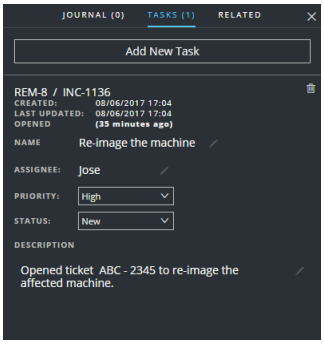
2. Dans le champ ID DE TÂCHE, saisissez l'ID de tâche pour une tâche que vous souhaitez localiser, par exemple REM-1234.
   La tâche spécifiée s'affiche dans votre liste de tâches. Si vous ne voyez pas les résultats, essayez de réinitialiser vos filtres.

Modifier une tâche

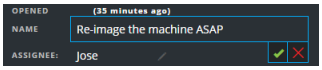
Vous pouvez modifier une tâche à partir d'un incident et dans la liste Tâches. Par exemple, vous souhaitez afficher l'état de la tâche En cours et ajouter des informations complémentaires à la tâche. Si la tâche possède un état fermé (Non applicable, Risque accepté ou Corrigé), vous ne pouvez pas modifier la Priorité ou la Personne affectée.

Pour modifier une tâche à partir d'un incident :

1. Accédez à **RÉPONDRE > Incidents**.
   La vue Liste d'incidents affiche la liste de tous les incidents.
2. Localisez l'incident qui a besoin d'une mise à jour de tâche, puis cliquez sur le lien dans le champ **ID** ou **NOM**.
   La vue Détails de l'incident s'ouvre.
3. Dans la barre d'outils en haut à droite de la vue, sélectionnez .
   Le panneau Journal s'ouvre.
4. Sélectionnez l'onglet **TÂCHES**.
5. Dans le panneau Tâches, une icône représentant un crayon indique un champ de texte que vous pouvez modifier. Un bouton indique qu'il existe une liste déroulante pour effectuer une sélection.

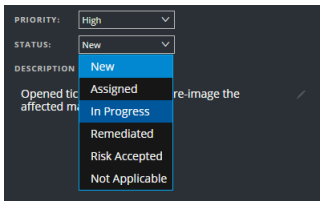


6. Vous pouvez modifier les champs suivants :
   - **NOM** - Cliquez sur le nom de la tâche en cours pour ouvrir un éditeur de texte.

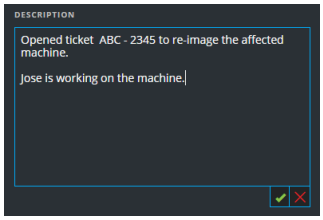


     Cliquez sur la coche pour confirmer la modification. Par exemple, vous pouvez remplacer « Nouvelle image de la machine » par « Nouvelle image de la machine dès que possible ».

- **PERSONNE AFFECTÉE** - Cliquez sur (Non affecté) ou sur le nom de la personne affectée précédente pour ouvrir un éditeur de texte. Saisissez le nom d'utilisateur de l'utilisateur auquel la tâche doit être attribuée.
  Cliquez sur la coche pour confirmer la modification.
- **PRIORITÉ** - Cliquez sur le bouton de priorité et sélectionnez une priorité pour la tâche dans la liste déroulante : Faible, Moyen, Élevé ou Critique.
- **ÉTAT** - Cliquez sur le bouton État et sélectionnez un état de la tâche dans la liste déroulante : Nouveau, Attribué, En cours, Corrigé, Risque accepté et Sans objet. Par exemple, vous pouvez modifier l'état En cours.



- **DESCRIPTION** - Cliquez sur le texte situé sous la description pour ouvrir un éditeur de texte.

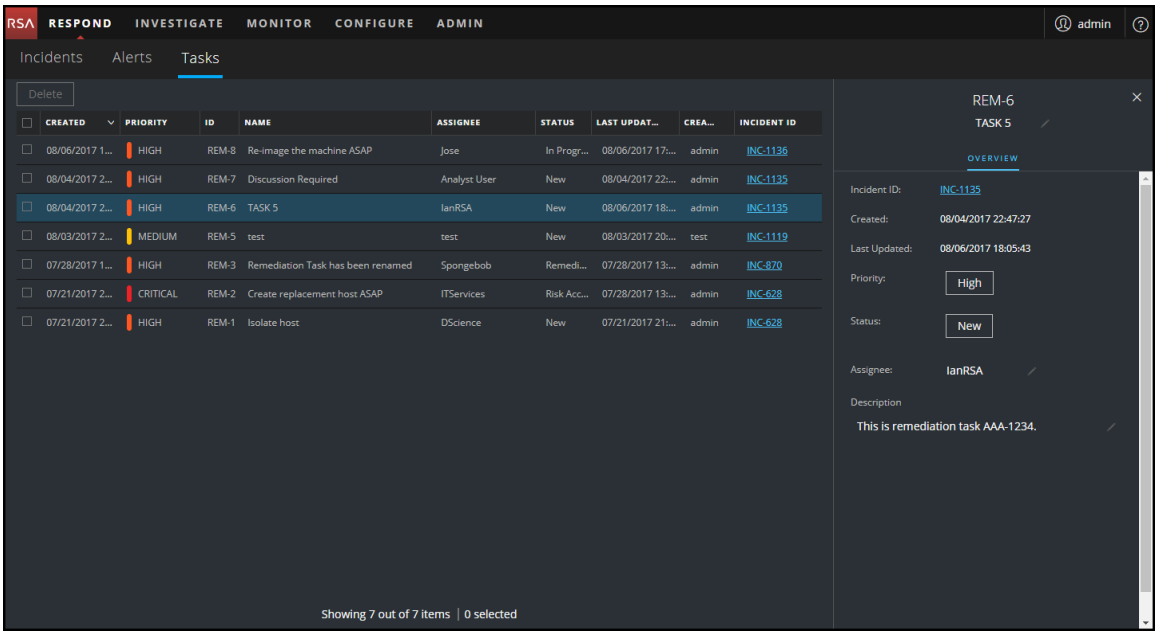


  Modifiez le texte et cliquez sur la coche pour confirmer la modification.

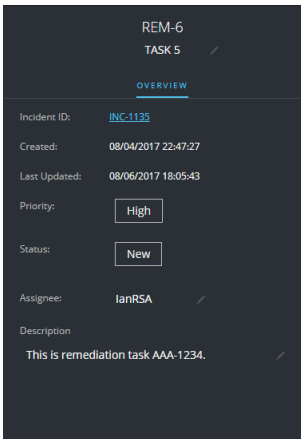
Pour chaque modification que vous apportez, vous verrez une confirmation indiquant que votre modification a réussi.

Pour modifier une tâche dans la liste des tâches :

1. Accédez à **RÉPONDRE > Tâches**.
   La vue Liste de tâches affiche la liste de toutes les tâches d'incidents.
2. Dans la liste Tâches, cliquez sur la tâche que vous voulez mettre à jour.
   Le panneau Présentation de la tâche s'affiche à droite de la liste Tâches.

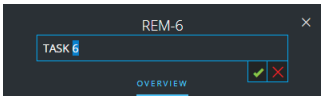


Dans le panneau Présentation de la tâche, une icône représentant un crayon indique un champ de texte que vous pouvez modifier. Un bouton indique qu'il existe une liste déroulante pour effectuer une sélection.



3. Vous pouvez modifier les champs suivants :

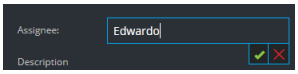
- **<Nom de la tâche>** - En haut du panneau Présentation de la tâche, sous l'ID de tâche, cliquez sur le nom de la tâche en cours pour ouvrir un éditeur de texte.

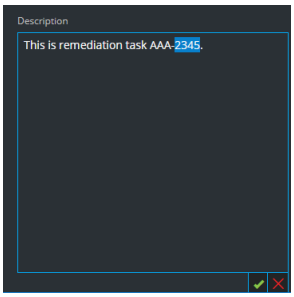
  Cliquez sur la coche pour confirmer la modification. Par exemple, vous pouvez remplacer TÂCHE5 par TÂCHE6.

- **Priorité** - Cliquez sur le bouton de priorité et sélectionnez une priorité pour la tâche dans la liste déroulante : Faible, Moyen, Élevé ou Critique.

- **État** - Cliquez sur le bouton État et sélectionnez un état de la tâche dans la liste déroulante : Nouveau, Attribué, En cours, Corrigé, Risque accepté et Sans objet.
- **Personne affectée** - Cliquez sur (Non affecté) ou sur le nom de la personne affectée précédente pour ouvrir un éditeur de texte. Saisissez le nom d'utilisateur de l'utilisateur auquel la tâche doit être attribuée.

  Cliquez sur la coche pour confirmer la modification.
- **Description** - Cliquez sur le texte situé sous la description pour ouvrir un éditeur de texte.

  Modifiez le texte et cliquez sur la coche pour confirmer la modification.

Pour chaque modification que vous apportez, vous verrez une confirmation indiquant que votre modification a réussi.

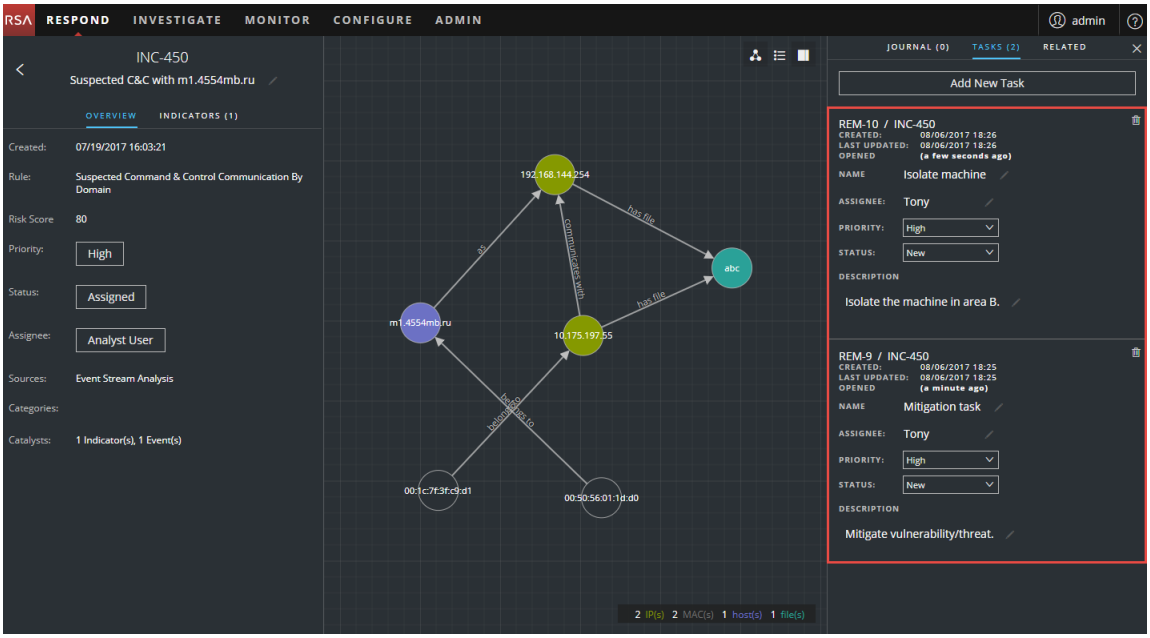
Déléguer une tâche

Vous pouvez supprimer une tâche, si, par exemple, vous l'avez créée par erreur ou trouvez qu'elle n'est pas nécessaire. Vous pouvez supprimer une tâche à partir d'un incident et dans la vue Liste de tâches. Dans la vue Liste de tâches, vous pouvez supprimer plusieurs tâches en même temps.

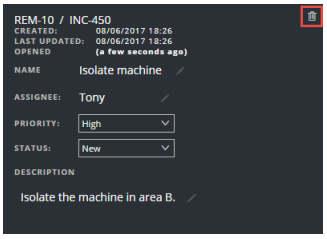
Pour supprimer une tâche à partir d'un incident :

1. Accédez à **RÉPONDRE > Incidents**.
   La vue Liste d'incidents affiche la liste de tous les incidents.
2. Localisez l'incident qui a besoin d'une mise à jour de tâche, puis cliquez sur le lien dans le champ **ID** ou **NOM**.
   La vue Détails de l'incident s'ouvre.
3. Dans la barre d'outils en haut à droite de la vue, sélectionnez ◘.
   Le panneau Journal s'ouvre.
4. Sélectionnez l'onglet TÂCHES.

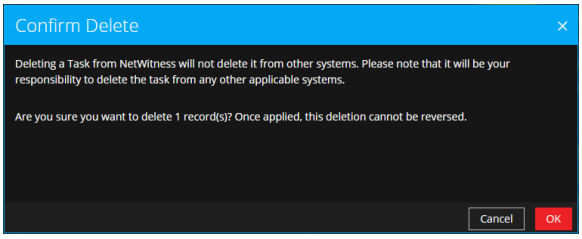
5. Dans le panneau Tâches, vous voyez les tâches créées pour l'incident.



6. Cliquez sur 🗑 à droite de la tâche que vous désirez supprimer.



7. Confirmez la suppression de la tâche et cliquez sur **OK**.

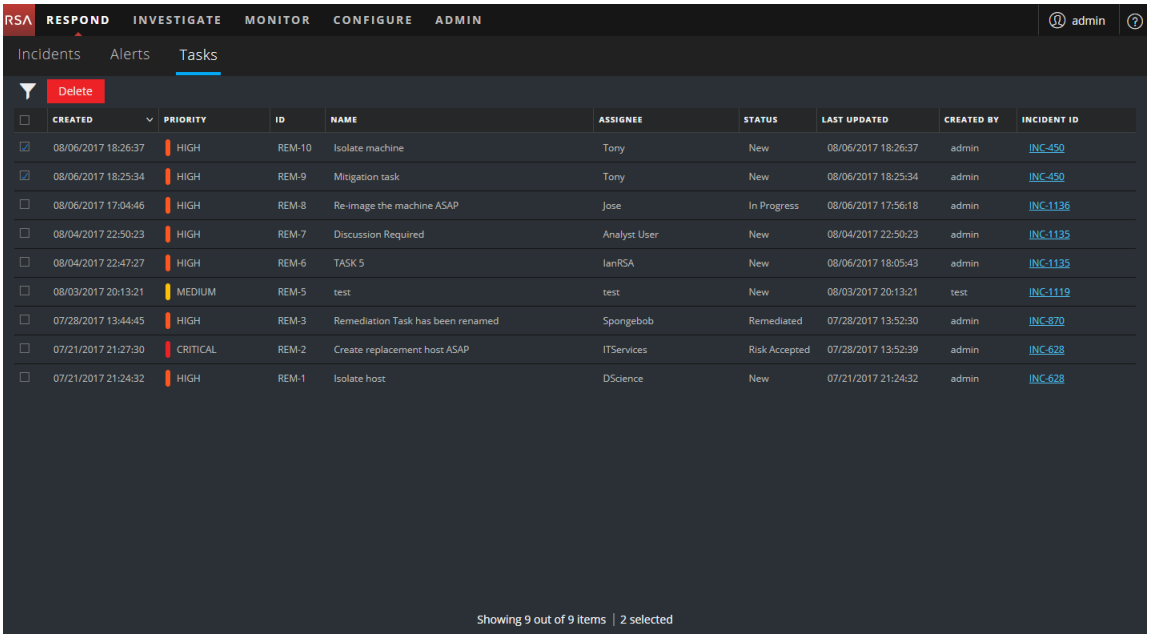


La tâche est supprimée de NetWitness Suite. La suppression de tâches depuis NetWitness Suite ne les supprime pas des autres systèmes.

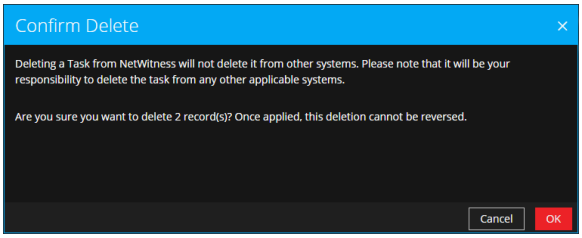
Pour supprimer des tâches dans la liste des tâches :

1. Accédez à **RÉPONDRE > Tâches**.
   La vue Liste de tâches affiche la liste de toutes les tâches d'incidents.

2. Dans la liste des tâches, sélectionnez les tâches que vous souhaitez supprimer, puis cliquez sur **Supprimer**.



3. Confirmez la suppression des tâches et cliquez sur **OK**.



Les tâches sont supprimées de NetWitness Suite. La suppression de tâches depuis NetWitness Suite ne les supprime pas des autres systèmes.

Clore un incident

Lorsque vous parvenez à une solution après avoir procédé à une enquête sur un incident et avoir corrigé ce dernier, vous le clôturez.

1. Accédez à **RÉPONDRE > Incidents**.
2. Dans la vue Liste d'incidents, sélectionnez l'incident que vous souhaitez fermer, puis cliquez sur **Modifier l'état**.
3. Dans la liste déroulante, sélectionnez **Clôturé**.
   Vous verrez une notification de modification réussie. L'incident est désormais clôturé. Vous ne pouvez pas modifier la priorité ou la personne affectée d'un incident clos.

Remarque : Vous pouvez également fermer un incident dans le panneau Présentation. Vous pouvez fermer plusieurs incidents en même temps dans la vue Liste d'incidents. Modifier l'état des incidents fournit des informations supplémentaires.

Vérifier les alertes

NetWitness Suite vous permet d'afficher une liste consolidée des alertes de menace générées à partir de plusieurs sources dans un emplacement unique. Vous pouvez trouver ces alertes dans la vue RÉPONDRE > Alertes. La source des alertes peut être les règles de corrélation ESA, ESA Analytics, NetWitness Endpoint, Malware Analysis, Reporting Engine et autres. Vous pouvez voir la source d'origine des alertes, la gravité des alertes et d'autres détails.

Remarque : les alertes de règle de corrélation ESA ne se trouvent QUE dans la vue RÉPONDRE > Alertes.

Pour mieux gérer un grand nombre d'alertes, vous avez la possibilité de filtrer la liste d'alertes selon des critères que vous spécifiez, par exemple la gravité, la plage horaire et la source de l'alerte. Par exemple, vous souhaiterez peut-être filtrer les alertes pour afficher uniquement celles possédant un niveau de gravité entre 90 et 100 qui ne font pas déjà partie d'un incident. Vous pouvez ensuite sélectionner un groupe d'alertes pour créer un incident ou l'ajouter à un incident existant.

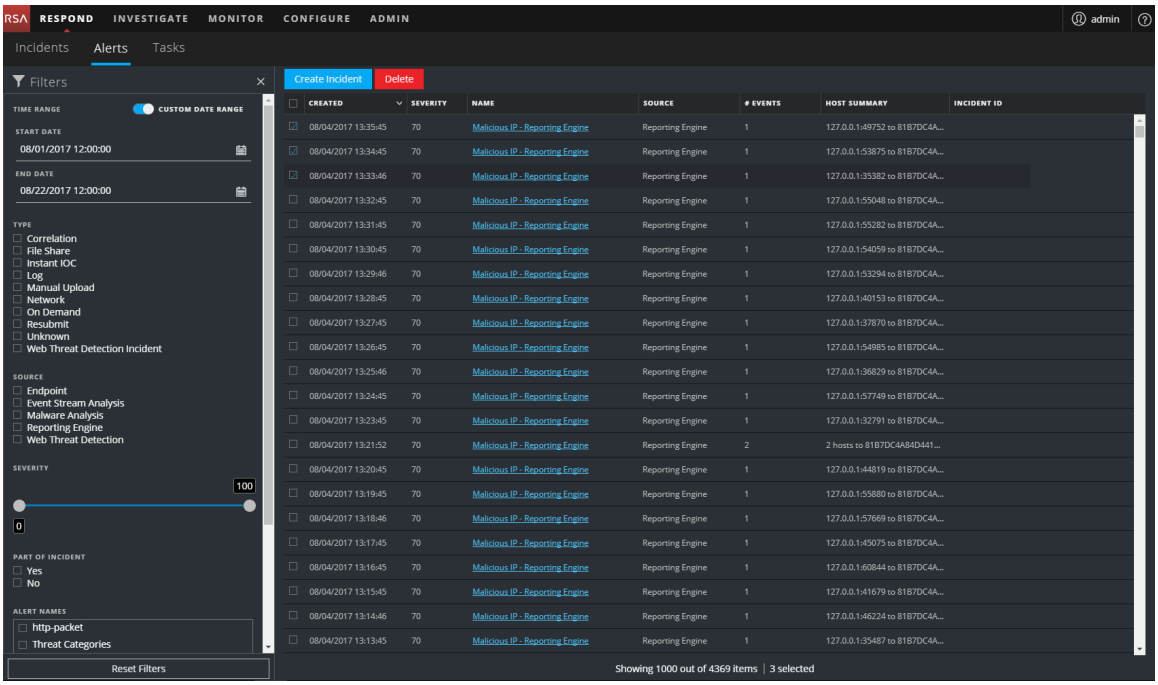
Vous pouvez effectuer les procédures suivantes afin de vérifier et de gérer les alertes :

- Afficher les alertes
- Filtrer la liste des alertes
- Supprimer Mes filtres de la liste des alertes
- Afficher les informations récapitulatives relatives aux alertes
- Afficher les détails relatifs à l'événement pour une alerte
- Examiner les événements
- Créer un incident manuellement
- Vérifier les alertes
- Supprimer les alertes

Afficher les alertes

Dans la vue Liste des alertes, vous pouvez parcourir les différentes alertes de plusieurs sources, les filtrer et les regrouper pour créer des incidents. Cette procédure vous indique comment accéder à la liste des alertes.

1. Accédez à **RÉPONDRE > Alertes**.
   La vue Liste des alertes affiche une liste de toutes les alertes NetWitness Suite.



2. Faites défiler la liste des alertes, qui affiche des informations de base sur chaque alerte, comme décrit dans le tableau suivant.

Colonne	Description
DATE DE CRÉATION	Affiche la date et l'heure auxquelles l'alerte a été enregistrée dans le système source.
GRAVITÉ	Affiche le niveau de gravité de l'alerte. Les valeurs sont comprises entre 1 et 100.
NOM	Affiche une description de base de l'alerte.
SOURCE	Affiche la source originale de l'alerte. La source des alertes peut être NetWitness Endpoint, Malware Analysis, Event Stream Analysis (règles de corrélation ESA), l'analytique ESA, Reporting Engine, la détection des cybermenaces, et autres.

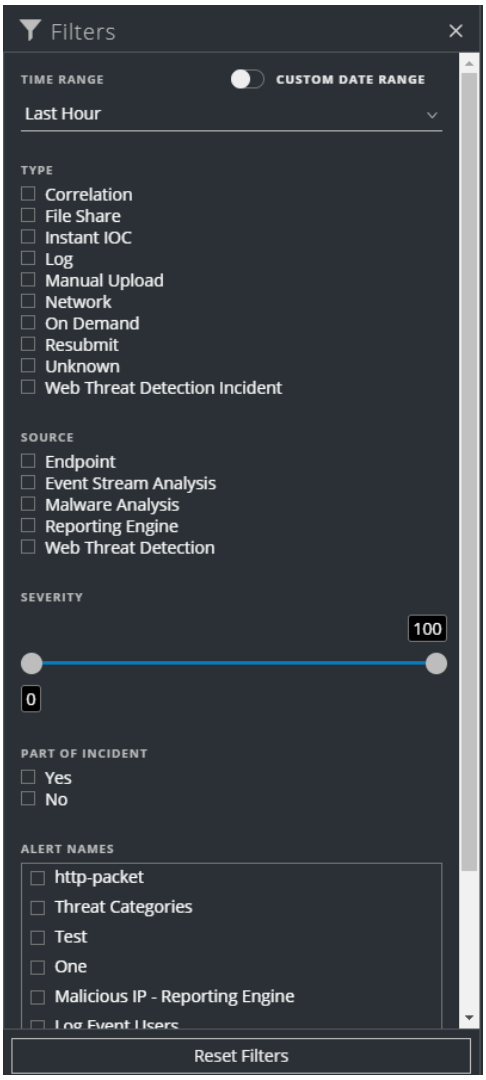
Colonne	Description
NOMBRE D'ÉVÉNEMENTS	Indique le nombre d'événements contenus dans une alerte. Cela varie en fonction de la source de l'alerte. Par exemple, les alertes NetWitness Endpoint et Malware Analysis ont toujours un événement. Pour certains types d'alertes, un nombre élevé d'événements peut signifier que l'alerte est plus risquée.
RÉCAPITULATIF DE L'HÔTE	Affiche les détails relatifs à l'hôte tels que le nom de l'hôte d'où l'alerte a été déclenchée. Les détails peuvent inclure des informations sur les hôtes source et cible dans une alerte . Certaines alertes peuvent décrire des événements sur plusieurs hôtes.
ID d'incident	Affiche l'ID d'incident de l'alerte. S'il n'y a pas d'ID d'incident, cela signifie que l'alerte ne fait pas partie d'un incident. Vous pouvez alors créer un incident pour inclure cette alerte ou l'alerte peut être ajoutée à un incident existant.

Au bas de la liste, vous voyez le nombre d'alertes sur la page en cours et le nombre total d'alertes. Par exemple : **Affichage de 377 éléments sur 377**

Filtrer la liste des alertes

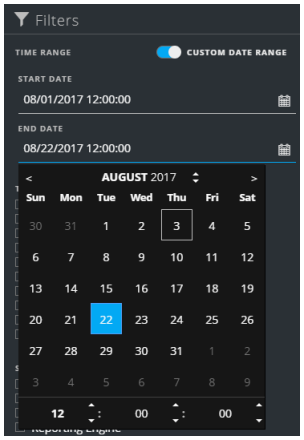
Le nombre de tâches dans la Liste des alertes peut être très volumineux, ce qui complexifie la recherche d'alertes particulières. Le Filtre vous permet d'afficher les alertes que vous souhaitez afficher, par exemple les alertes d'une source donnée, les alertes d'un niveau de gravité spécifique, les alertes qui ne font pas partie d'un incident, etc.

1. Accédez à **RÉPONDRE > Alertes**.
   Le panneau Filtres s'affiche à gauche de la liste des alertes. Si vous ne voyez pas le panneau Filtres, dans la barre d'outils de la vue Liste des alertes, cliquez sur afin d'ouvrir le panneau Filtres.



2. Dans le panneau Filtres, sélectionnez une ou plusieurs options pour filtrer la liste des alertes :
   - **PLAGE TEMPORELLE** : Vous pouvez sélectionner une période spécifique dans la liste déroulante Période. La période est basée sur la date de réception des alertes. Par exemple, si vous sélectionnez Dernière heure, vous verrez les alertes qui ont été créées au cours des 60 dernières minutes.
   - **PLAGE DE DATES PERSONNALISÉE** : Vous pouvez spécifier une plage de dates spécifique au lieu de sélectionner une option de période. Pour ce faire, cliquez sur le cercle blanc devant PLAGE DE DATES PERSONNALISÉE pour afficher les champs

Date de début et Date de fin. Sélectionnez les dates et heures dans le calendrier.



- **TYPE** : Sélectionnez le type d'événements dans l'alerte à afficher, par exemple, les logs, sessions réseau, etc.
- **SOURCE** : Sélectionnez une ou plusieurs sources pour afficher les alertes déclenchées par les sources sélectionnées. Par exemple, pour afficher les alertes NetWitness Endpoint uniquement, sélectionnez Endpoint en tant que source.
- **GRAVITÉ** : Sélectionnez le niveau de gravité des alertes à afficher. Les valeurs sont comprises entre 1 et 100. Par exemple, pour vous concentrer tout d'abord sur les alertes possédant la gravité la plus élevée, affichez uniquement les alertes avec un niveau de gravité de 90 à 100.
- **PARTIE DE L'INCIDENT** : pour afficher uniquement les alertes qui ne font pas partie d'un incident, sélectionnez **Non**. Pour afficher uniquement les alertes qui font partie d'un incident, sélectionnez **Oui**. Par exemple, lorsque vous êtes prêt à créer un incident à partir d'un groupe d'alertes, vous pouvez sélectionner Non pour afficher uniquement les alertes qui ne font pas déjà partie d'un incident.
- **NOMS DES ALERTES** : Sélectionnez le nom de l'alerte à afficher. Vous pouvez utiliser ce filtre pour rechercher toutes les alertes générées par une règle ou une source spécifique, par exemple, IP malveillantes - Reporting Engine.

La Liste des alertes affiche une liste d'alertes qui répondent à vos critères de sélection. Vous pouvez voir le nombre d'éléments dans votre liste filtrée en bas de la liste des alertes. Par exemple : **Affichage de 30 élément(s) sur 30**

3. Si vous souhaitez fermer le panneau Filtres, cliquez sur **X**. Vos filtres restent en place jusqu'à ce que vous les supprimiez.

Supprimer Mes filtres de la liste des alertes

NetWitness Suite mémorise vos sélections de filtre dans la liste d'alertes. Vous pouvez supprimer vos sélections de filtre lorsque vous n'en avez plus besoin. Par exemple, si vous ne voyez pas le nombre d'alertes que vous devriez voir ou si vous souhaitez afficher toutes les alertes dans la liste des alertes, vous pouvez réinitialiser les filtres.

1. Accédez à **RÉPONDRE > Alertes**.

   Le panneau Filtres s'affiche à gauche de la liste des alertes. Si vous ne voyez pas le panneau Filtres, dans la barre d'outils de la vue Liste des alertes, cliquez sur afin d'ouvrir le panneau Filtres.

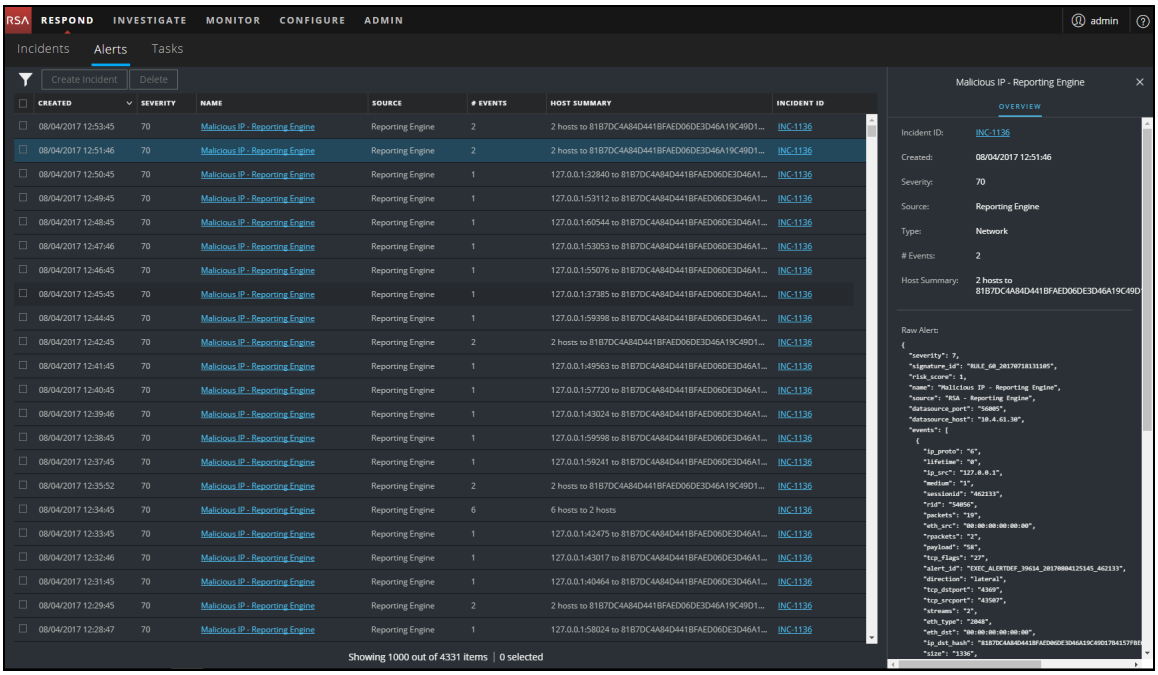
2. Au bas du panneau Filtres, cliquez sur **Réinitialiser les filtres**.

Afficher les informations récapitulatives relatives aux alertes

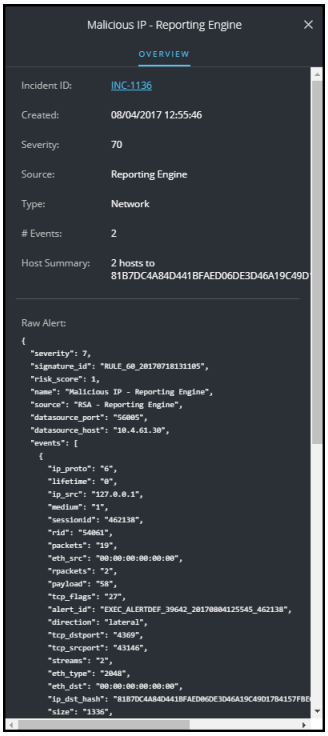
En plus de voir des informations de base sur une alerte, vous pouvez également afficher des métadonnées d'alerte brutes dans le panneau Présentation.

1. Dans la liste Alertes, cliquez sur l'alerte que vous voulez afficher.

   Le panneau Présentation des alertes s'affiche à droite de la liste Tâches.

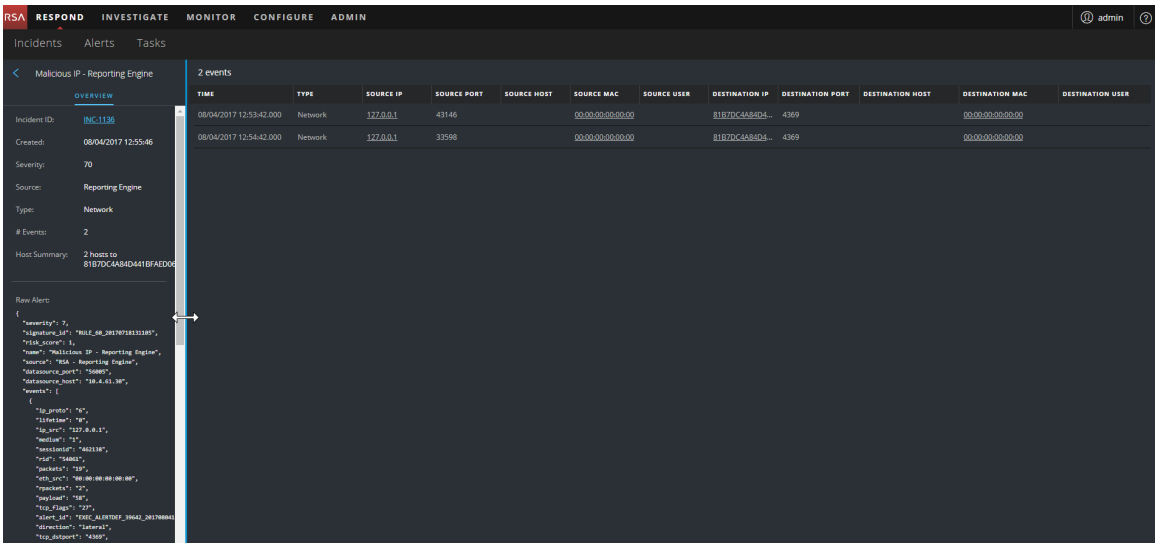


2. Dans la section Alerte brute, vous pouvez faire défiler pour afficher les métadonnées de l'alerte brute.



Afficher les détails relatifs à l'événement pour une alerte

Une fois que vous avez révisé les informations générales sur l'alerte dans la vue Liste des alertes, vous pouvez accéder à la vue Détails de l'alerte pour plus d'informations afin de déterminer l'action requise. Une alerte contient un ou plusieurs événements. Dans la vue Détails de l'alerte, vous pouvez effectuer une recherche verticale sur une alerte afin d'obtenir des informations supplémentaires et d'examiner davantage l'alerte. La figure suivante est un exemple d'événements de la vue Détails de l'alerte.



Le panneau Présentation sur la gauche contient les mêmes informations pour une alerte que le panneau Présentation de la vue Liste des alertes.

Le panneau Événements sur la droite présente des informations sur les événements dans l'alerte, comme l'heure de l'événement, l'adresse IP source, l'adresse IP de destination, l'adresse IP du détecteur, l'utilisateur source, l'utilisateur de destination et les informations de fichier sur les événements. La quantité d'informations répertoriées varie selon le type d'événement.

Il existe deux types d'événements :

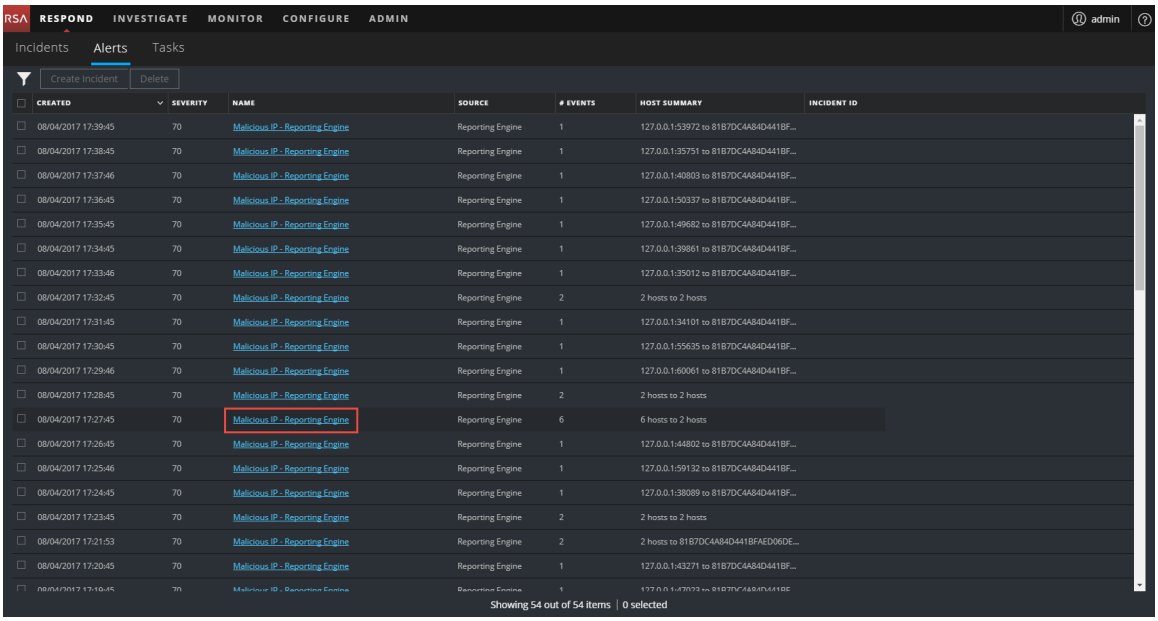
- Une transaction entre deux machines (une source et une destination)
- Une anomalie détectée sur une seule machine (un détecteur)

Certains événements ne disposent que d'un détecteur. Par exemple, NetWitness Endpoint détecte des malware sur votre machine. D'autres événements posséderont une source et une destination. Par exemple, les données de paquets affichent une communication entre votre ordinateur et une commande et le domaine de contrôle (C2).

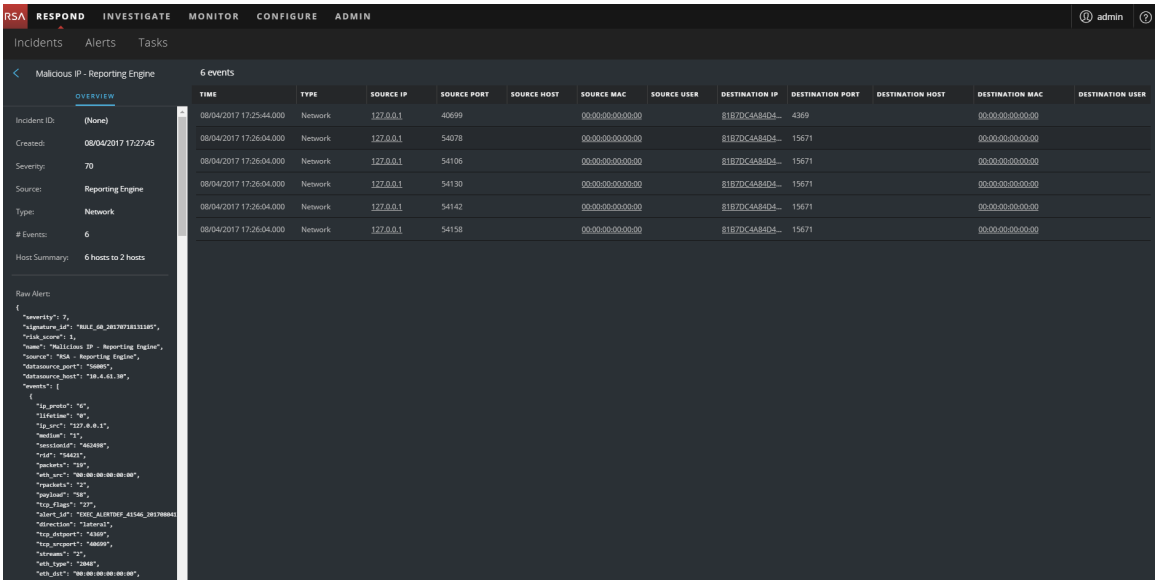
Vous pouvez effectuer une recherche verticale dans un événement pour obtenir des données détaillées à son sujet.

Pour afficher les détails relatifs à l'événement pour une alerte :

1. Pour afficher les détails relatifs à l'événement pour une alerte, dans la vue Liste d'alertes, choisissez une alerte à afficher, puis cliquez sur le lien dans la colonne NOM de cette alerte.



La vue Détails des alertes affiche le panneau Présentation sur la gauche et le panneau Événements sur la droite.



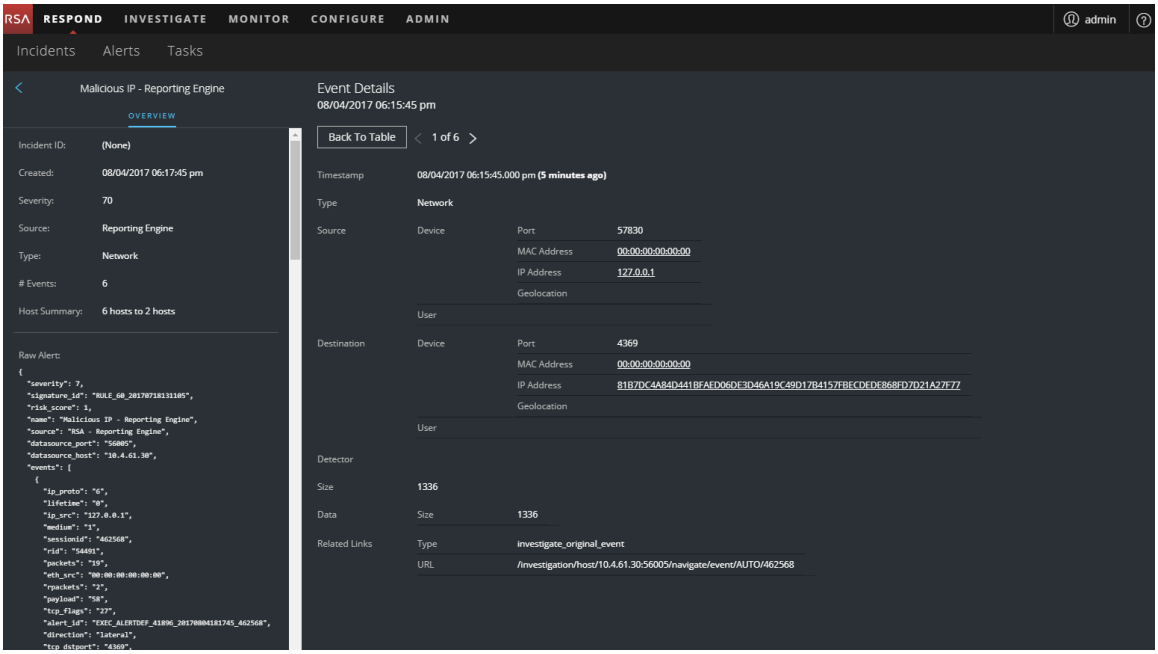
Le volet Événements présente une liste d'événements avec des informations sur chaque événement. Le tableau suivant présente certaines colonnes qui peuvent s'afficher dans la liste Événements (Table d'événements).

Colonne	Description
HEURE	Affiche l'heure à laquelle l'événement s'est produit.
TYPE	Affiche le type d'alerte, comme Log et Réseau.

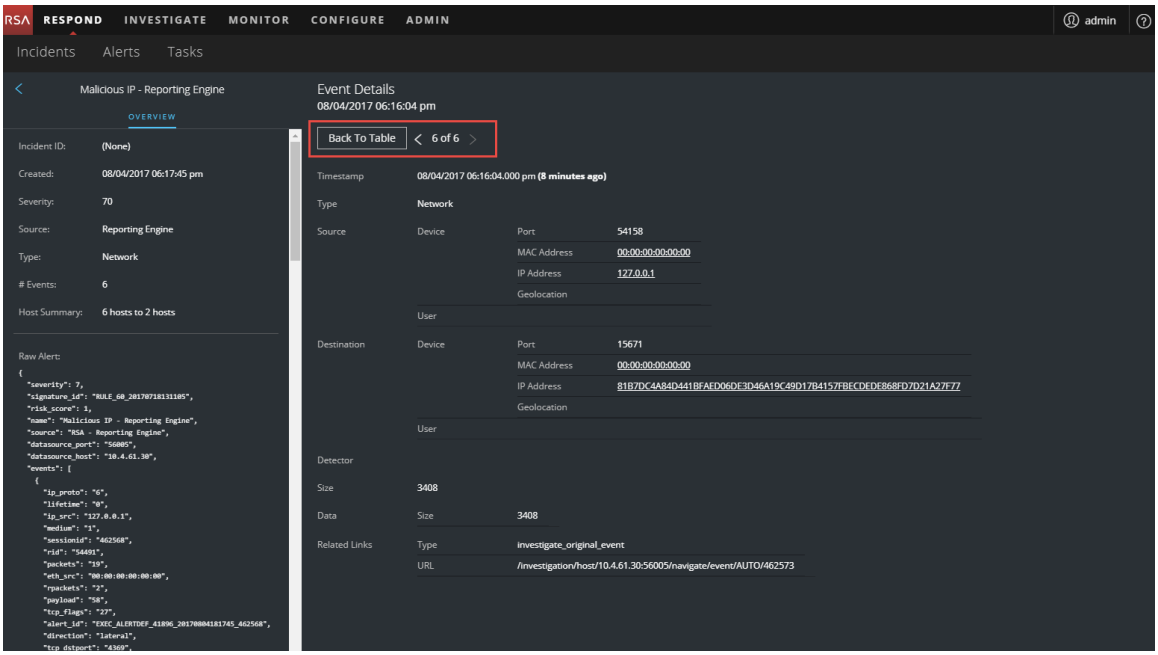
Colonne	Description
IP SOURCE	Affiche l'adresse IP source s'il y a eu une transaction entre les deux machines.
IP DE DESTINATION	Affiche l'adresse IP de destination s'il y a eu une transaction entre les deux machines
IP DÉTECTEUR	Affiche l'adresse IP de la machine sur laquelle une anomalie a été détectée.
UTILISATEUR SOURCE	Affiche l'utilisateur de la machine source.
UTILISATEUR DE DESTINATION	Affiche l'utilisateur de la machine de destination.
NOM DE FICHIER	Affiche le nom du fichier si un fichier est impliqué dans l'événement.
HACHAGE DE FICHIER	Présente un hachage du contenu du fichier.

S'il existe un seul événement dans la liste, vous verrez les détails de l'événement pour cet événement au lieu d'une liste.

2. Cliquez sur un événement dans la liste Événements pour afficher les détails Événement.
   Cet exemple montre les détails de l'événement pour le premier événement dans la liste.



3. Utilisez la navigation de la page à droite du bouton Revenir à la table pour afficher les autres événements. Cet exemple montre les détails de l'événement pour le dernier événement dans la liste.



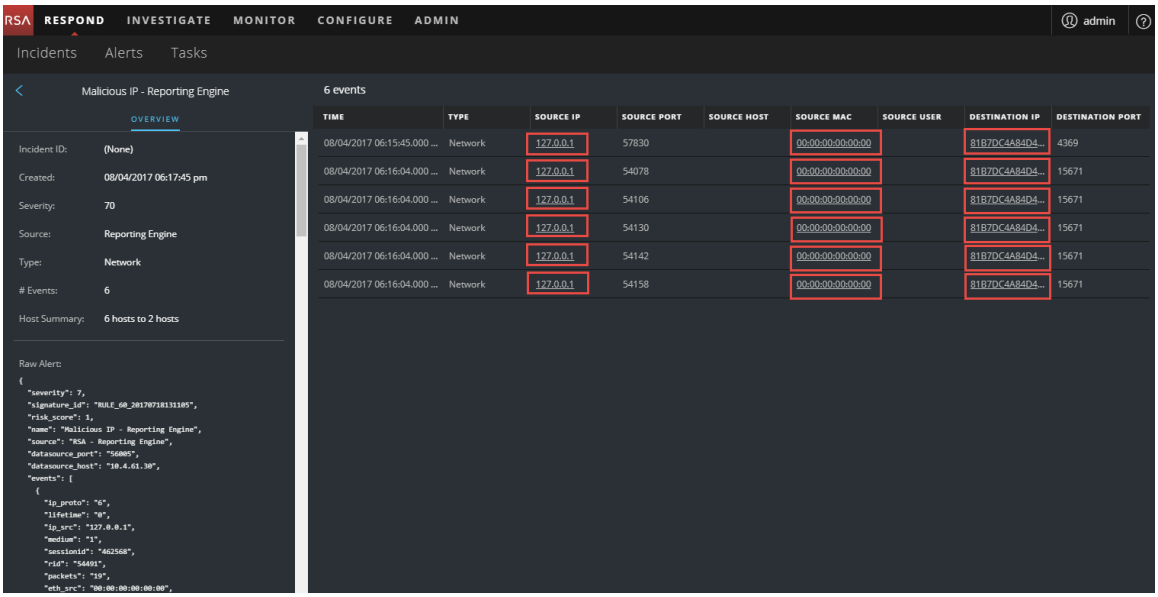
Reportez-vous à la section Vue Détails relatifs aux alertes pour obtenir des informations détaillées sur les données d'événement répertoriées dans le panneau Détails de l'alerte.

Examiner les événements

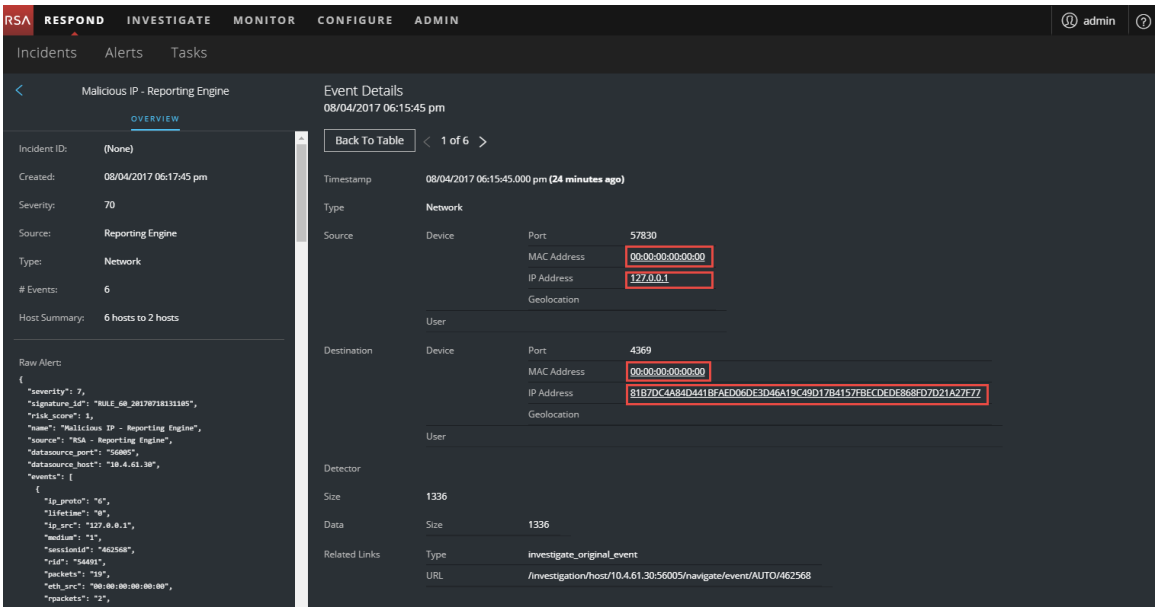
Pour examiner davantage les événements, vous trouverez des liens vers des informations contextuelles supplémentaires. Vous disposez ensuite d'options en fonction de votre sélection.

Afficher les informations contextuelles

Dans la vue Détails de l'alerte, vous pouvez voir les entités soulignées dans le panneau Événements. Une entité soulignée est considérée comme une entité du service Context Hub et propose des informations contextuelles supplémentaires. La figure suivante illustre les entités soulignées dans la liste Événements.



La figure suivante illustre les entités soulignées dans les Détails de l'événement.

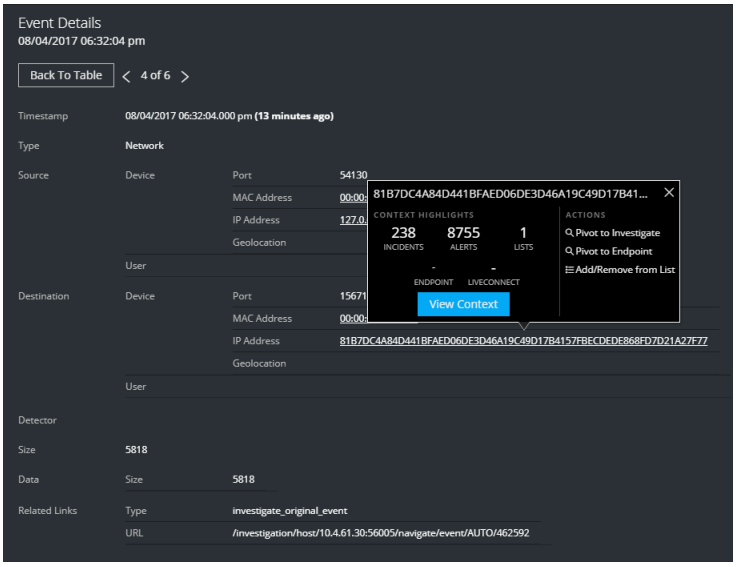


Le service Context Hub est préconfiguré avec les champs méta mappés aux entités. NetWitness Respond et Investigation utilisent ces mappages par défaut pour la recherche contextuelle. Pour plus d'informations sur l'ajout de clés méta, consultez « Configurer les paramètres pour une source de données » dans le *Guide de configuration de Context Hub*.

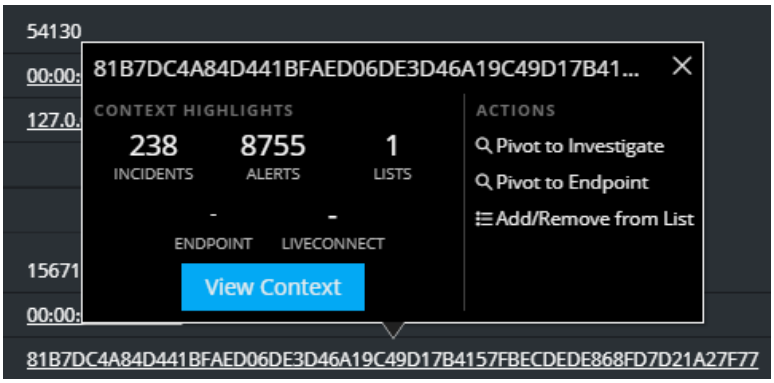
Attention : Pour que la recherche contextuelle fonctionne correctement dans les vues Répondre et Enquêter, RSA vous recommande, lorsque vous mappez des clés méta dans l'onglet **ADMIN > SYSTÈME > Procédures d'enquête > Recherche contextuelle**, d'ajouter uniquement les clés méta aux mappages de clé méta, et non aux champs dans MongoDB. Par exemple, ip.address est une clé méta et ip_address n'est pas une clé méta (il s'agit d'un champ dans MongoDB).

Pour afficher les informations contextuelles :

1. Dans la Liste des événements ou les Détails de l'événement de la vue Détails de l'alerte, survolez une entité soulignée.
   Une info-bulle contextuelle s'affiche avec un bref résumé du type de données contextuelles disponible pour l'entité sélectionnée.



   L'info-bulle contextuelle comporte deux sections : Points forts du contexte et actions.



   Les informations contenues dans la section **Points forts du contexte** vous aident à déterminer les actions que vous devez entreprendre. Elles indiquent le nombre d'incidents et les alertes associées. En fonction de vos données, vous pourrez peut-être cliquer sur ces éléments numérotés pour plus d'informations. L'exemple ci-dessus présente 238 incidents associés et 8 755 alertes associées, ainsi qu'1 liste Context Hub associée.

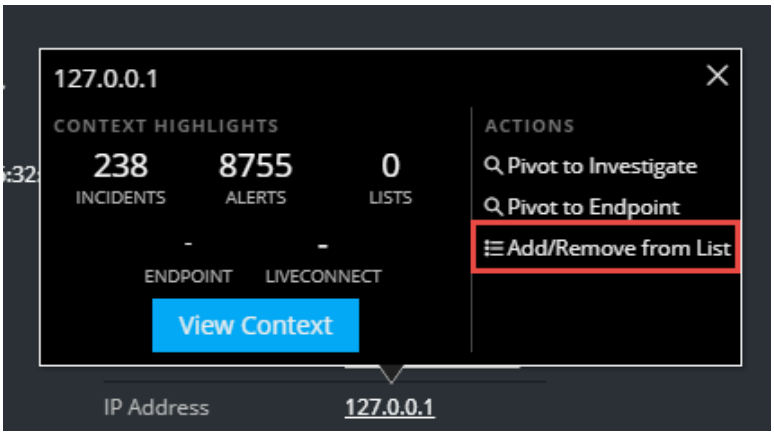
   La section **Actions** répertorie les actions disponibles. Dans l'exemple ci-dessus, les options Pivoter vers la fonction Enquêter, Pivot vers le point de terminaison, et Ajouter à la liste/Supprimer de la liste sont disponibles.

2. Pour obtenir plus de détails sur l'entité sélectionnée, cliquez sur le bouton **Afficher le contexte**.
   Le panneau Contexte s'ouvre et affiche toutes les informations relatives à l'entité.
   Le Panneau Recherche contextuelle - Vue Répondre fournit des informations supplémentaires.

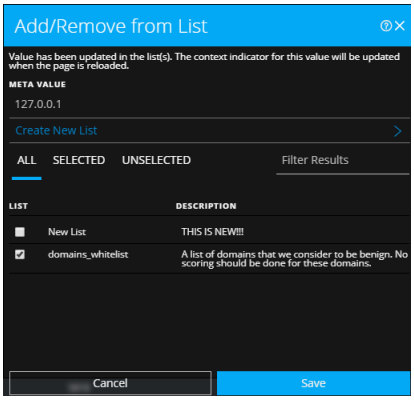
Ajouter une entité à une liste blanche

Vous pouvez ajouter n'importe quelle entité soulignée à une liste, comme une liste blanche ou noire, à partir d'une info-bulle de contexte. Par exemple, pour réduire les faux positifs, vous pouvez ajouter à la liste blanche un domaine souligné pour l'exclure des entités associées.

1. Dans la vue Détails de l'alerte, Liste d'événements ou Détails de l'événement, survolez l'entité soulignée que vous souhaitez ajouter à une liste Context Hub.
   Une info-bulle contextuelle s'affiche et présente les actions disponibles.



2. Dans la section **Actions** de l'info-bulle, cliquez sur **Ajouter à la liste/Supprimer de la liste**.
   La boîte de dialogue Ajouter à la liste/Supprimer de la liste affiche les listes disponibles.



3. Sélectionnez une ou plusieurs listes, puis cliquez sur **Enregistrer**.
   L'entité s'affiche dans les listes sélectionnées.

Boîte de dialogue Ajouter à la liste/Supprimer de la liste fournit des informations supplémentaires.

Créer une liste blanche

Vous pouvez créer une liste blanche dans Context Hub de la même manière que vous la créeriez dans la vue Détails de l'incident. Reportez-vous à la section Créer une liste.

Pivoter vers le point de terminaison NetWitness

Si l'application de client Thick NetWitness Endpoint est installée, vous pouvez la démarrer via l'info-bulle de contexte. À partir de là, vous pouvez mener davantage l'enquête sur une adresse IP suspecte, un hôte ou une adresse MAC.

1. Dans la Liste des événements ou les Détails de l'événement de la vue Détails de l'alerte, survolez une entité soulignée pour accéder à une info-bulle de contexte.
2. Dans la section **ACTIONS** de l'info-bulle, sélectionnez **Pivoter vers le point de terminaison**.
   L'application NetWitness Endpoint s'ouvre en dehors de votre navigateur Web.

Pour plus d'informations, consultez le *NetWitness EndpointGuide d'utilisation*.

Pivoter vers Investigation

Pour une procédure d'enquête plus approfondie de l'incident, vous pouvez accéder à la vue Procédure d'enquête.

1. Dans la Liste des événements ou les Détails de l'événement de la vue Détails de l'alerte, survolez une entité soulignée pour accéder à une info-bulle de contexte.
2. Dans la section **ACTIONS** de l'info-bulle, sélectionnez **Pivoter vers la fonction Enquêter**.
   Enquêter - vue Naviguer s'ouvre, ce qui vous permet d'effectuer une procédure d'enquête plus approfondie.

Pour plus d'informations, consultez le *Guide d'utilisation Investigation et Malware Analysis*.

Créer un incident manuellement

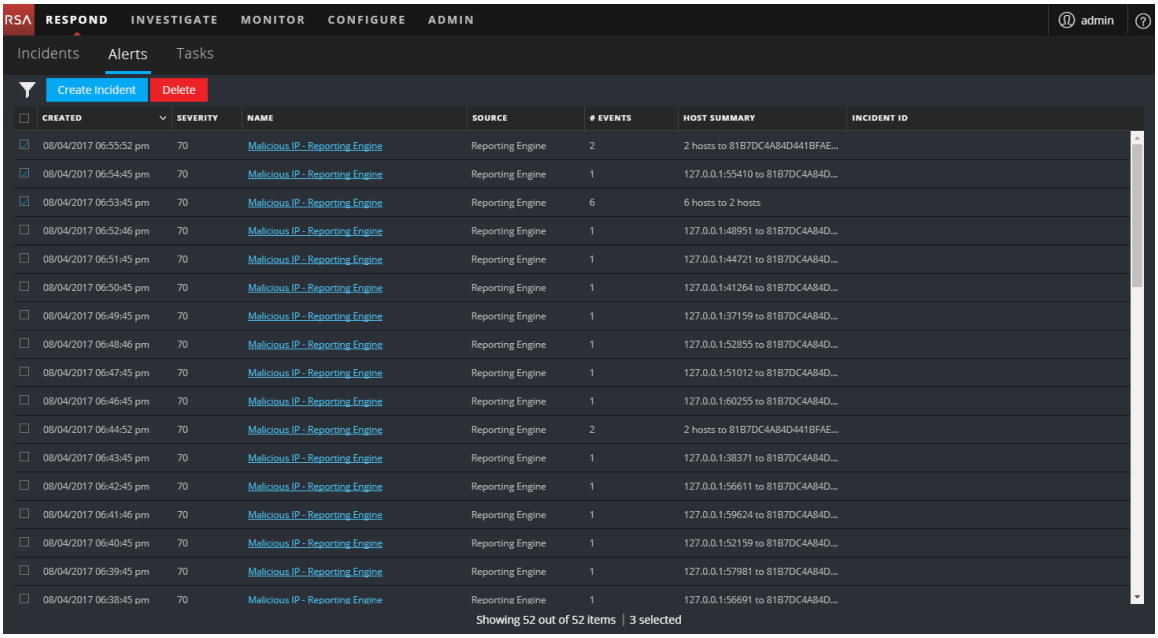
Vous pouvez créer des incidents manuellement à partir des alertes dans la vue Liste des alertes. Les alertes que vous sélectionnez ne peuvent pas faire partie d'un autre incident. Les incidents créés manuellement à partir d'alertes prennent la priorité Basse par défaut, mais vous pouvez modifier la priorité après la création. Vous ne pouvez pas ajouter de catégories à des incidents créés manuellement.

Remarque : Les incidents peuvent être créés manuellement ou automatiquement. Une alerte ne peut être associée qu'à un seul incident. Vous pouvez créer des règles d'agrégation pour analyser les alertes collectées et les regrouper en incidents en fonction des règles auxquelles elles correspondent. Pour plus d'informations, reportez-vous à la rubrique « Création d'une règle d'agrégation pour les alertes » dans le *NetWitness Respond Guide de Configuration.*

Pour créer un incident manuellement :

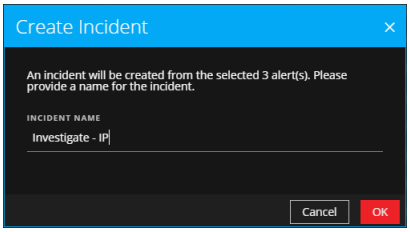
1. Accédez à **RÉPONDRE > Alertes**.
2. Sélectionnez une ou plusieurs alertes dans la Liste des alertes.

   Remarque : Si vous sélectionnez des alertes qui n'ont pas d'ID d'incident, le bouton **Créer un incident** s'active. Si l'alerte fait déjà partie d'un incident, le bouton est désactivé. Vous pouvez filtrer les alertes qui n'appartiennent à aucun incident en définissant l'option **PARTIE INTÉGRANTE DE L'INCIDENT** sur **Non** dans le panneau Filtres.

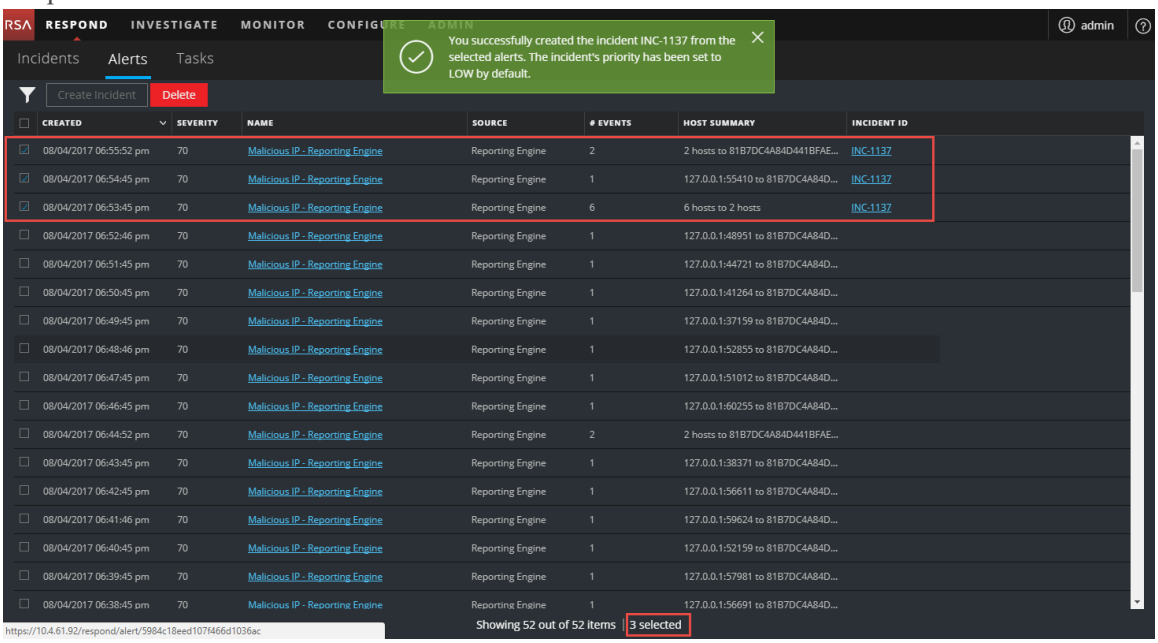


3. Cliquez sur **Créer un incident**.

   La boîte de dialogue **Créer un incident** s'affiche.



4. Dans le champ **NOM DE L'INCIDENT**, entrez un nom pour identifier l'incident. Par exemple, Enquêter - IP.
5. Cliquez sur **OK**.

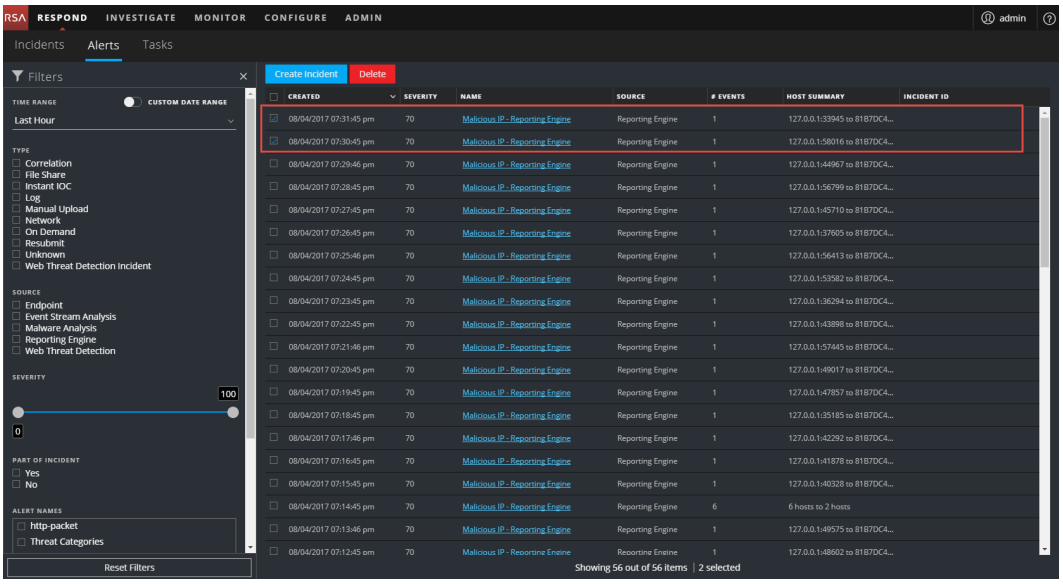


Vous verrez un message de confirmation indiquant qu'un incident a été créé à partir des alertes sélectionnées. Le nouvel ID d'incident s'affiche sous la forme d'un lien dans la colonne ID D'INCIDENT des alertes sélectionnées. Si vous cliquez sur le lien, il vous mène à la vue Détails de l'incident pour cet incident, où vous pouvez mettre à jour les informations telles que la Priorité, de faible à élevée.

Supprimer les alertes

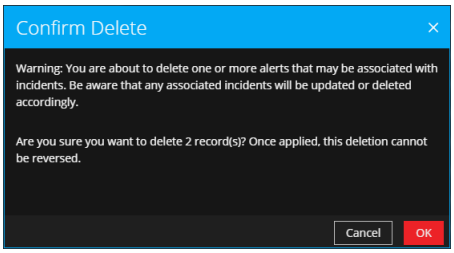
Avec les autorisations appropriées, par exemple Administrateurs et Agents de confidentialité des données, les utilisateurs peuvent supprimer les alertes. Cette procédure est utile lorsque vous souhaitez supprimer les alertes inutiles ou non pertinentes. La suppression de ces alertes libèrent de l'espace disque.

1. Accédez à **RÉPONDRE > Alertes**.
   La vue Liste des alertes affiche une liste de toutes les alertes NetWitness Suite.
2. Dans la liste des alertes, sélectionnez les alertes que vous souhaitez supprimer, puis cliquez sur **Supprimer**.



Si vous n’avez pas l’autorisation de supprimer des alertes, vous ne verrez pas le bouton Supprimer.

3. Confirmez la suppression des alertes et cliquez sur **OK**.



Les alertes sont supprimées de NetWitness Suite. Si une alerte supprimée est la seule alerte figurant dans un incident, l'incident est aussi supprimé. Si une alerte supprimée n'est pas la seule alerte figurant dans un incident, l'incident est mis à jour pour refléter la suppression.

Informations de référence de NetWitness Respond

L'interface utilisateur de la vue Répondre permet d'accéder aux fonctions NetWitness Respond. Cette rubrique contient des descriptions de l'interface utilisateur ainsi que d'autres informations de référence pour aider les utilisateurs à comprendre les fonctions de NetWitness Respond.

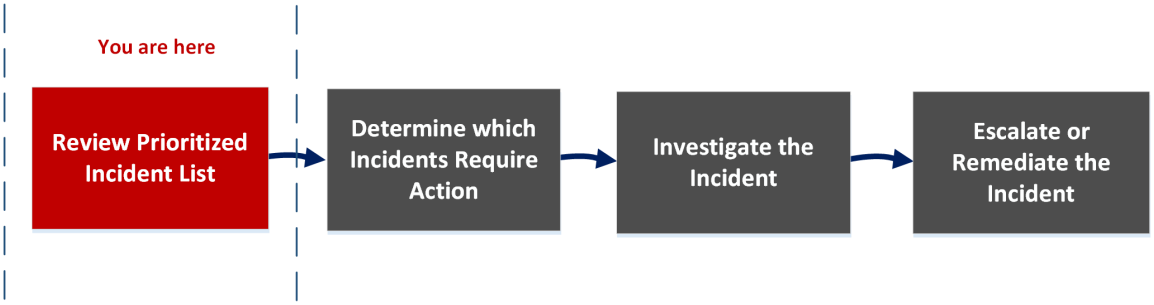
Sections

Vue Liste des incidents

La liste des incidents (RÉPONDRE > Incidents) affiche la liste hiérarchisée des résultats des incidents créés à partir de différentes sources, à l'attention des responsables de la réponse aux incidents et des analystes. Par exemple, la liste de vos résultats peut afficher les incidents créés à partir de règles ESA, NetWitness Endpoint, ou des modules d'ESA Analytics pour la détection automatisée des menaces, comme C2 pour les paquets ou les logs. Dans la liste des incidents, vous accédez facilement aux informations dont vous avez besoin pour trier et gérer rapidement les incidents jusqu'à leur résolution.

Workflow

Ce workflow montre le processus de haut niveau que les responsables de la réponse aux incidents utilisent pour répondre aux incidents dans NetWitness Suite.



Dans la liste des incidents, vous pouvez consulter la liste hiérarchisée des incidents, qui donne des informations relatives à chaque incident. Vous pouvez également modifier la personne affectée, la priorité et l'état des incidents. Étant donné que les résultats peuvent être volumineux dans la liste des incidents, vous pouvez filtrer ces incidents par période, par ID d'incident, par plage de dates personnalisée, par priorité, par état, par personne affectée et par catégorie.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Responsables de la réponse aux incidents, analystes, responsables du SOC	Afficher les incidents prioritaires*	Passer en revue la liste des incidents hiérarchisés
Responsables de la réponse aux incidents, analystes, responsables du SOC	Filtrer et trier la liste des incidents*	Filtrer la liste des incidents
Responsables de la réponse aux incidents, analystes	Afficher mes incidents*	Afficher mes incidents
Responsables de la réponse aux incidents, analystes	Attribuer les incidents à moi-même*	Attribuer les incidents à moi-même
Responsables de la réponse aux incidents, analystes, responsables du SOC	Trouver les incidents*	Trouver un incident
Responsables de la réponse aux incidents, analystes, responsables du SOC	Mettre à jour un incident.*	Faire remonter ou corriger l'incident
Responsables de la réponse aux incidents, analystes	Afficher les détails sur l'incident.	Déterminer les incidents exigeant une action
Responsables de la réponse aux incidents, analystes	Enquêter davantage sur un incident.	Enquêter sur l'incident
Responsables de la réponse aux incidents, analystes, responsables du SOC	Créer une tâche.	Faire remonter ou corriger l'incident

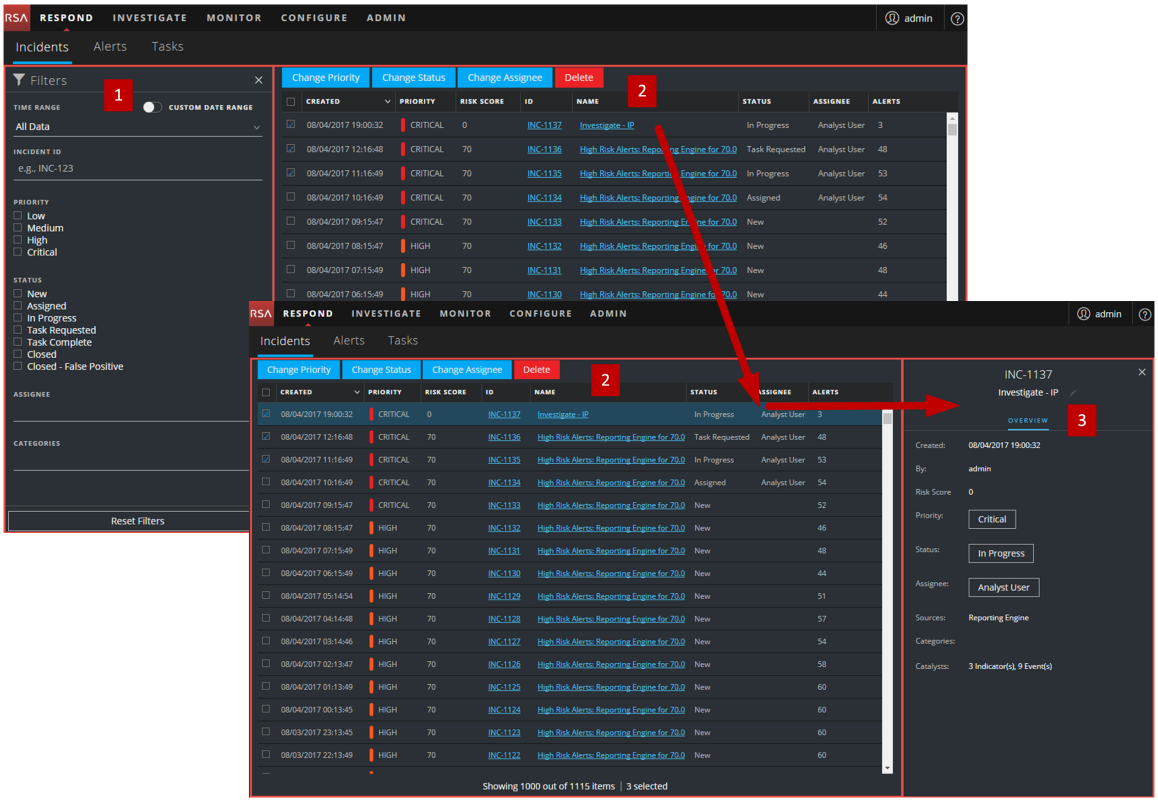
*Vous pouvez effectuer ces tâches ici (c'est-à-dire dans la liste des incidents).

Rubriques connexes

- Vue Détails sur l'incident
- Réponse aux incidents

Aperçu rapide

L'exemple suivant présente la liste des incidents initiale avec le panneau Filtres. Vous pouvez ouvrir le panneau Présentation concernant un incident en cliquant sur la Liste des incidents.



1 Panneau Filtres

2 Liste des incidents

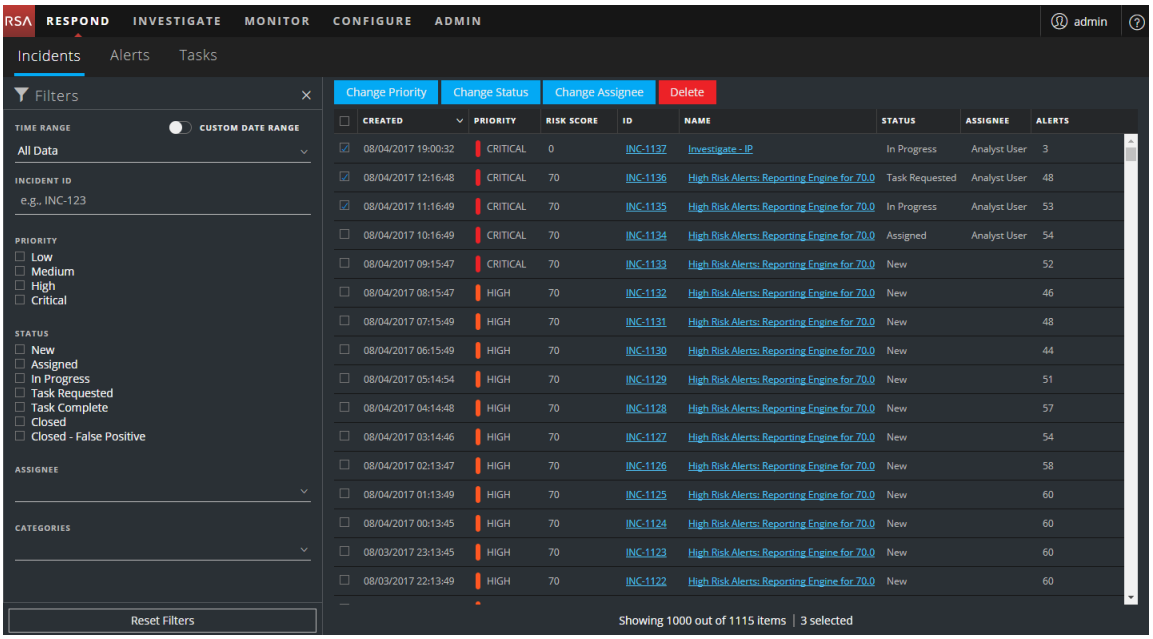
3 Panneau Présentation

Vous pouvez accéder directement à la vue Détails sur l'incident à partir de la liste des incidents en cliquant sur le lien de l'ID ou du nom. Le panneau Présentation est également disponible dans la vue Détails sur l'incident. Pour plus d'informations sur la vue Détails sur l'incident, reportez-vous à la section Vue Détails sur l'incident.

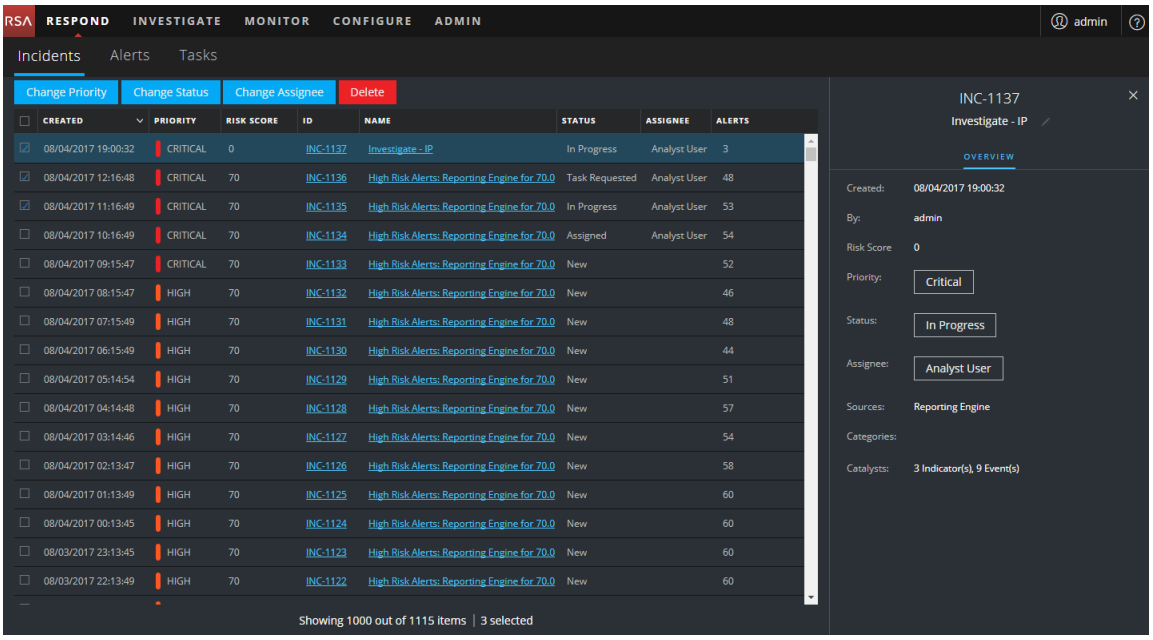
Vue Liste des incidents

Pour accéder à la liste des incidents, accédez à **RÉPONDRE > Incidents**. La liste des incidents affiche tous les incidents. La liste des incidents se compose du panneau Filtres, de la liste des incidents et du panneau Présentation des incidents.

La figure suivante illustre le panneau Filtres sur la gauche et la liste des incidents sur la droite.

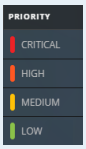


La figure suivante illustre la Liste des incidents sur la gauche et le panneau Présentation des incidents sur la droite.



Liste des incidents

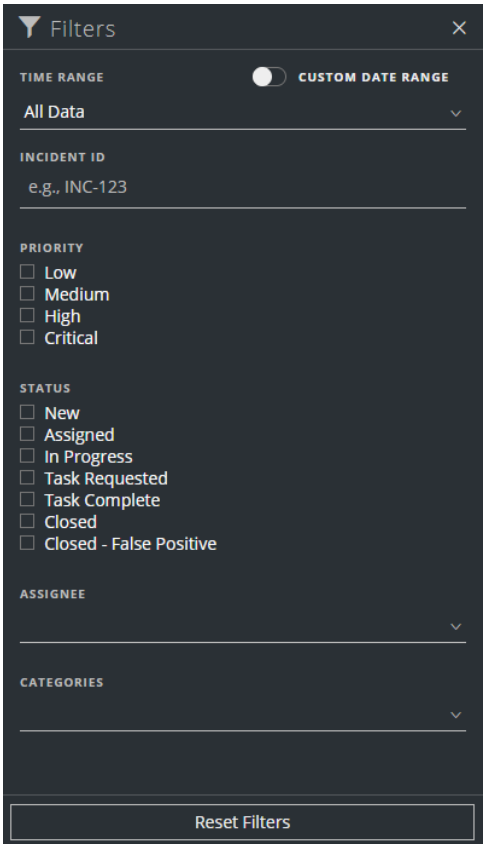
La liste des incidents répertorie tous les incidents sous une forme hiérarchisée. Vous pouvez filtrer cette liste pour afficher uniquement les incidents intéressants.

Colonne	Description
CRÉÉ	Affiche la date de création de l'incident.
PRIORITÉ	Affiche la priorité de l'incident. La priorité peut être critique, élevée, moyenne ou faible. La priorité est désignée par un code couleur où le rouge indique un incident **critique**, l'orange un incident à risque **élevé**, le jaune un incident à risque **moyen** et le vert un incident à **faible** risque. Par exemple : 
SCORE DE RISQUE	Affiche le score de risque de l'incident. Le score de risque indique le risque de l'incident, calculé via un algorithme et compris entre 0 et 100. 100 désigne le score de risque le plus élevé.
ID	Indique le numéro d'un incident créé automatiquement. Un numéro unique que vous pouvez utiliser pour effectuer le suivi de l'incident est attribué à chaque incident.
NOM	Affiche le nom de l'incident. Le nom de l'incident est dérivé de la règle utilisée pour déclencher l'incident. Cliquez sur le lien pour accéder à la vue Détails sur l'incident de l'incident sélectionné.
ÉTAT	Affiche l'état de l'incident. L'état peut être : Nouveau, Attribué, En cours, Tâche demandée, Tâche terminée, Clôturé et Clôturé - Faux positif.
PERSONNE AFFECTÉE	Affiche le membre de l'équipe actuellement affecté à l'incident.
ALERTES	Affiche le nombre d'alertes associées à l'incident. Un incident peut inclure de nombreuses alertes. Un grand nombre d'alertes peut signifier que vous êtes confronté à une attaque à grande échelle.

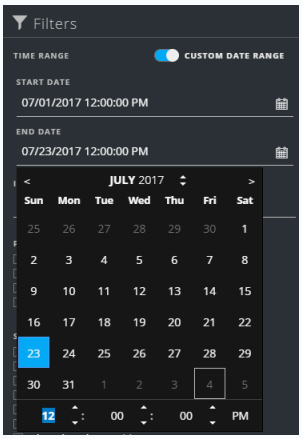
Au bas de la liste, vous voyez le nombre d'incidents sur la page en cours, le nombre total d'incidents et le nombre d'incidents sélectionnés. Par exemple : **Affichage 1 000 éléments sur 2 517 | 2 sélectionnés**. Le nombre maximal d'incidents que vous pouvez afficher en même temps est 1 000.

Panneau Filtres

La figure suivante présente les filtres disponibles dans le panneau Filtres.



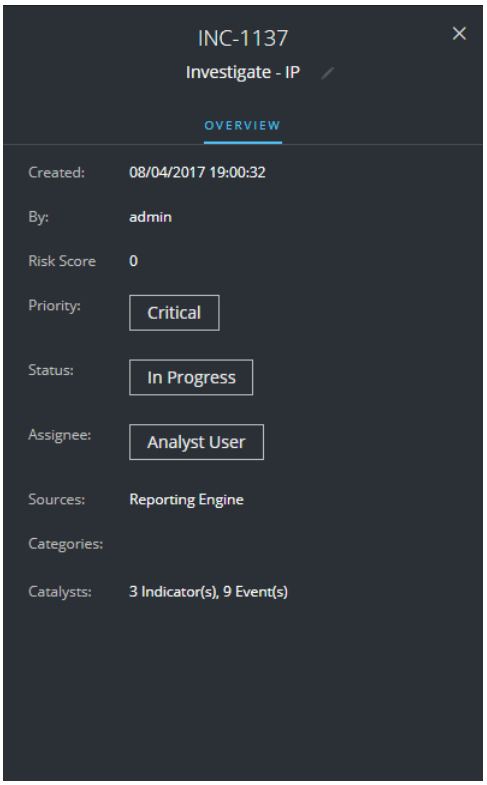
Le panneau Filtres, sur la gauche de la liste des incidents, propose des options que vous pouvez utiliser pour filtrer la liste des incidents. Lorsque vous quittez le panneau Filtres, la liste des incidents conserve vos sélections de filtre.

Option	Description
PÉRIODE	Vous pouvez sélectionner une période spécifique dans la liste déroulante Période. La période est basée sur la date de réception des alertes. Par exemple, si vous sélectionnez Dernière heure, vous verrez les alertes qui ont été créées au cours des 60 dernières minutes.
PLAGE DE DATES PERSONNALISÉE	Vous pouvez spécifier une plage de dates spécifique au lieu de sélectionner une option de période. Pour ce faire, cliquez sur le cercle blanc devant Plage de dates personnalisée pour afficher les champs Date de début et Date de fin. Sélectionnez les dates et heures dans le calendrier. 
ID D'INCIDENT	Vous pouvez saisir l'ID d'incident pour un incident que vous souhaitez rechercher, par exemple INC-1050.
PRIORITÉ	Sélectionnez les priorités que vous souhaitez afficher.
ÉTAT	Sélectionnez un ou plusieurs états d'incident. Par exemple, sélectionnez Clôturé - Faux positif pour afficher uniquement les incidents à l'état faux positif, c'est-à-dire qui ont été initialement identifiés comme suspects et qui ont ensuite été identifiés comme sûrs.

Option	Description
PERSONNE AFFECTÉE	Sélectionnez la ou les personnes affectées aux incidents que vous souhaitez afficher. Par exemple, si vous souhaitez uniquement afficher les incidents attribués à Cale ou à Stanley, sélectionnez Cale et Stanley dans la liste déroulante Personne affectée. Si vous souhaitez afficher les incidents, quelle que soit la personne affectée, n'effectuez pas de sélection dans la liste Personne affectée.
CATÉGORIES	Dans la liste déroulante, sélectionnez une ou plusieurs catégories. Par exemple, si vous souhaitez uniquement afficher les incidents classés avec les catégories Porte dérobée ou Abus de privilège, sélectionnez Porte dérobée et Abus de privilège.
Réinitialiser les filtres	Supprime vos sélections de filtre.

Panneau Présentation

Le panneau Présentation contient des informations récapitulatives de base sur un incident sélectionné. Dans la liste Incidents, vous pouvez cliquer sur un incident pour accéder au panneau Présentation. Le panneau Présentation de la liste des incidents contient les mêmes informations.



Le tableau suivant répertorie les champs affichés dans le panneau Présentation des incidents.

Champ	Description
<ID d'incident>	Affiche l'ID de l'incident.
<Nom de l'incident>	Affiche le nom de l'incident. Vous pouvez cliquer sur le nom de l'incident pour le modifier. Par exemple, les règles peuvent créer de nombreux incidents portant le même nom. Vous pouvez modifier les noms des incidents pour plus de précision.
Créé	Affiche la date et l'heure de création de l'incident.
Règle/Par	Affiche le nom de la règle qui a créé l'incident ou le nom de la personne qui a créé l'incident.

Champ	Description
Score de risque	Indique le risque de l'incident, calculé via un algorithme et compris entre 0 et 100. 100 est le score de risque le plus élevé.
Priorité	Affiche la priorité de l'incident. La priorité peut être critique, élevée, moyenne ou faible. Pour modifier la priorité, vous pouvez cliquer sur le bouton Priorité et sélectionner une nouvelle priorité dans la liste déroulante.
État	Affiche l'état de l'incident. L'état peut être Nouveau, Attribué, En cours, Tâche demandée, Tâche terminée, Clôturé et Clôturé - Faux positif. Pour modifier l'état, vous pouvez cliquer sur le bouton État et sélectionner un nouvel état dans la liste déroulante.
Personne affectée	Affiche le membre de l'équipe actuellement affecté à l'incident. Pour modifier la personne affectée, vous pouvez cliquer sur le bouton Personne affectée et sélectionner un nouveau destinataire dans la liste déroulante.
Sources	Indique les sources de données utilisées pour localiser l'activité suspecte.
Catégories	Affiche les catégories des événements d'incidents.
Catalyseurs	Affiche le nombre d'indicateurs ayant donné lieu à l'incident.

Actions de la barre d'outils

Ce tableau répertorie les actions de la barre d'outils disponibles dans la liste des incidents.

Option	Description
	Vous permet d'ouvrir le panneau Filtres afin que vous puissiez spécifier les alertes que vous aimeriez afficher dans la vue Liste des alertes.
	Ferme le panneau.

Option	Description
Bouton **Modifier la priorité**	Vous permet de modifier la priorité d'un ou de plusieurs incidents sélectionnés dans la liste des incidents.
Bouton **Modifier l'état**	Vous permet de modifier l'état d'un ou de plusieurs incidents.
Bouton **Changer la personne affectée**	Vous permet de modifier la personne affectée d'un ou de plusieurs incidents.
Bouton **Supprimer**	Vous permet de supprimer les incidents sélectionnés si vous disposez des autorisations appropriées, par exemple Administrateur ou Responsable de la confidentialité des données.

Vue Détails sur l'incident

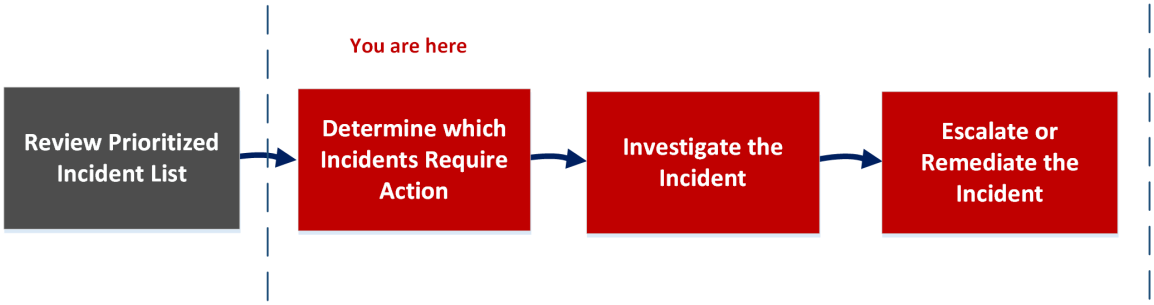
Dans la vue Détails sur l'incident (RÉPONDRE > Incidents > cliquez sur le lien d'un ID ou d'un nom dans la liste des incidents), vous pouvez afficher des détails étendus relatifs à l'incident. La vue Détails sur l'incident contient plusieurs panneaux qui offrent les avantages suivants :

- **Présentation** : Afficher un récapitulatif de l'incident et mettre à jour l'incident.
- **Indicateurs** : Afficher les indicateurs (alertes) impliqués dans l'incident, les événements au sein de ces alertes et les informations d'enrichissement disponibles.
- **Graphique de nœud** : Visualiser la taille et les interactions entre les entités (adresse IP, adresse MAC, utilisateur, hôte, domaine, nom de fichier ou hachage de fichier).
- **Fiche produit des événements** : Examiner les événements associés à l'incident.
- **Journal** : Ajouter des remarques et collaborer avec d'autres analystes.
- **Tâches** : Créer des tâches d'incidents et effectuer leur suivi jusqu'à leur résolution.
- **Indicateurs connexes** : Afficher les indicateurs (alertes) qui sont liés à l'incident et les ajouter à l'incident s'ils ne sont pas associés à un incident.

Vous pouvez également filtrer les données dans la vue Détails sur l'incident pour étudier des indicateurs et les entités dignes d'intérêt.

Workflow

Ce workflow montre le processus de haut niveau que les responsables de la réponse aux incidents utilisent pour répondre aux incidents dans NetWitness Suite.



Dans la vue Détails sur l'incident, vous pouvez utiliser les informations détaillées fournies sur les incidents afin de déterminer les incidents qui exigent une action. Vous disposez également des outils et des informations nécessaires pour enquêter sur l'incident, et le faire remonter ou le corriger.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Responsables de la réponse aux incidents, analystes, responsables du SOC	Afficher les incidents prioritaires, filtrer et trier la liste des incidents, trouver des incidents, afficher mes incidents et attribuer les incidents à moi-même.	Passer en revue la liste des incidents hiérarchisés
Responsables de la réponse aux incidents, analystes	Afficher les détails sur l'incident.*	Afficher les détails sur l'incident
Responsables de la réponse aux incidents, analystes	Afficher les alertes et enrichissements.*	Afficher les indicateurs et les enrichissements
Responsables de la réponse aux incidents, analystes	Afficher les événements.*	Afficher et étudier les événements
Responsables de la réponse aux incidents, analystes	Afficher un graphique des entités impliquées dans les événements.*	Afficher et étudier les entités impliquées dans les événements
Responsables de la réponse aux incidents, analystes	Filtrer les données relatives aux incidents.*	Filtrer les données dans la vue Détails de l'incident
Responsables de la réponse aux incidents, analystes	Afficher et ajouter des remarques relatives aux incidents.*	Afficher les notes sur l'incident et Documenter les étapes suivies en dehors de NetWitness
Responsables de la réponse aux incidents, analystes	Afficher et créer des tâches.*	Afficher les tâches associées à un incident et Créer une tâche
Responsables de la réponse aux incidents, analystes	Ajouter des alertes associées et les ajouter à l'incident.*	Rechercher des indicateurs associés et Ajouter des indicateurs associés à l'incident

Rôle	Je souhaite...	Me montrer comment
Responsables de la réponse aux incidents, analystes	Afficher des informations contextuelles sur un incident à partir de Context Hub.*	Afficher les informations contextuelles
Responsables de la réponse aux incidents, analystes	Réduire les faux positifs en ajoutant une entité à la liste blanche.*	Ajouter une entité à une liste blanche
Responsables de la réponse aux incidents, analystes	Pivoter vers la fonction Enquêter.*	Pivoter vers la fonction Enquêter
Responsables de la réponse aux incidents, analystes	Pivoter vers NetWitness Endpoint. *	Pivoter vers le point de terminaison NetWitness
Responsables de la réponse aux incidents, analystes	Mettre à jour ou clore un incident.*	Mettre à jour un incident et Clore un incident
Responsables de la réponse aux incidents, analystes, responsables du SOC	Afficher toutes les tâches.	Faire remonter ou corriger l'incident
Responsables de la réponse aux incidents, analystes, responsables du SOC	Mettre à jour les incidents et les tâches en bloc.	Faire remonter ou corriger l'incident

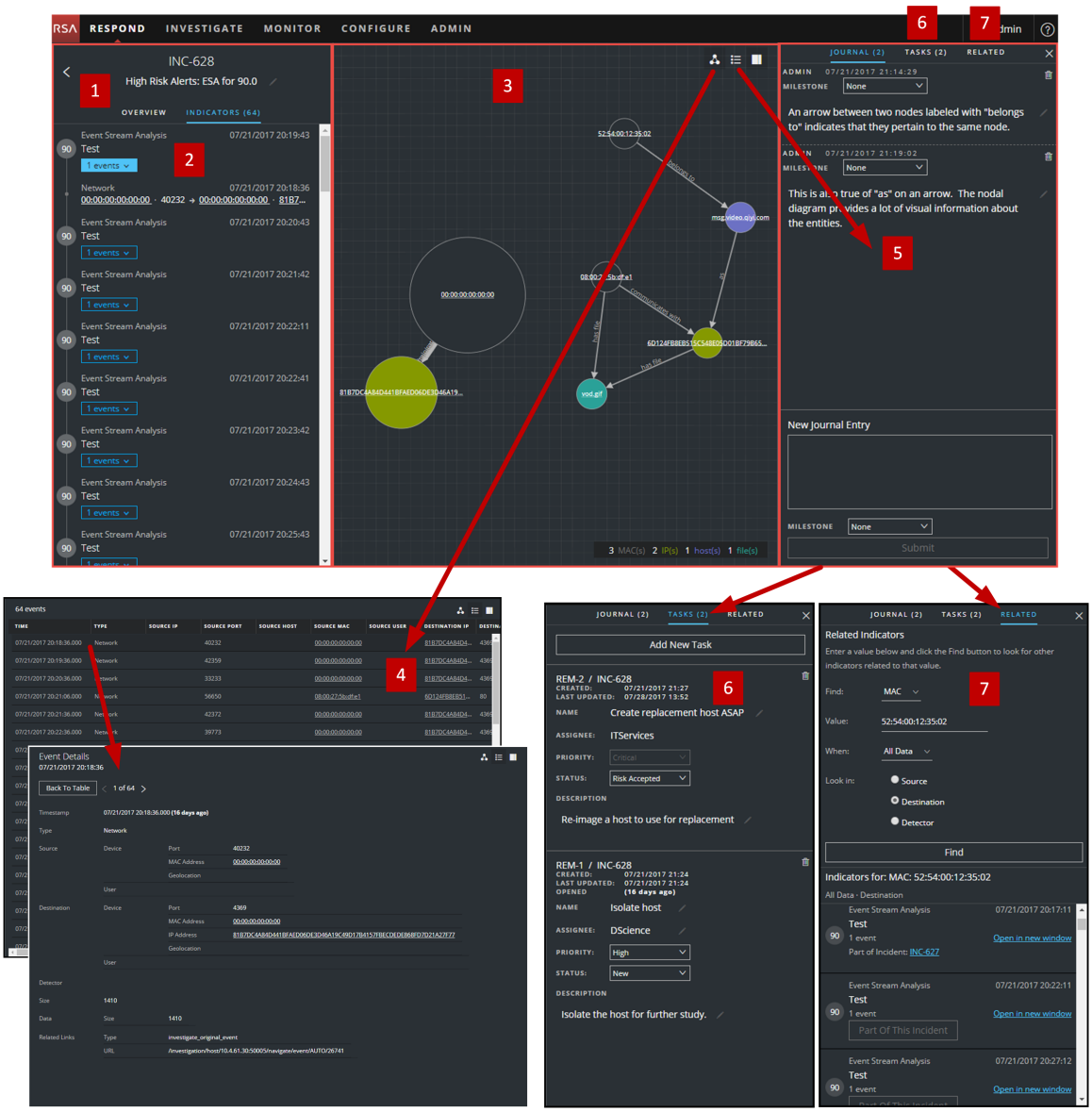
*Vous pouvez effectuer ces tâches ici (c'est-à-dire dans la vue Détails sur l'incident).

Rubriques connexes

- Vue Liste des incidents
- Déterminer les incidents exigeant une action
- Enquêter sur l'incident
- Faire remonter ou corriger l'incident

Aperçu rapide

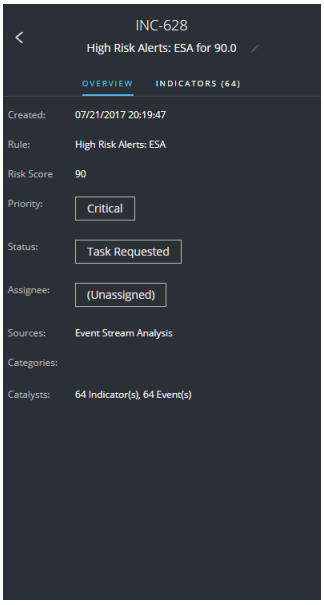
L'exemple suivant montre les emplacements des panneaux de la vue Détails sur l'incident.



1	Panneau de présentation (cliquez sur l'onglet PRÉSENTATION pour l'afficher.)
2	Panneau Indicateurs
3	Graphique de nœud
4	Fiche produit des événements (Cliquez sur un événement dans la liste Événements pour afficher les détails sur l'événement.).
5	Panneau Journal
6	Panneau Tâches (cliquez sur l'onglet TÂCHES pour l'afficher.)
7	Panneau Indicateurs connexes (cliquez sur l'onglet associé pour l'afficher.)

Panneau Présentation

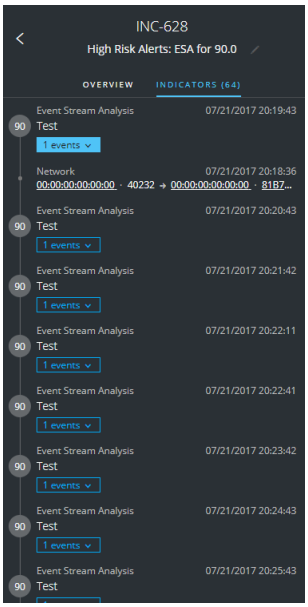
Le panneau Présentation contient des informations récapitulatives de base sur un incident sélectionné. Il vous permet également de modifier le nom de l'incident et de mettre à jour sa priorité, son état et la personne affectée. Le panneau Présentation de la vue Liste des incidents contient les mêmes informations. La rubrique Panneau Présentation de la vue Liste des incidents fournit des détails.



Panneau Indicateurs

Le panneau Indicateurs contient une liste chronologique des indicateurs. Les *indicateurs* sont des alertes, comme une alerte ESA ou une alerte NetWitness Endpoint. (Il ne s'agit pas d'une chronologie, qui fournit une représentation visuelle de la chronologie des événements dans l'incident). Cette liste vous aide à connecter les indicateurs et les données importantes. Par exemple, une adresse IP est connectée à une commande, et une alerte ESA de communication peut également avoir déclenché une alerte NetWitness Endpoint ou d'autres activités suspectes.

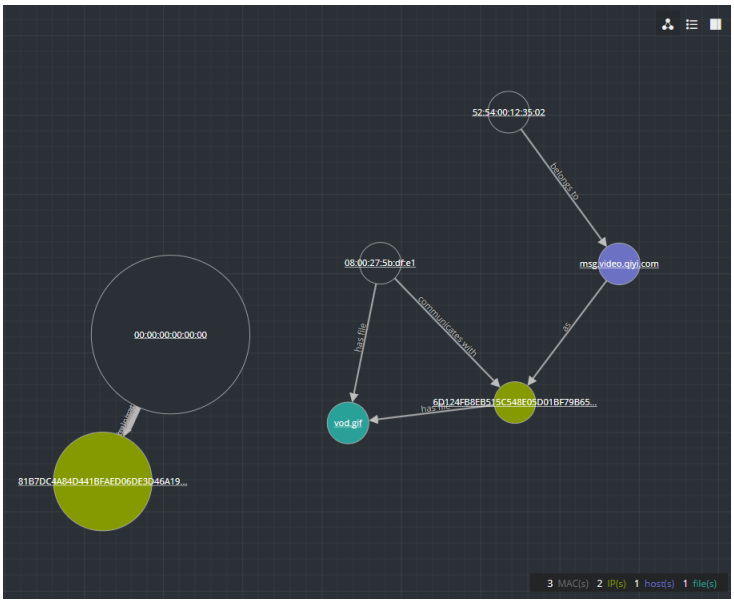
Pour afficher le panneau Indicateurs, dans le panneau gauche de la vue Détails sur l'incident, sélectionnez **INDICATEURS**.



Les informations de sources de données sont présentées sous les noms des indicateurs. Vous pouvez également voir la date de création et l'heure de l'indicateur, ainsi que le nombre d'événements dans l'indicateur.

Graphique de nœud

Le graphique de nœud est un graphique interactif qui illustre les entités impliquées dans l'incident. Une *entité* est un composant spécifié de méta, comme l'adresse IP, l'adresse MAC, l'utilisateur, l'hôte, le domaine, le nom de fichier ou le hachage de fichier.



Nœuds

Dans le graphique de noeud, des cercles représentent les nœuds. Le tableau suivant présente les types de nœuds du graphique de nœud.

Nœud	Description
Adresse IP	Si l'événement est une anomalies détectée, vous pouvez voir une adresse IP de détecteur. Si l'événement est une transaction, vous pouvez voir une adresse IP de destination et une adresse IP source.
Adresse MAC	Vous pouvez voir une adresse MAC pour chaque type d'adresse IP.
Utilisateur	Si la machine est associée à un utilisateur, vous pouvez voir un nœud d'utilisateur.
Hôte	Un hôte peut être un équipement physique ou une machine virtuelle. Il est désigné par un nom de domaine complet (FQDN) ou une adresse IP sur laquelle un service est installé.
Domaine	
Nom du fichier	Si l'événement implique des fichiers, vous pouvez voir un nom de fichier.
Hachage de fichier	Si l'événement implique des fichiers, vous pouvez voir un hachage de fichier.

La légende en bas du graphique de nœud indique le nombre de nœuds de chaque type et le code couleur des nœuds. Elle permet également de localiser les entités lorsque les valeurs, telles que les adresses IP, sont hachées.

Vous pouvez cliquer sur n'importe quel nœud et le faire glisser pour le repositionner.

Flèches

Les flèches entre les nœuds fournissent des informations supplémentaires relatives aux relations d'entité. Le tableau suivant présente les types de flèches du graphique de nœud.

Flèche	Description
Communique avec	Une flèche entre un nœud de machine source (adresse IP ou adresse MAC) et un nœud de machine de destination nommée « communique avec » indique la direction de la communication.

Flèche	Description
En tant que	Une flèche entre les nœuds nommée « en tant que » fournit des informations complémentaires sur l'adresse IP vers laquelle la flèche pointe. Par exemple, s'il existe une flèche partant du cercle du nœud hôte qui pointe vers le nœud d'une adresse IP et qui est nommée « en tant que », elle indique que le nom du cercle du noeud hôte est le nom d'hôte de cette adresse IP et qu'il ne s'agit pas d'une autre entité.
Contient le fichier	Une flèche entre un nœud de machine (adresse IP, adresse MAC ou hôte) et un nœud de hachage de fichier identifié par « contient » indique que l'adresse IP contient ce fichier.
Utilisations	Une flèche entre un nœud d'utilisateur et un nœud de machine (adresse IP, adresse MAC ou hôte) nommée « utilise » indique la machine que l'utilisateur utilisait lors de l'événement.
Est nommé	Une flèche à partir d'un nœud de hachage de fichier vers un nœud de nom de fichier accompagné de « est nommé » indique que le hachage de fichier correspond à un fichier portant ce nom.
Appartient à	Une flèche entre deux nœuds identifiée par « appartient à » indique qu'ils appartiennent au même nœud. Par exemple, une flèche entre une adresse MAC et un hôte nommée « appartient à » indique qu'il s'agit de l'adresse MAC de l'hôte.

Des flèches avec une ligne de taille supérieure représentent plus de communication entre les nœuds. Des nœuds plus grands (cercles) indiquent davantage d'activité que les nœuds plus petits. Les nœuds de plus grande taille sont les entités les plus courantes mentionnées dans les événements.

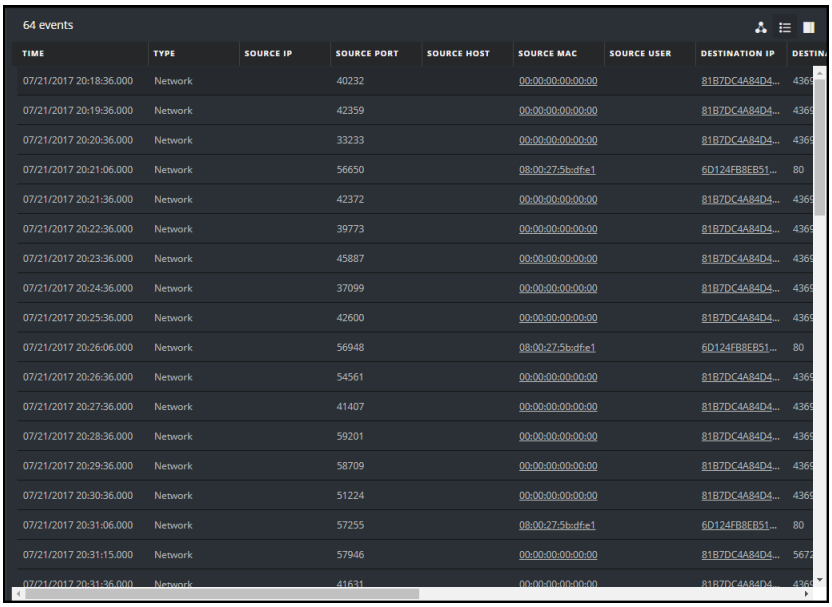
Fiche produit des événements

La fiche produit des événements affiche les événements associés à l'incident. Il présente des informations relatives aux événements, comme l'heure de l'événement, l'adresse IP source, l'adresse IP de destination, l'adresse IP du détecteur, l'utilisateur source, l'utilisateur de destination et les informations de fichier sur les événements. La quantité d'informations répertoriées varie selon le type d'événement.

La fiche produit des événements affiche une liste d'événements pour plusieurs événements ou les détails de l'événement pour un seul événement.

Liste d'événements

La figure ci-dessous présente la liste des événements.



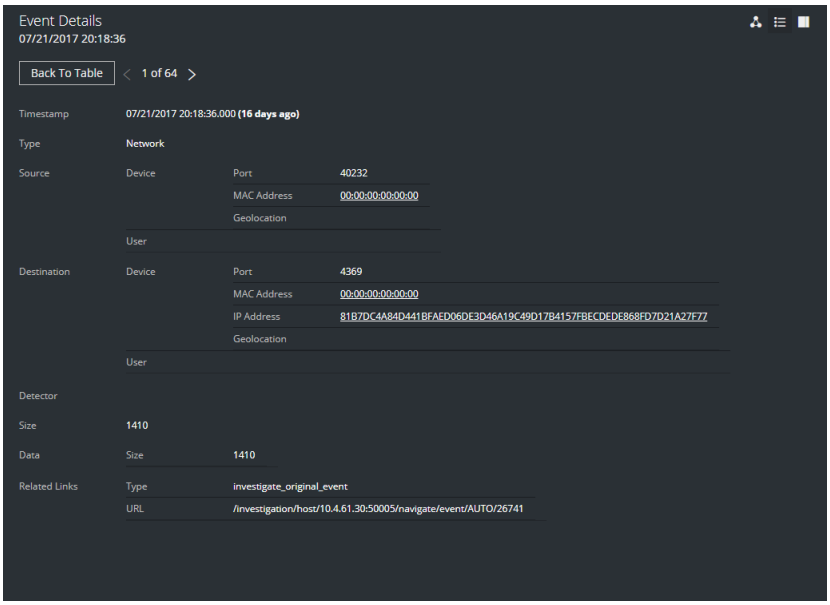
Le tableau suivant décrit les colonnes de la liste des événements.

Colonne	Description
HEURE	Affiche l'heure à laquelle l'événement s'est produit.
TYPE	Affiche le type d'alerte, comme Log et Réseau.
IP SOURCE	Affiche l'adresse IP source s'il y a eu une transaction entre les deux machines.
PORT SOURCE	Indique le port de la source de la transaction. Les ports source et de destination peuvent être sur la même adresse IP.
HÔTE SOURCE	Affiche l'hôte de destination sur lequel l'événement a eu lieu.
MAC SOURCE	Affiche l'adresse MAC de la machine source.
UTILISATEUR SOURCE	Affiche l'utilisateur de la machine source.

Colonne	Description
IP de destination	Affiche l'adresse IP de destination s'il y a eu une transaction entre les deux machines
Port de destination	Indique le port de la destination de la transaction. Les ports source et de destination peuvent être sur la même adresse IP.
HÔTE DE DESTINATION	Affiche le nom d'hôte de la machine de destination.
ADRESSE MAC DE DESTINATION	Affiche l'adresse MAC de la machine de destination.
UTILISATEUR DE DESTINATION	Affiche l'utilisateur de la machine de destination.
IP DÉTECTEUR	Affiche l'adresse IP de la machine sur laquelle une anomalie a été détectée.
NOM DE FICHIER	Affiche le nom du fichier si un fichier est impliqué dans l'événement.
HACHAGE DE FICHIER	Présente un hachage du contenu du fichier.

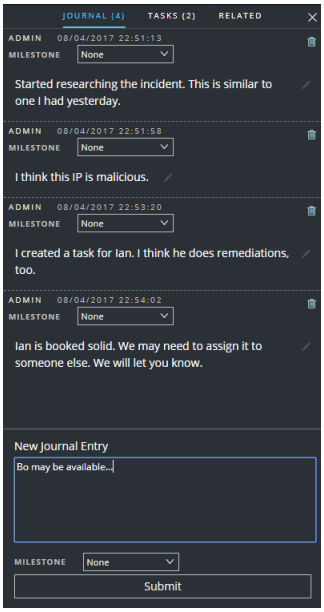
Détails de l'événement

Cliquez sur un événement dans la liste des événements pour afficher les détails relatifs à l'événement. S'il existe un seul événement dans la liste, vous verrez les détails de l'événement pour cet événement au lieu d'une liste.



Panneau Journal

Le Journal de l'incident présente l'historique de l'activité sur un incident.



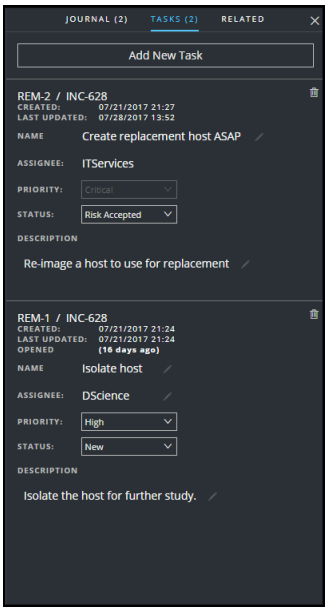
Le tableau suivant décrit les options de la Nouvelle entrée de journal.

Champ	Description
Nouvelle entrée de journal	Saisissez votre remarque dans le champ.

Champ	Description
Étape	(Facultatif) Sélectionnez une étape, le cas échéant. Ce champ est utilisé pour effectuer le suivi des événements importants pour l'incident.
Bouton **Envoyer**	Cliquez sur Envoyer pour ajouter une entrée dans le journal. Votre entrée de journal sera visible par tout utilisateur qui affiche l'incident.

Panneau Tâches

Dans le panneau Tâches, vous pouvez gérer et suivre les tâches relatives aux incidents jusqu'à sa fermeture.



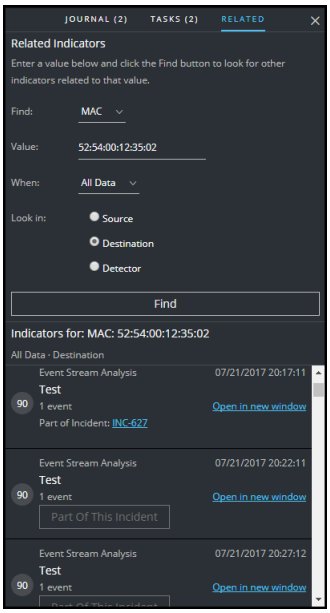
Le tableau suivant présente les champs de la tâche.

Champ	Description
<ID tâche / <ID incident>	ID tâche généré automatiquement / Incident associé à la tâche.
CRÉÉ	Date de création de la tâche.
DERNIÈRE MISE À JOUR	Date à laquelle la tâche a été modifiée pour la dernière fois.
OUVERT	Heure depuis la dernière ouverture de la tâche. Par exemple, il y a 3 minutes ou il y a 2 jours.

Champ	Description
NOM	Nom de la tâche. Par exemple : Nouvelle image de la machine. Vous pouvez cliquer sur ce champ pour le modifier.
PERSONNE AFFECTÉE	Nom d'utilisateur de la personne à laquelle le dossier est attribué. Vous pouvez cliquer sur ce champ pour le modifier.
PRIORITÉ	Priorité de la tâche : Faible, Moyenne, Élevée ou Critique. Vous pouvez cliquer sur le bouton de priorité et sélectionner une nouvelle priorité pour la tâche dans la liste déroulante.
ÉTAT	État de la tâche : Nouveau, Attribué, En cours, Corrigé, Risque accepté et Sans objet. Vous pouvez cliquer sur le bouton d'état et sélectionner un nouvel état de la tâche dans la liste déroulante.
DESCRIPTION	Saisissez les informations qui décrivent la tâche. Vous pouvez inclure des numéros de référence applicables. Vous pouvez cliquer sur ce champ pour le modifier.

Panneau Indicateurs connexes

Le panneau Indicateurs associés vous permet d'effectuer une recherche dans la base de données des alertes NetWitness Suite pour trouver les alertes liées à cet incident. Vous pouvez ajouter des alertes que vous trouvez associées à l'incident, si elles ne sont pas déjà associées à un incident.



Le tableau suivant décrit les champs de la section de recherche en haut du panneau.

Champ	Description
Rechercher	Sélectionnez l'entité que vous souhaitez trouver dans les alertes. Par exemple, IP.
Valeur	Saisissez la valeur de l'entité. Par exemple, saisissez l'adresse IP réelle de l'entité.
Quand	Sélectionnez une plage de temps pour rechercher les alertes. Par exemple, Dernières 24 heures.
Rechercher dans	Spécifiez le type de l'entité à rechercher : • **Source** : La machine source dans une transaction entre deux machines. • **Destination** : La machine de destination dans une transaction entre deux machines. • **Détecteur** : Une machine unique dans laquelle une anomalie a été détectée. • **Domaine** : Cette option est disponible lorsque vous sélectionnez Domaine dans le champ Rechercher. Par exemple, sélectionnez la source pour rechercher des alertes où une adresse IP particulière est traitée en tant que périphérique source. Vous pouvez effectuer des recherches séparées pour chaque type de périphérique : Source, Destination et Détecteur.
Bouton **Rechercher**	Permet de lancer des recherches. Une liste des indicateurs associés s'affiche sous le bouton **Rechercher** dans la section **Indicateurs pour**.

Le tableau suivant décrit les options de la section **Indicateurs pour** (résultats) au bas du panneau.

Option	Description
Indicateurs pour :	Affiche les résultats de la recherche.
Lien **Ouvrir dans une nouvelle fenêtre**	Affiche les détails sur l'alerte pour l'indicateur.
Bouton **Ajouter à un incident**	Permet d'ajouter l'indicateur associé à l'incident. L'indicateur associé est ajouté dans le panneau Indicateurs.

Option	Description
Bouton **Partie intégrante de cet incident**	Indique que l'indicateur fait déjà partie de l'incident.

Actions de la barre d'outils

Option	Description
	(Revenir aux Incidents) Vous permet de revenir à la vue Liste des incidents.
	Ferme le panneau.
	Supprime l'entrée, par exemple une entrée de journal ou une tâche.
Bouton **Priorité**	(Dans le panneau Présentation) Vous permet de modifier la priorité d'un ou de plusieurs incidents sélectionnés dans la liste des Incidents.
Bouton **État**	(Dans le panneau Présentation) Vous permet de modifier l'état d'un ou de plusieurs incidents.
Bouton **Personne affectée**	(Dans le panneau Présentation) Vous permet de modifier la personne affectée d'un ou de plusieurs incidents.
 (Vue : Graphique)	Vous permet d'afficher le graphique de noeud.
 (Vue : Fiche produit)	Vous permet d'afficher la fiche produit des événements qui affiche une liste d'événements pour plusieurs événements ou les détails de l'événement pour un seul événement.

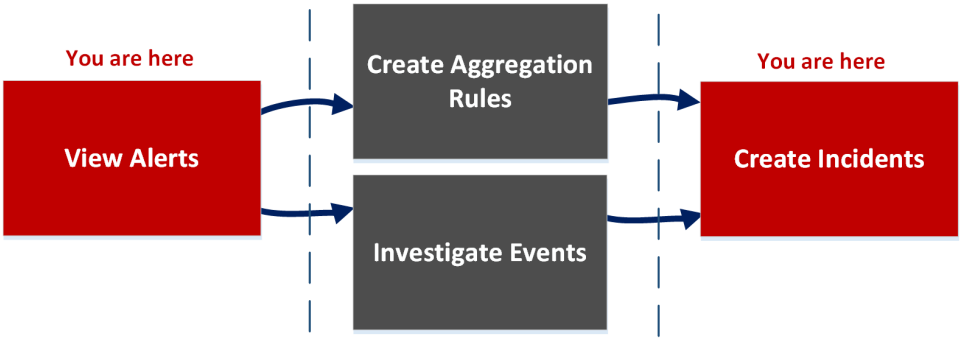
Option	Description
 (Journal, Tâches et Éléments connexes)	Vous permet d'afficher les panneaux Journal, Tâches et Indicateurs connexes.

Vue Liste des alertes

La vue Liste des alertes (RÉPONDRE > Alertes) vous permet d'afficher toutes les alertes de menace et les indicateurs reçus par NetWitness Suite dans un emplacement unique. Cela peut inclure les alertes provenant des règles de corrélation ESA, d'ESA Analytics, de Malware Analysis, de Reporting Engine, de NetWitness Endpoint et de nombreuses autres sources. Dans la vue Liste des alertes, vous pouvez parcourir les différentes alertes, les filtrer et les regrouper pour créer des incidents.

Workflow

Ce workflow montre le processus de haut niveau que les analystes utilisent pour vérifier les alertes et créer des incidents.



Dans la vue Liste des alertes, vous pouvez consulter la liste des alertes provenant de toutes les sources reçues par NetWitness Suite. Ensuite, vous pouvez examiner davantage ces alertes et créer des incidents à partir des alertes. Vous pouvez aussi créer des règles d'agrégation pour créer des incidents.

Remarque : vous pouvez utiliser l'option Détection automatisée des menaces NetWitness Suite pour créer des incidents sans créer manuellement des règles.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Responsables de la réponse aux incidents, analystes	Afficher toutes les alertes dans NetWitness Suite.*	Afficher les alertes

Rôle	Je souhaite...	Me montrer comment
Responsables de la réponse aux incidents, analystes	Filtrer les alertes.*	Filtrer la liste des alertes
Responsables de la réponse aux incidents, analystes	Afficher les informations de présentation des alertes et les métadonnées de l'alerte brute.*	Afficher les informations récapitulatives relatives aux alertes
Responsables de la réponse aux incidents, analystes	Créer des incidents à partir des alertes.*	Créer un incident manuellement
Administrateurs, agents de confidentialité des données	Supprimer les alertes.*	Supprimer les alertes
Responsables du SOC, administrateurs	Créer des règles d'agrégation.	Reportez-vous à la rubrique « Création d'une règle d'agrégation pour les alertes » dans le *NetWitness RespondGuide de Configuration*.
Responsables de la réponse aux incidents, analystes	Examiner les événements d'une d'alerte.	Afficher les détails relatifs à l'événement pour une alerte et Examiner les événements
Responsables de la réponse aux incidents, analystes	Ajouter des alertes à un incident existant	Ajouter des indicateurs associés à l'incident

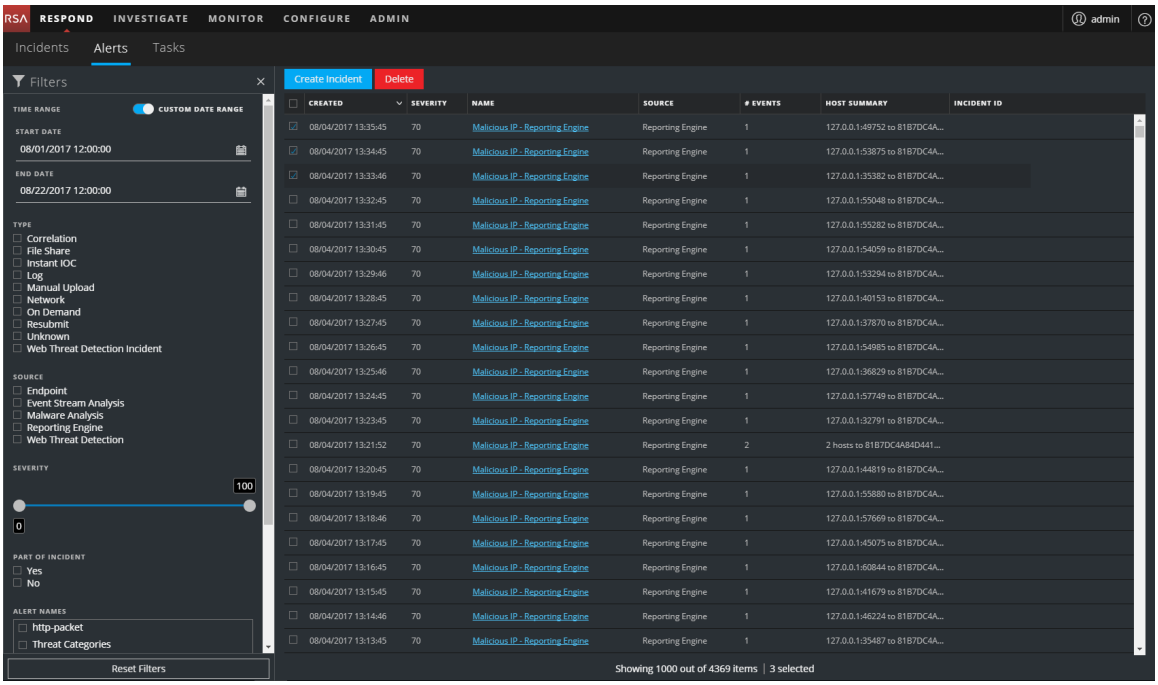
*Vous pouvez effectuer ces tâches ici (c'est-à-dire dans la vue Liste des alertes).

Rubriques connexes

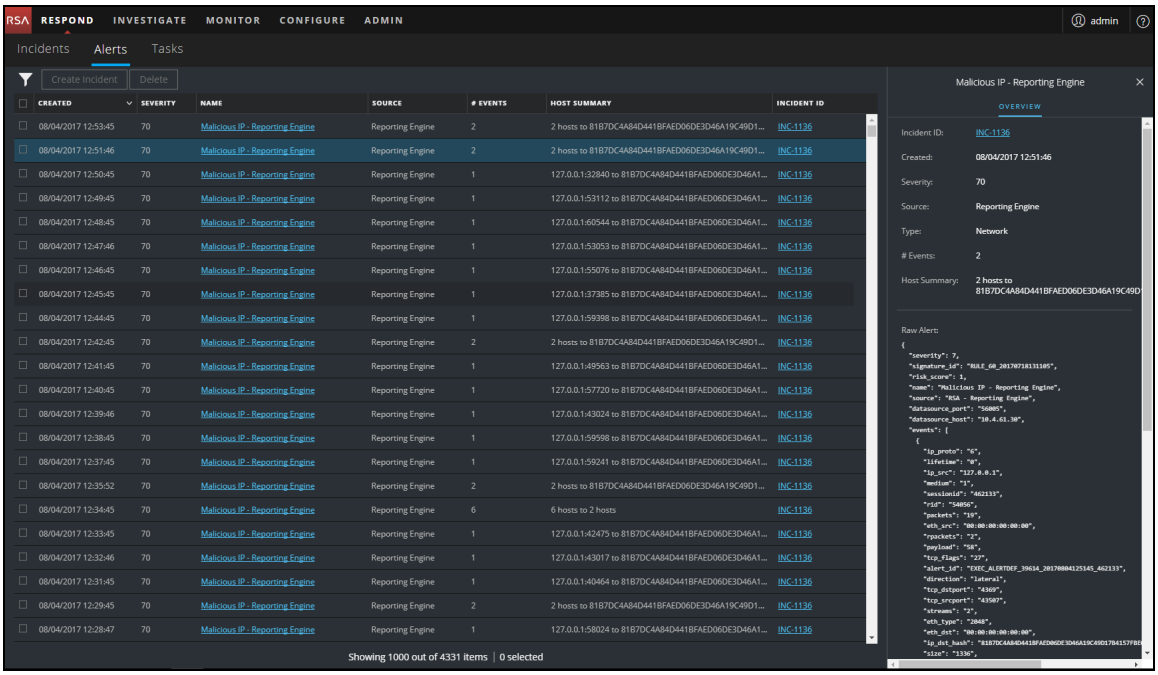
- Vue Détails relatifs aux alertes
- Vérifier les alertes

Vue Liste des alertes

Pour accéder à la vue Liste des alertes, accédez à **RÉPONDRE > Alertes**. La vue Liste des alertes affiche une liste des alertes et indicateurs reçus par la base de données Serveur Respond dans NetWitness Suite. La figure suivante illustre le panneau Filtres sur la gauche.

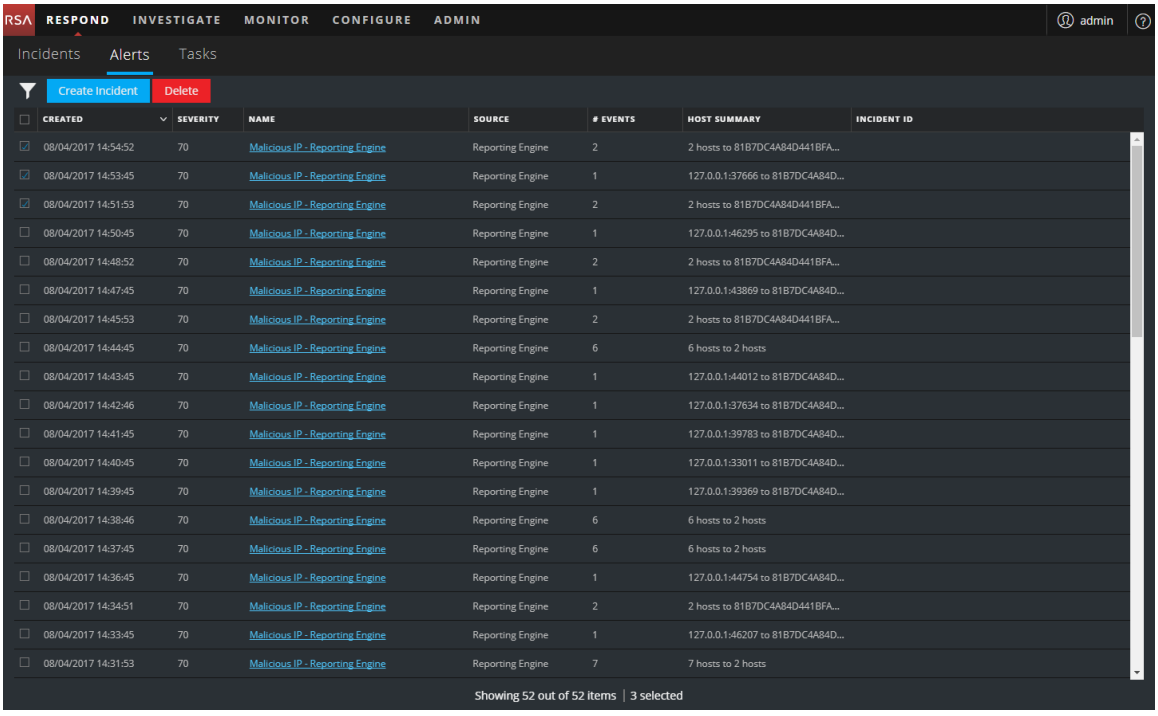


La vue Liste des alertes se compose d'un panneau Filtres, d'une vue Liste des alertes et d'un panneau Présentation des alertes. Vous pouvez cliquer sur une alerte dans la liste Alertes pour afficher le panneau Présentation des alertes sur la droite.



Liste des alertes

La vue Liste des alertes affiche toutes les alertes dans NetWitness Suite. Vous pouvez filtrer cette liste pour afficher uniquement les alertes intéressantes.

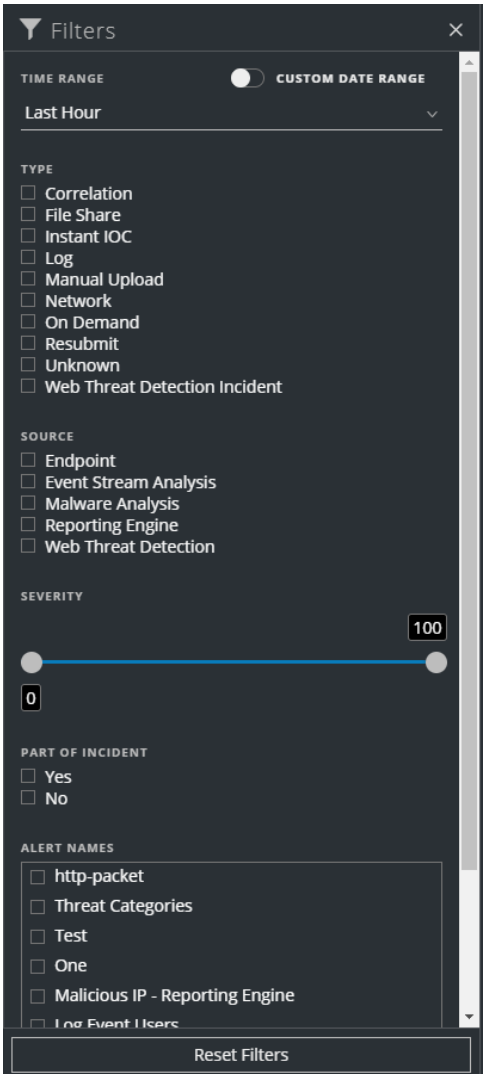


Colonne	Description
	Vous permet de sélectionner une ou plusieurs alertes à modifier ou supprimer. Avec les autorisations appropriées, par exemple Administrateurs et Agents de confidentialité des données, les utilisateurs peuvent supprimer les alertes.
CRÉÉ	Affiche la date et l'heure auxquelles l'alerte a été enregistrée dans le système source.
GRAVITÉ	Affiche le niveau de gravité de l'alerte. Les valeurs sont comprises entre 1 et 100.
NOM	Affiche une description de base de l'alerte.
SOURCE	Affiche la source originale de l'alerte. La source des alertes peut être NetWitness Endpoint, Malware Analysis, les règles de corrélation ESA, ESA Analytics, Reporting Engine, et bien d'autres.
NOMBRE D'ÉVÉNEMENTS	Indique le nombre d'événements contenus dans une alerte. Cela varie en fonction de la source de l'alerte. Par exemple, les alertes NetWitness Endpoint et Malware Analysis ont toujours un événement. Pour certains types d'alertes, un nombre élevé d'événements peut signifier que l'alerte est plus risquée.
RÉCAPITULATIF DE L'HÔTE	Affiche les détails relatifs à l'hôte tels que le nom de l'hôte d'où l'alerte a été déclenchée. Les détails peuvent inclure des informations sur les hôtes source et cible dans une alerte . Certaines alertes peuvent décrire des événements sur plusieurs hôtes.
ID D'INCIDENT	Affiche l'ID d'incident de l'alerte. S'il n'y a pas d'ID d'incident, cela signifie que l'alerte ne fait pas partie d'un incident. Vous pouvez alors créer un incident pour inclure cette alerte. Cette alerte peut être ajoutée à un incident existant.

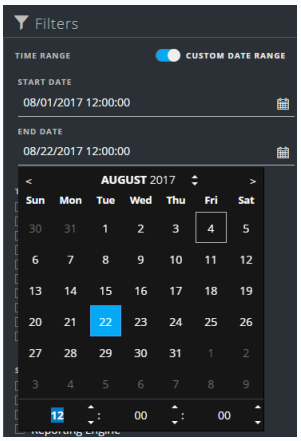
Au bas de la liste, vous voyez le nombre d'alertes sur la page en cours, le nombre total d'alertes et le nombre d'alertes sélectionnées. Par exemple : **Affichage de 377 éléments sur 377 | 3 sélectionnés**

Panneau Filtres

La figure suivante présente les filtres disponibles dans le panneau Filtres.



Le panneau Filtres, sur la gauche de la vue Liste des alertes, propose des options que vous pouvez utiliser pour filtrer la liste des alertes. Lorsque vous quittez le panneau Filtres, la vue Liste des alertes conserve vos sélections de filtre.

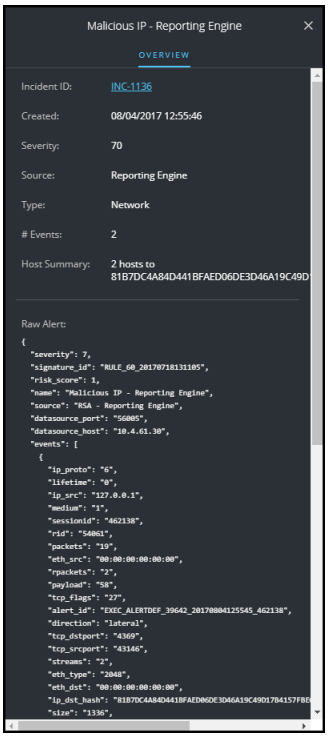
Option	Description
PÉRIODE	Vous pouvez sélectionner une période spécifique dans la liste déroulante Période. La période est basée sur la date de réception des alertes. Par exemple, si vous sélectionnez Dernière heure, vous verrez les alertes qui ont été créées au cours des 60 dernières minutes.
PLAGE DE DATES PERSONNALISÉE	Vous pouvez spécifier une plage de dates spécifique au lieu de sélectionner une option de période. Pour ce faire, cliquez sur le cercle blanc devant Plage de dates personnalisée pour afficher les champs Date de début et Date de fin. Sélectionnez les dates et heures dans le calendrier. 
TYPE	Indique le type d'événements liés à l'alerte, par exemple, les logs, sessions réseau, etc.
SOURCE	Affiche la source originale de l'alerte. La source des alertes peut être NetWitness Endpoint, Malware Analysis, Event Stream Analysis (règles de corrélation ESA), ESA Analytics, Reporting Engine, Web Threat Detection, et bien d'autres.
GRAVITÉ	Affiche le niveau de gravité de l'alerte. Les valeurs sont comprises entre 1 et 100.

Option	Description
PARTIE INTÉGRANTE DE L'INCIDENT	Classe les alertes selon qu'elles sont associées ou non à un incident. Sélectionnez **Oui** pour afficher les alertes qui font partie d'un incident. Sélectionnez **Non** pour afficher les alertes qui ne sont pas liées aux incidents. Par exemple, avant de créer des incidents à partir des alertes, vous pouvez sélectionner Non pour afficher uniquement les alertes qui ne font pas déjà partie d'un incident.
NOMS DES ALERTES	Affiche le nom de l'alerte. Vous pouvez utiliser ce filtre pour rechercher toutes les alertes générées par une règle ou une source spécifique, par exemple, IP malveillantes - Reporting Engine.
Réinitialiser les filtres	Supprime vos sélections de filtre.

La vue Liste des alertes affiche une liste d'alertes qui répondent à vos critères de sélection. Vous pouvez voir le nombre d'éléments dans votre liste filtrée en bas de la liste des alertes. Par exemple : **Affichage de 30 éléments sur 30**

Panneau Présentation

Le panneau Présentation contient des informations récapitulatives de base sur l'alerte sélectionnée et les métadonnées de l'alerte brute. Le panneau Présentation de la vue Détails relatifs aux alertes contient les mêmes informations, mais dans la vue Détails relatifs aux alertes, vous pouvez développer le panneau pour afficher plus d'informations.



Le tableau suivant répertorie les champs affichés dans le panneau Présentation des alertes.

Champ	Description
<Nom de l'alerte>	Affiche le nom de l'alerte.
ID d'incident	Affiche l'ID d'incident associé à l'alerte. Vous pouvez cliquer sur le lien de l'ID d'incident pour accéder à la vue Détails sur l'incident pour l'incident associé. S'il n'existe aucun ID d'incident, l'alerte n'appartient pas à un incident. Vous pouvez créer un incident pour cette alerte ou l'ajouter à un incident.
Créé	Affiche la date et l'heure de création de l'alerte.
Gravité	Affiche le niveau de gravité de l'alerte. Les valeurs sont comprises entre 1 et 100.
Source	Affiche la source originale de l'alerte. La source des alertes peut être NetWitness Endpoint, Malware Analysis, les règles de corrélation ESA, ESA Analytics, Reporting Engine, et bien d'autres.

Champ	Description
Type	Indique le type d'événements liés à l'alerte, par exemple, les logs, sessions réseau, etc.
Nombre d’événements	Indique le nombre d'événements contenus dans une alerte. Cela varie en fonction de la source de l'alerte. Par exemple, les alertes NetWitness Endpoint et Malware Analysis ont toujours un événement. Pour certains types d'alertes, un nombre élevé d'événements peut signifier que l'alerte est plus risquée.
Alerte brute	Affiche les métadonnées de l’alerte brute.

Actions de la barre d'outils

Ce tableau répertorie les actions de la barre d'outils disponibles dans la vue Liste des alertes.

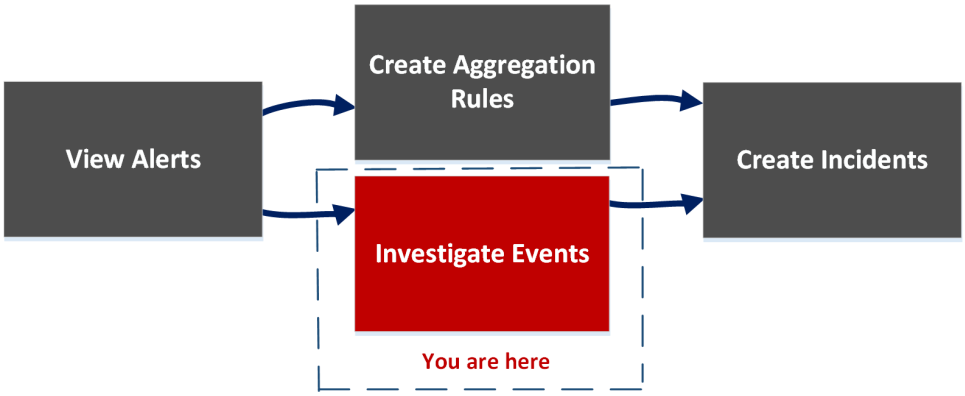
Option	Description
	Vous permet d'ouvrir le panneau Filtres afin que vous puissiez spécifier les alertes que vous aimeriez afficher dans la vue Liste des alertes.
	Ferme le panneau.
Bouton **Créer un incident**	Permet de créer des incidents à partir des alertes. Les alertes ne peuvent pas faire partie d'un incident. Pour obtenir la liste des alertes sans incidents, vous pouvez filtrer la Liste des alertes. Dans la section PARTIE INTÉGRANTE DE L'INCIDENT, sélectionnez Non.
Bouton **Supprimer**	Permet de supprimer des alertes.

Vue Détails relatifs aux alertes

Dans la vue Détails relatifs aux alertes (RÉPONDRE > Alertes > cliquez sur un lien hypertexte de NOM dans la liste des alertes), vous pouvez afficher des informations récapitulatives sur une alerte, telles que la source de l'alerte, le nombre d'événements au sein de l'alerte, et si elle fait partie ou non d'un incident. Vous pouvez également afficher des informations détaillées sur les événements au sein de l'alerte, ainsi que les métadonnées de l'événement.

Workflow

Ce workflow montre le processus de haut niveau que les analystes utilisent pour vérifier les alertes et créer des incidents.



Après avoir vérifié la liste des alertes, dans la vue Détails relatifs aux alertes, vous pouvez examiner ces alertes davantage et créer des incidents à partir des alertes. Dans CONFIGURER > vue RÈGLES DE L'INCIDENT, vous pouvez créer des règles d'agrégation pour créer des incidents.

Remarque : Vous pouvez également utiliser l'option Détection automatisée des menaces NetWitness Suite pour créer des incidents sans créer manuellement des règles.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Responsables de la réponse aux incidents, analystes	Afficher toutes les alertes dans NetWitness Suite.	Afficher les alertes

Rôle	Je souhaite...	Me montrer comment
Responsables du SOC, administrateurs	Créer des règles d'agrégation.	Reportez-vous à la rubrique « Création d'une règle d'agrégation pour les alertes » dans le *NetWitness Respond Guide de Configuration*.
Responsables de la réponse aux incidents, analystes	Afficher la liste des événements dans l'alerte.*	Afficher les détails relatifs à l'événement pour une alerte
Responsables de la réponse aux incidents, analystes	Afficher les métadonnées d'événements pour chaque événement dans l'alerte.*	Afficher les détails relatifs à l'événement pour une alerte
Responsables de la réponse aux incidents, analystes	Examiner les événements dans l'alerte.*	Examiner les événements
Responsables de la réponse aux incidents, analystes	Ajouter des alertes à un incident existant.	Ajouter des indicateurs associés à l'incident
Responsables de la réponse aux incidents, analystes	Créer des incidents à partir des alertes.	Créer un incident manuellement
Agents de confidentialité des données, administrateurs	Supprimer les alertes.	Supprimer les alertes

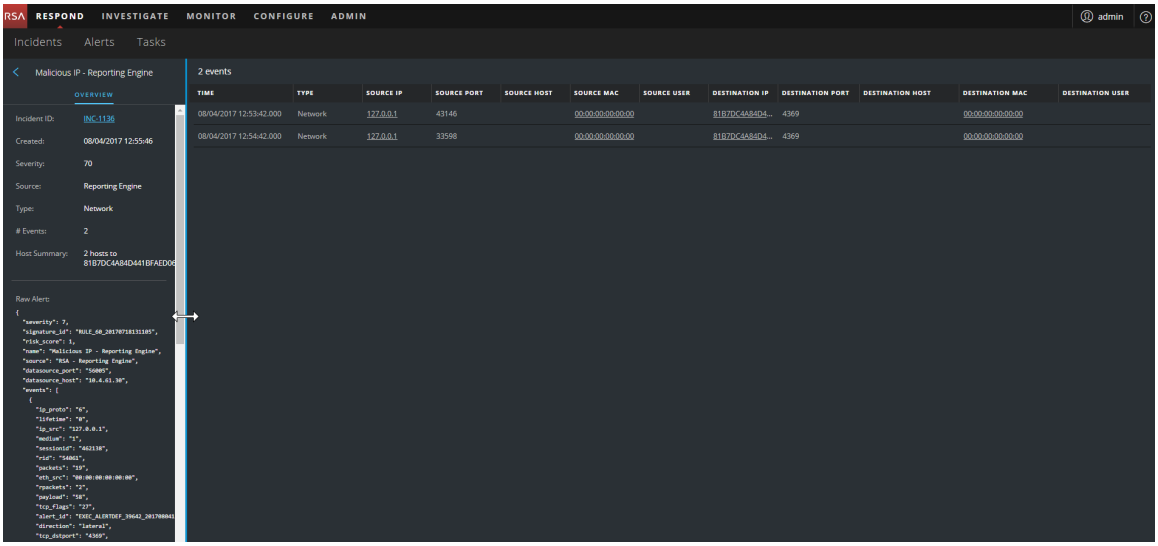
*Vous pouvez effectuer ces tâches ici (c'est-à-dire dans la vue Détails relatifs aux alertes).

Rubriques connexes

- Vue Liste des alertes
- Vérifier les alertes

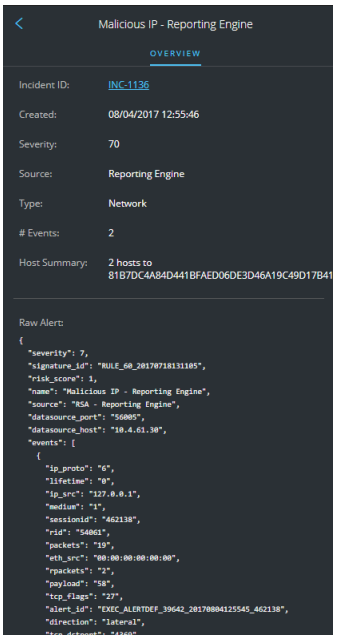
Vue Détails relatifs aux alertes

1. Pour accéder à la vue Détails relatifs aux alertes, accédez à **RÉPONDRE > Alertes**.
2. Dans la liste des alertes, choisissez une alerte à afficher, puis cliquez sur le lien dans la colonne NOM de cette alerte.
   La vue Détails relatifs aux alertes comporte un panneau Présentation sur la gauche et un panneau Événements sur la droite. Vous pouvez redimensionner les panneaux pour afficher plus d'informations, comme illustré sur la figure suivante.



Panneau Présentation

Le panneau Présentation contient des informations récapitulatives de base sur l'alerte sélectionnée. Le panneau Présentation de la vue Liste des alertes contient les mêmes informations. La rubrique Panneau Présentation de la vue Liste des alertes fournit des détails.

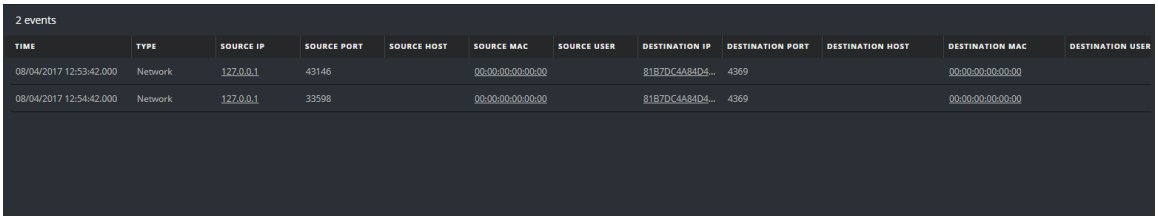


Panneau Événements

Le panneau Événements peut afficher une liste d'événements s'il existe plusieurs événements dans l'alerte. Si l'alerte comporte un seul événement ou si vous cliquez sur un événement dans la liste des événements, vous pouvez voir les détails relatifs à l'événement dans le panneau Événements.

Liste d'événements

La liste d'événements d'une alerte sélectionnée présente tous les événements contenus dans cette alerte.



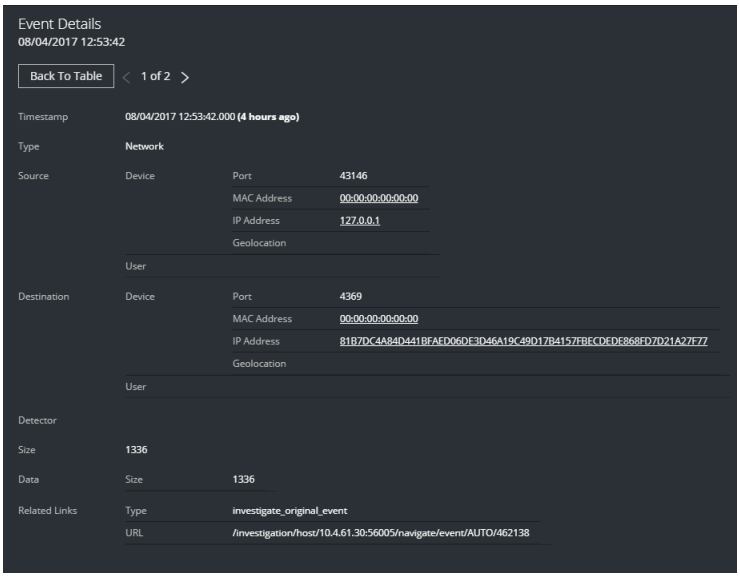
Le tableau suivant répertorie certaines des colonnes affichées dans la liste des événements, qui fournissent un résumé des événements répertoriés.

Colonne	Description
HEURE	Affiche l'heure à laquelle l'événement s'est produit.
TYPE	Affiche le type d'alerte, comme Log et Réseau.

Colonne	Description
IP SOURCE	Affiche l'adresse IP source s'il y a eu une transaction entre les deux machines.
IP DE DESTINATION	Affiche l'adresse IP de destination s'il y a eu une transaction entre les deux machines.
IP DÉTECTEUR	Affiche l'adresse IP de la machine sur laquelle une anomalie a été détectée.
UTILISATEUR SOURCE	Affiche l'utilisateur de la machine source.
UTILISATEUR DE DESTINATION	Affiche l'utilisateur de la machine de destination.
NOM DE FICHIER	Affiche le nom du fichier si un fichier est impliqué dans l'événement.
HACHAGE DE FICHIER	Présente un hachage du contenu du fichier.

Détails de l'événement

Les détails de l'événement contenus dans le panneau Événements affichent les métadonnées d'événement pour chaque événement de l'alerte.



Métadonnées de l'événement

Le tableau suivant répertorie des sections et sous-sections de métadonnées d'événement illustrées dans les deux premières colonnes des détails de l'événement. Cette liste n'est pas complète.

Section	Sous-section	Description
Données		Affiche des informations relatives aux données impliquées dans l'événement, telles que les fichiers concernés. Il peut en exister 0 ou plusieurs par événement.
	Nom du fichier	Affiche le nom du fichier si un fichier est impliqué dans l'événement.
	Hachage	Présente un hachage du contenu du fichier, par exemple, MD5 ou SHA1.
	Taille	Affiche la taille de la transmission ou du fichier impliqué dans l'événement.
Description		Affiche une description générale de l'événement.
Destination		Affiche l'utilisateur et le périphérique de destination.
	Périphérique	Affiche des informations relatives au périphérique de destination. Reportez-vous à la section Attributs de la source d'événement ou du périphérique de destination ci-dessous.
	Utilisateur	Affiche des informations relatives à l'utilisateur ou aux utilisateurs de la destination. Reportez-vous à la section Attributs de la source d'événement ou de l'utilisateur du périphérique de destination ci-dessous.
Détecteur		Présente le produit logiciel ou hôte qui a détecté le problème. Ceci est particulièrement vrai pour les logs et les scanneurs de malware

Section	Sous-section	Description
	Classe de périphérique	Affiche la classe du périphérique du produit qui a détecté l'alerte.
	Adresse IP	Affiche l'adresse IP du périphérique du produit qui a détecté l'alerte.
	Nom du produit	Affiche le nom du périphérique du produit qui a détecté l'alerte.
Domaine		Affiche le domaine associé à l'événement.
Enrichissement		Affiche les informations d'enrichissement disponibles.
Liens associés		Le cas échéant, affiche un lien vers l'interface utilisateur (IU) du produit source.
	Type	Affiche le type d'événement, tel qu'investigate_original_event.
	URL	Affiche le lien URL vers l'interface utilisateur du produit source.
Taille		Affiche la taille de la transmission ou du fichier impliqué.
Source		Affiche le périphérique source et l'utilisateur.
	Périphérique	Affiche des informations relatives à la machine source. Reportez-vous à la section Attributs de la source d'événement ou du périphérique de destination ci-dessous.
	Utilisateur	Affiche des informations relatives à l'utilisateur ou aux utilisateurs de la machine source. Reportez-vous à la section Attributs de la source d'événement ou de l'utilisateur du périphérique de destination ci-dessous.
Horodatage		Affiche l'heure à laquelle l'événement s'est produit.
Type		Affiche le type de l'alerte, par exemple log, réseau, corrélation, Renvoyer, Téléchargement manuel, À la demande, Partage de fichiers ou IOC instantané.

Attributs de la source d'événement ou du périphérique de destination

Le tableau suivant répertorie les attributs d'une source d'événement ou d'un périphérique de destination qui peuvent être affichés dans les détails des événements.

Nom	Description
Type de ressource	Affiche le type de périphérique, par exemple, ordinateur de bureau, ordinateur portable, serveur, équipement réseau, tablette, etc.
Entité	Affiche l'entité associée à .
Évaluation de la conformité	Indique le niveau de conformité du périphérique. Le niveau peut être Faible, Moyen ou Élevé.
Degré de criticité	Indique à quel point le périphérique est stratégique pour l'entreprise (criticité).
Site	Indique l'emplacement du périphérique.
Géolocalisation	Indique l'emplacement géographique de l'hôte. Peut contenir les attributs suivants : ville, pays, latitude, longitude, organisation et domaine.
Adresse IP	Affiche l'adresse IP du périphérique du périphérique.
Adresse MAC	Affiche l'adresse MAC du périphérique.
Nom NetBIOS	Affiche le nom NetBIOS du périphérique.
Port	Affiche le port TCP, le port UDP ou le port IP Src (le premier disponible) utilisé pour se connecter à l'hôte.

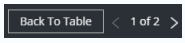
Attributs de la source d'événement ou de l'utilisateur du périphérique de destination

Le tableau suivant répertorie les attributs d'une source d'événement ou de l'utilisateur d'un périphérique de destination qui peuvent être affichés dans les détails des événements.

Nom de l'attribut	Description
Domaine AD	Affiche le domaine Active Directory.
Nom d'utilisateur AD	Affiche le nom de l'utilisateur Active Directory.
Adresse e-mail	Affiche l'adresse électronique de l'utilisateur.
Nom d'utilisateur	Affiche un nom général s'affiche si vous ne connaissez pas la source du nom d'utilisateur, par exemple UNIX ou un nom d'utilisateur dans un système spécifique.

Actions de la barre d'outils

Ce tableau répertorie les actions de la barre d'outils disponibles dans la vue Liste des alertes.

Option	Description
	(Revenir aux alertes) Vous permet de revenir à la vue Liste des alertes.
	Cliquez sur les flèches pour parcourir les détails des métadonnées d'événements pour chaque événement de l'alerte. Les nombres, tels que « 1 sur 2 », affichent le numéro de l'événement que vous visualisez. Cliquez sur **Revenir au Tableau** pour revenir à la vue Liste des événements, également appelée Tableau des événements.

Vue Liste des tâches

Après avoir effectué une enquête sur les incidents, dans la vue Liste des tâches (RÉPONDRE > Tâches), vous pouvez créer et suivre les tâches d'un incident. Par exemple, vous pouvez créer des tâches de correction lorsque vous avez besoin d'actions sur les incidents de la part d'équipes en dehors de vos opérations de sécurité. Vous pouvez référencer des numéros de tickets externes dans les tâches et ensuite effectuer le suivi de ces tâches, jusqu'à la fin. Vous pouvez également modifier et supprimer des tâches selon les besoins, en fonction de vos autorisations d'utilisateur.

Que voulez-vous faire ?

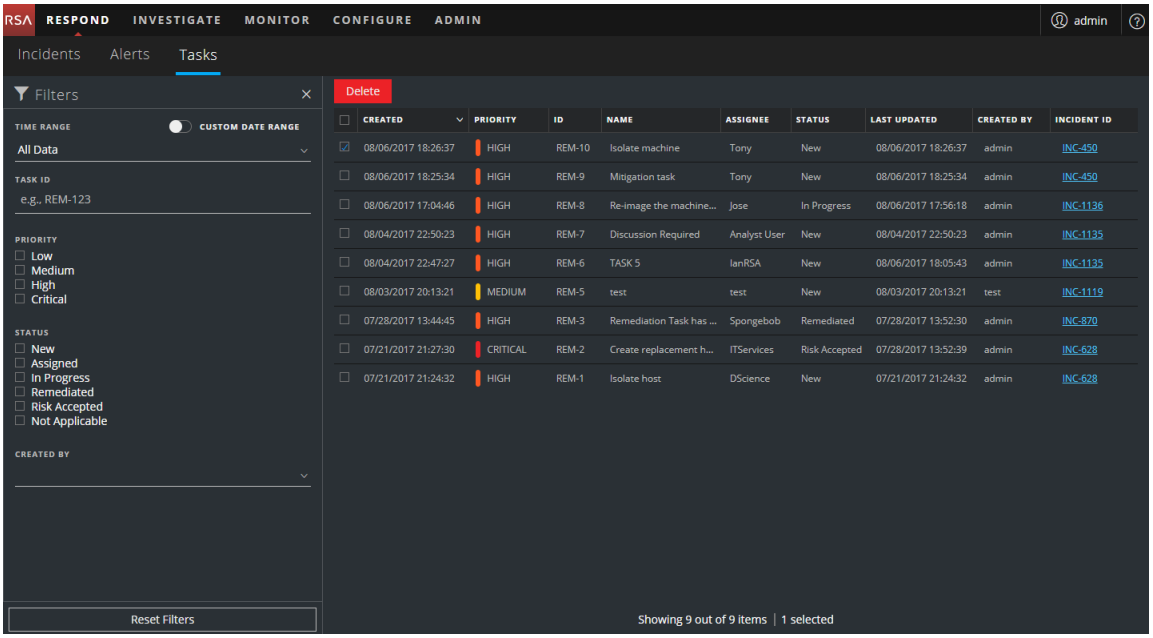
Rôle	Je souhaite...	Me montrer comment
Responsables de la réponse aux incidents, analystes	Afficher les tâches.	Afficher toutes les tâches d'incident et Afficher les tâches associées à un incident
Responsables de la réponse aux incidents, analystes	Filtrer des tâches.	Filtrer la liste des tâches
Responsables de la réponse aux incidents, analystes	Créer une tâche.	Créer une tâche
Responsables de la réponse aux incidents, analystes	Rechercher et modifier des tâches.	Recherche d'une tâche et Modifier une tâche
Responsables de la réponse aux incidents, analystes	Fermer une tâche (remplacer l'état par Corrigé, Risque accepté ou Sans objet).	Modifier une tâche
Responsables de la réponse aux incidents, analystes, responsables du SOC	Déléguer une tâche.	Déléguer une tâche

Rubriques connexes

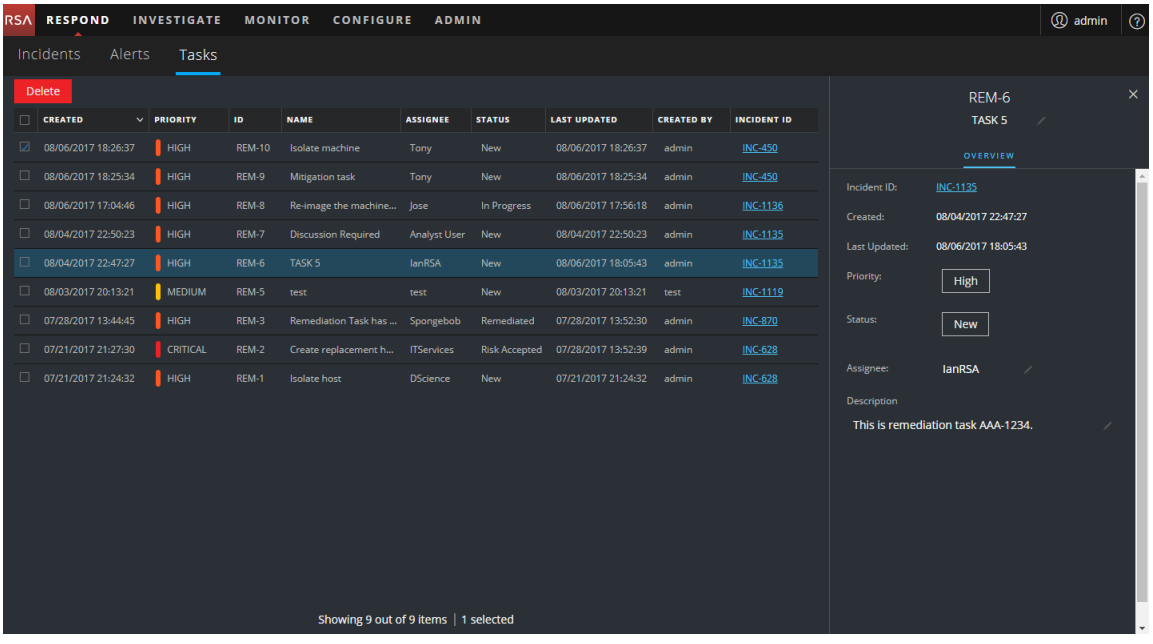
- Vue Détails sur l'incident
- Faire remonter ou corriger l'incident

Listes des tâches

Pour accéder à la vue Liste des tâches, allez à **RÉPONDRE >Tâches**. La vue Liste des tâches affiche la liste de toutes les tâches de l'incident.

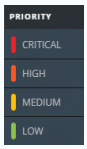


La vue Liste des tâches comprend un panneau Filtres, un panneau Liste des tâches et un panneau Présentation de la tâche. La figure suivante présente la vue Liste des tâches et le panneau Présentation.



Listes des tâches

La liste des tâches affiche toutes les tâches de l'incident. Vous pouvez filtrer cette liste pour afficher uniquement les tâches intéressantes.

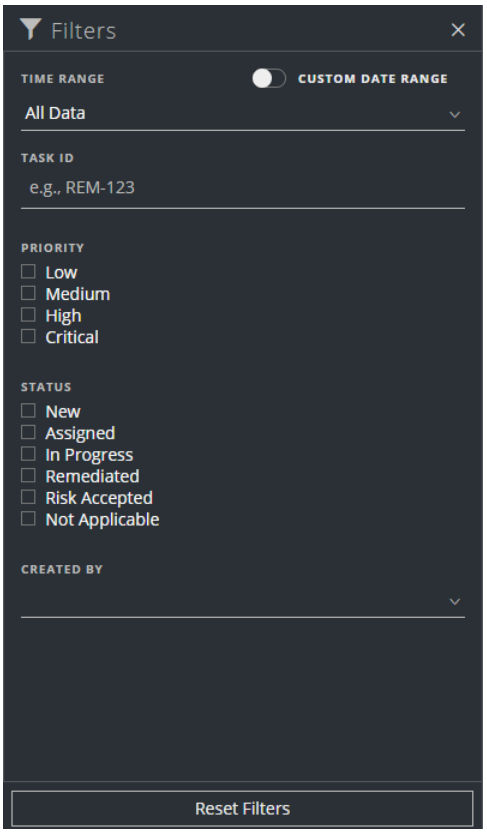
Colonne	Description
	Vous permet de sélectionner une ou plusieurs tâches à modifier ou supprimer. Les utilisateurs disposant des autorisations appropriées peuvent effectuer des mises à jour et supprimer des tâches en bloc, comme des responsables du SOC. Par exemple, un responsable du SOC peut souhaiter attribuer plusieurs tâches à un utilisateur en même temps.
CRÉÉ	Affiche la date de création de la tâche.
PRIORITÉ	Affiche la priorité attribuée à la tâche. La priorité peut être l'une des suivantes : Critique, Élevé, Moyen ou Faible. La priorité est également indiquée à l'aide d'un code couleur, où rouge indique **Critique**, orange représente un risque **Élevé**, jaune indique un risque **Moyen** et vert représente un risque **Faible**, comme illustré dans la figure suivante : 
ID	Affiche l'ID de tâche.
NOM	Affiche le nom de la tâche.
PERSONNE AFFECTÉE	Affiche le nom de l'utilisateur auquel la tâche est attribuée.
ÉTAT	Affiche l'état de la tâche : Nouveau, Attribué, En cours, Corrigé, Risque accepté et Sans objet.
DERNIÈRE MISE À JOUR	Affiche la date et l'heure auxquelles la tâche a été mise à jour pour la dernière fois.

Colonne	Description
CRÉÉ PAR	Affiche l'utilisateur qui a créé la tâche.
ID DE L'INCIDENT	Affiche l'ID d'incident pour lequel la tâche a été créée. Cliquez sur cet ID pour afficher les détails de l'incident.

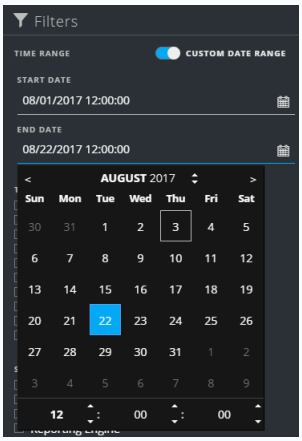
Au bas de la liste, vous voyez le nombre de tâches sur la page en cours et le nombre total de tâches. Par exemple : **Affichage de 23 éléments sur 23**

Panneau Filtres

La figure suivante présente les filtres disponibles dans le panneau Filtres.



Le panneau Filtres, sur la gauche de la vue Liste des tâches, propose des options que vous pouvez utiliser pour filtrer les tâches de l'incident.

Option	Description
PÉRIODE	Vous pouvez sélectionner une période spécifique dans la liste déroulante Période. La période est basée sur la date de création des tâches. Par exemple, si vous sélectionnez Dernière heure, vous verrez les tâches qui ont été créées au cours des 60 dernières minutes.
PLAGE DE DATES PERSONNALISÉE	Vous pouvez spécifier une plage de dates spécifique au lieu de sélectionner une option de période. Pour ce faire, cliquez sur le cercle blanc devant Plage de dates personnalisée pour afficher les champs Date de début et Date de fin. Sélectionnez les dates et heures dans le calendrier. 
ID DE LA TÂCHE	Vous pouvez saisir l'ID de tâche pour une tâche que vous souhaitez localiser, par exemple REM-123.
PRIORITÉ	Vous pouvez sélectionner les priorités que vous souhaitez afficher. Si vous effectuez une ou plusieurs sélections, la liste des tâches affiche uniquement les tâches avec les priorités sélectionnées. Si vous sélectionnez Critique, le panneau Tâches affiche uniquement les tâches possédant la priorité Critique.

Option	Description
ÉTAT	Vous pouvez sélectionner les états que vous souhaitez afficher. Si vous effectuez une ou plusieurs sélections, la liste Tâches affiche uniquement les tâches avec les états sélectionnés. Par exemple : si vous sélectionnez Attribué, le panneau Tâches affiche uniquement les tâches qui sont attribuées aux utilisateurs.
CRÉÉ PAR	Vous pouvez sélectionner l'utilisateur qui a créé les tâches que vous souhaitez afficher. Par exemple, si vous souhaitez afficher les tâches créées par Edwardo uniquement, sélectionnez Edwardo dans la liste déroulante CRÉÉ PAR. Si vous souhaitez afficher les tâches quelle que soit la personne qui a créé la tâche, n'effectuez aucune sélection sous CRÉÉ PAR.
Réinitialiser les filtres	Supprime vos sélections de filtre.

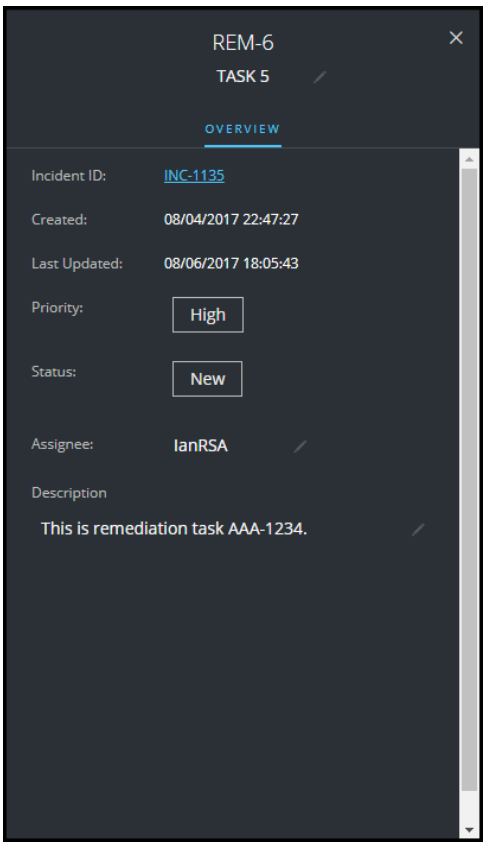
La liste des tâches affiche une liste de tâches qui répondent à vos critères de sélection. Vous pouvez voir le nombre d'éléments dans votre liste filtrée en bas de la liste des tâches. Par exemple : **Affichage de 18 éléments sur 18**

Panneau Présentation de la tâche

Pour accéder au panneau Présentation de la tâche :

1. Accédez à **RÉPONDRE > Tâches**.

2. Dans la liste Tâches, cliquez sur la tâche que vous voulez afficher.
   Le panneau Présentation de la tâche s'affiche à droite de la liste Tâches.



Le tableau suivant répertorie les champs affichés dans le panneau Présentation de la tâche.

Champ	Description
<ID de la tâche>	Affiche l'ID de tâche automatiquement attribué.
<Nom de la tâche>	Affiche le nom de la tâche. Ce champ est modifiable. Pour modifier le nom de la tâche, vous pouvez cliquer sur le nom actuel de la tâche pour ouvrir un éditeur de texte. Par exemple, vous pouvez remplacer un nom de la tâche « Créer une nouvelle image d'un ordinateur portable » par « Créer une nouvelle image d'un serveur ».
ID d'incident	Affiche l'ID d'incident pour lequel la tâche a été créée. Cliquez sur cet ID pour afficher les détails de l'incident.
Créé	Affiche des détails sur la date et l'heure de création de la tâche.

Champ	Description
Dernière mise à jour	Affiche la date et l'heure auxquelles la tâche a été mise à jour pour la dernière fois.
Priorité	Affiche la priorité de la tâche : Faible, Moyen, Élevé ou Critique. Pour modifier la priorité, vous pouvez cliquer sur le bouton de priorité et sélectionner une priorité pour la tâche dans la liste déroulante.
État	Affiche l'état de la tâche : Nouveau, Attribué, En cours, Corrigé, Risque accepté et Sans objet. Pour modifier l'état, vous pouvez cliquer sur le bouton d'état et sélectionner un état de la tâche dans la liste déroulante.
Personne affectée	Affiche l'utilisateur affecté à la tâche. Pour modifier l'utilisateur affecté à la tâche, vous pouvez cliquer sur (Non attribué) ou le nom de la personne affectée précédente pour ouvrir un éditeur de texte.
Description	Affiche les détails de la tâche. Pour modifier la description, vous pouvez cliquer sur le texte situé sous la description afin d'ouvrir un éditeur de texte.

Actions de la barre d'outils

Ce tableau répertorie les actions de la barre d'outils disponibles dans la vue Liste des tâches.

Option	Description
	Vous permet d'ouvrir le panneau Filtres afin que vous puissiez spécifier les tâches que vous aimeriez afficher dans la liste Tâches.
	Ferme le panneau.
Bouton **Supprimer**	Vous permet de supprimer les tâches sélectionnées.

Boîte de dialogue Ajouter à la liste/Supprimer de la liste

La boîte de dialogue Ajouter à la liste/Supprimer de la liste permet d'ajouter une valeur d'entité ou une métadonnée à une liste existante, ou de l'en supprimer, ou encore de créer une nouvelle liste. Par exemple, lorsque vous recherchez une adresse IP et que vous la trouvez suspecte ou intéressante, vous pouvez l'ajouter à une liste pertinentes, qui a été ajoutée à une source de données. Cela améliore la visibilité des adresses IP suspectes. Vous pouvez également ajouter des entités ou des métadonnées à différentes listes. Par exemple, vous pouvez les ajouter à une liste de domaines suspects liés à des connexions de commande et de contrôle, et à une autre liste concernant les adresses IP liées aux connexions de chevaux de Troie autorisant un accès à distance. Si aucune liste n'est disponible, vous pouvez en créer une. Vous pouvez également supprimer les entités ou les métadonnées d'une liste.

Remarque : À partir de la boîte de dialogue Ajouter à la liste/Supprimer de la liste, vous pouvez uniquement ajouter (ou supprimer) des entités ou métadonnées dans des listes à colonne unique ajoutées comme sources de données, et non comme listes à plusieurs colonnes. Et lorsque vous modifiez une liste ou une valeur dans une liste à partir de la vue nodale ou de la vue de recherche contextuelle, veillez à actualiser la page Web pour afficher les données mises à jour.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Responsables de la réponse aux incidents, analystes	Ajouter une entité à une liste.	Dans la vue Détails sur l'incident, reportez-vous à la section Ajouter une entité à une liste blanche. Dans la vue Détails relatifs aux alertes, reportez-vous à la section Ajouter une entité à une liste blanche.
Responsables de la réponse aux incidents, analystes	Créer une liste blanche, une liste noire ou une autre liste.	Créer une liste
Administrateurs	Ajouter une liste Context Hub en tant que source de données.	Consultez la rubrique « Configurer des listes en tant que sources de données » du *Guide de configuration de Context Hub*.

Rôle	Je souhaite...	Me montrer comment
Administrateurs	Importer ou exporter des listes pour Context Hub.	Consultez la rubrique « Importer ou exporter des listes pour Context Hub » dans le *Guide de configuration de Context Hub*.

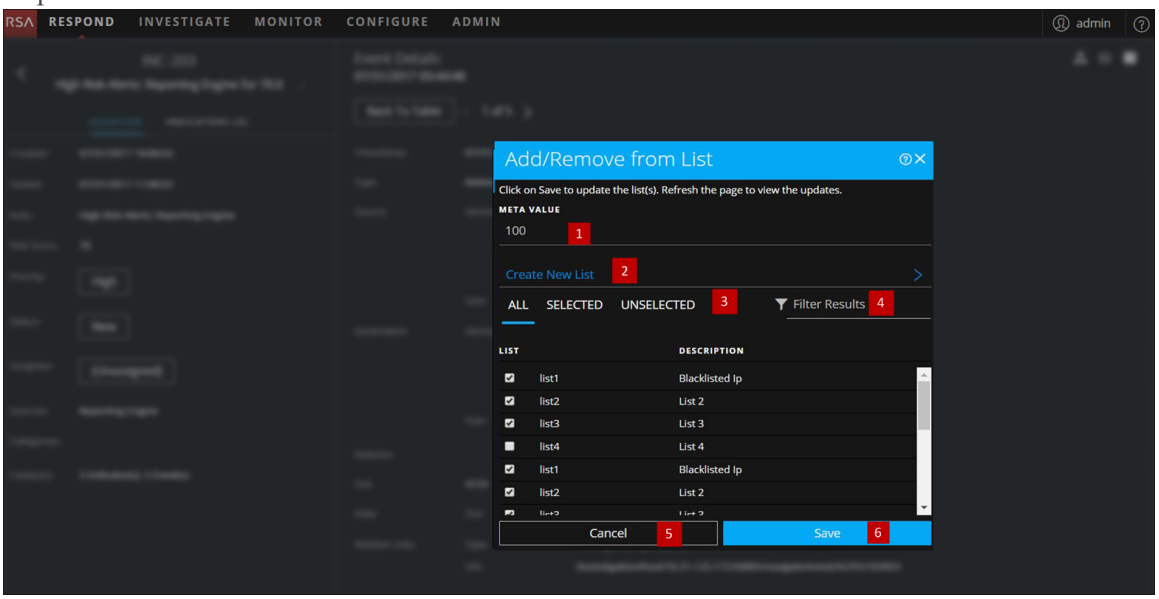
Rubriques connexes

- Enquêter sur l'incident
- Vérifier les alertes
- Afficher les informations contextuelles (vue Détails sur l'incident)
- Afficher les informations contextuelles (vue Détails relatifs aux alertes)

Remarque : Vous ne pouvez pas supprimer une liste, mais vous pouvez supprimer des valeurs d'une liste.

Aperçu rapide

Voici un exemple de la boîte de dialogue **Ajouter à la liste/Supprimer de la liste** de la vue Répondre.



1 Entités ou métadonnées à ajouter ou supprimer.

2 Créer une nouvelle liste à l'aide des métadonnées sélectionnées.

3 Sélectionnez l'un des onglets : Tous, Sélectionné ou Désélectionné.

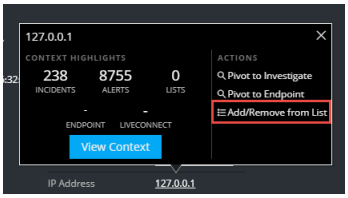
4 Effectuer une recherche à l'aide du nom de la liste ou de sa description.

5 Annuler l'action.

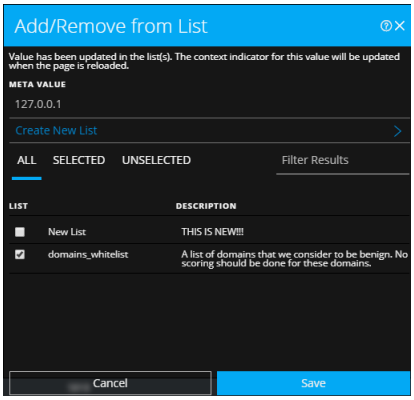
6 Enregistrer pour mettre à jour les listes ou créer une nouvelle liste.

Ajouter à la liste/Supprimer de la liste

Pour accéder à la boîte de dialogue Ajouter à la liste/Supprimer de la liste, dans la vue Détails sur l'incident ou la vue Détails relatifs aux alertes, survolez l'entité soulignée que vous souhaitez ajouter ou supprimer d'une liste de Context Hub. Une info-bulle contextuelle s'affiche et présente les actions disponibles.



Dans la section Actions de l'info-bulle, cliquez sur Ajouter à la liste/Supprimer de la liste. La boîte de dialogue Ajouter à la liste/Supprimer de la liste affiche les listes disponibles.



Le tableau suivant présente les options de la boîte de dialogue Ajouter à la liste/Supprimer de la liste.

Option	Description
VALEUR MÉTA	Affiche l'entité ou la métadonnée sélectionnée qui doit être ajoutée ou supprimée à partir d'une ou plusieurs listes. Vous pouvez également créer une nouvelle liste à l'aide de la valeur sélectionnée.

Option	Description
Créer une nouvelle liste	Lorsque vous cliquez sur cette option, une boîte de dialogue vous permet de créer une nouvelle liste à l'aide de la métadonnée sélectionnée.
TOUT	Affiche toutes les listes de Context Hub disponibles. Les listes qui contiennent l'entité ou la métadonnée sélectionnée sont sélectionnées. Cochez une case pour ajouter une entité ou une métadonnée à une liste. Désactivez une case à cocher pour la supprimer de la liste.
SÉLECTIONNÉ	Affiche les listes qui contiennent l'entité ou la métadonnée sélectionnée. (Toutes les listes sont sélectionnées.)
DÉSÉLECTIONNÉ	Affiche uniquement les listes qui contiennent l'entité ou la métadonnée sélectionnée. (Toutes les listes sont désélectionnées.)
Filtrage des résultats	Saisissez le nom ou la description d'une liste spécifique pour effectuer la recherche dans plusieurs listes.
LISTE	Affiche le nom de toutes les listes.
DESCRIPTION	Affiche des informations relatives à la liste sélectionnée. La description que vous fournissez lors de la création d'une liste s'affiche dans cette boîte de dialogue. Par exemple : Cette liste contient toutes les adresses IP répertoriées dans la liste noire.
Annuler	Annule l'opération.
Enregistrer	Enregistre les modifications.

Panneau Recherche contextuelle - Vue Répondre

Le service Context Hub rassemble des informations contextuelles issues de plusieurs sources de données dans la vue Répondre pour permettre aux analystes de prendre de meilleures décisions durant leurs analyses et d'appliquer les mesures appropriées. En affichant les entités, les métadonnées 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 la vue Répondre et qui englobent une entité ou une métadonnée s'affichent lorsque l'analyste recherche des informations contextuelles pour cette entité ou cette métadonnée. Le panneau Recherche contextuelle affiche les informations contextuelles relatives aux entités ou aux métadonnées sélectionnées telles que : Adresse IP, Utilisateur, Hôte, Domaine, Nom du fichier ou Hachage de fichier. Les données disponibles varient selon les sources configurées dans le service Context Hub.

Le panneau Recherche contextuelle affiche les informations contextuelles en fonction des données disponibles dans les sources configurées du service Context Hub.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Responsables de la réponse aux incidents, analystes, responsables de la recherche des menaces	Accéder au panneau Recherche contextuelle.	Dans la vue Détails sur l'incident, vous pouvez Afficher les informations contextuelles . Dans la vue Détails relatifs aux alertes, vous pouvez Afficher les informations contextuelles .
Responsables de la réponse aux incidents, analystes, responsables de la recherche des menaces	Comprendre les informations contenues dans le panneau Recherche contextuelle pour une entité sélectionnée.	Consultez les informations contenues dans cette rubrique.
Administrateur	Configurer des sources de données pour Context Hub.	Consultez la rubrique « Configurer les sources de données du service Context Hub » du *Guide de configuration de Context Hub*.

Rôle	Je souhaite...	Me montrer comment
Administrateur	Configurer les paramètres de Context Hub.	Consultez la rubrique « Configurer les paramètres de source de données pour Context Hub » du *Guide de configuration de Context Hub*.

Rubriques connexes

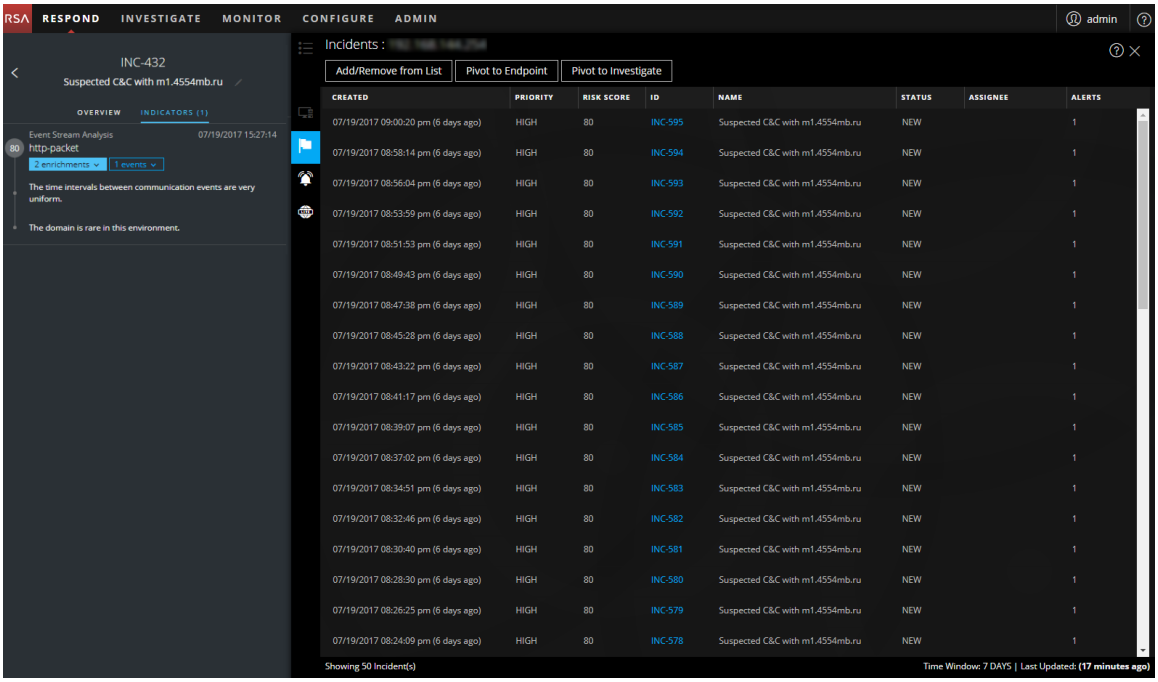
- Enquêter sur l'incident
- Vérifier les alertes

Informations contextuelles affichées dans le panneau Recherche contextuelle

Les informations contextuelles ou les résultats de la requête affichés dans le panneau Recherche contextuelle dépendent de l'entité sélectionnée et des sources de données associées.

Le panneau Recherche contextuelle comporte des onglets distincts pour chacune des sources de données. L'onglet Source de données de liste est l'onglet affiché en premier dans le panneau contextuel, suivi par Archer, EndPoint, Incidents, Alertes et Live Connect.

La figure suivante affiche le panneau Recherche contextuelle pour une entité sélectionnée dans la vue Détails sur l'incident. Onglet Incidents du panneau Recherche contextuelle.



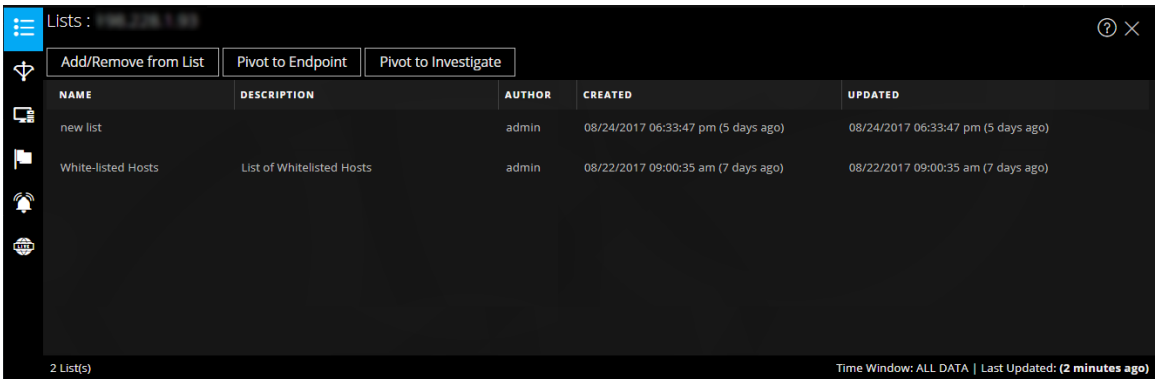
Le tableau suivant décrit les données disponibles sur chaque onglet et les entités prises en charge.

Onglet	Description	Entités prises en charge
(Listes)	Affiche toutes les données de liste associées à l'entité ou aux métadonnées sélectionnées. Le résultat est trié selon la dernière liste mise à jour.	Toutes les entités
(Archer)	Affiche des informations relatives aux ressources, ainsi que la criticité, à l'aide de la source de données Archer.	IP et hôte
(Active Directory)	Affiche toutes les informations utilisateur pour l'utilisateur sélectionné.	Utilisateur

Onglet	Description	Entités prises en charge
 (NetWitness Endpoint)	Affiche les informations de source de données NetWitness Endpoint pour l'entité ou les métadonnées sélectionnées, notamment les machines, les modules et les niveaux IIOC. Les modules sont triés de la valeur IOC la plus élevée à la valeur IIOC la plus faible et les niveaux IIOC sont triés du niveau IOC le plus élevé au niveau IOC le plus faible.	IP, adresse MAC et hôte
 (Incidents)	Affiche la liste des incidents associés à l'entité ou aux métadonnées sélectionnées. Le résultat est trié des incidents les plus récents aux incidents les plus anciens.	Toutes les entités
 (Alertes)	Affiche la liste des alertes associées à l'entité ou aux métadonnées sélectionnées. Le résultat est trié des alertes les plus récentes aux alertes les plus anciennes.	Toutes les entités
 (Live Connect)	Affiche les informations relatives à Live Connect.	IP, domaine et hachage de fichier

Listes

Le panneau Recherche contextuelle des listes présente une ou plusieurs listes associées à l'entité sélectionnée ou la métadonnée sélectionnée. La figure suivante offre un exemple du panneau Recherche contextuelle pour les listes.

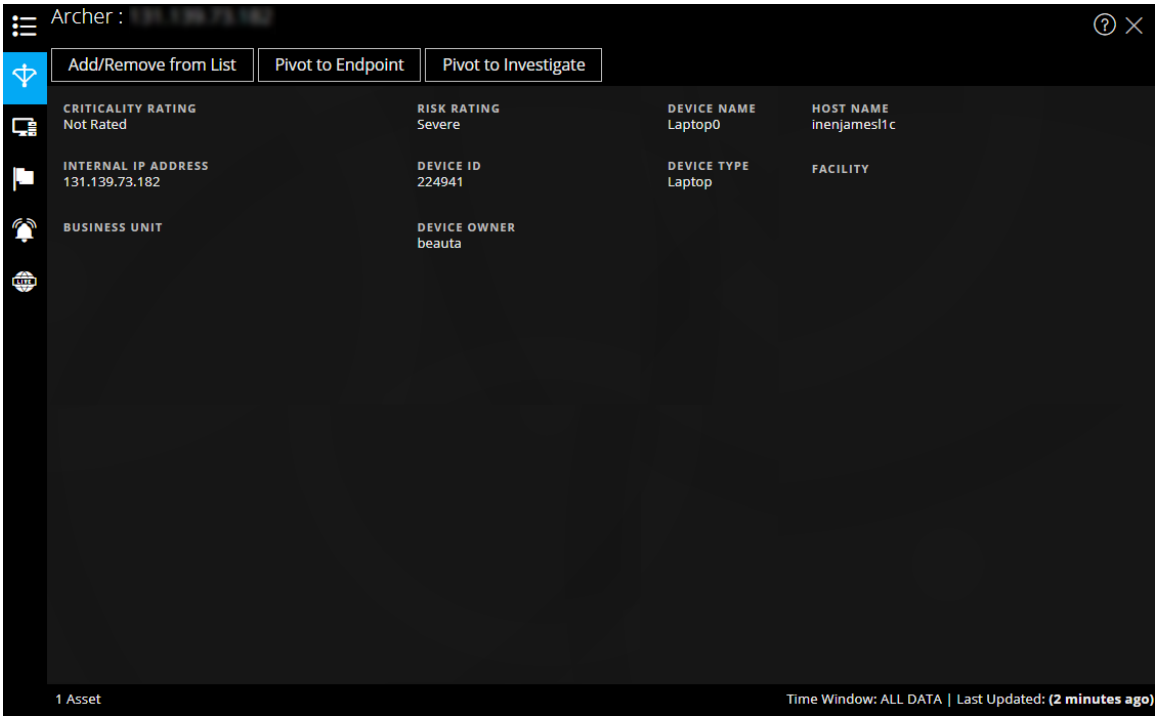


Les informations suivantes s'affichent pour les listes.

Champ	Description
Nom	Nom de la liste (défini lors de la création de la liste).
Description	Description de la liste (définie lors de la création de la liste).
Auteur	Propriétaire ayant créé la liste.
Créé	Date de création de la liste.
Mise à jour	Date de mise à jour ou de modification de la liste.
Nombre	Nombre de listes dans lesquelles l'entité ou la métadonnée sélectionnée est disponible.
Période	Elle se base sur la valeur définie dans le champ « Requête dans les derniers » de la fenêtre Configurer les réponses. Par défaut, toutes les données de listes sont extraites.
Dernière mise à jour	Heure à laquelle le service Context Hub a extrait et stocké les données recherchées dans le cache.

Archer

Le panneau Recherche contextuelle d'Archer affiche des informations relatives aux ressources, ainsi que la criticité à l'aide de la source de données Archer pour les entités et métadonnées IP et Hôte. La figure suivante offre un exemple du panneau Recherche contextuelle d'Archer.



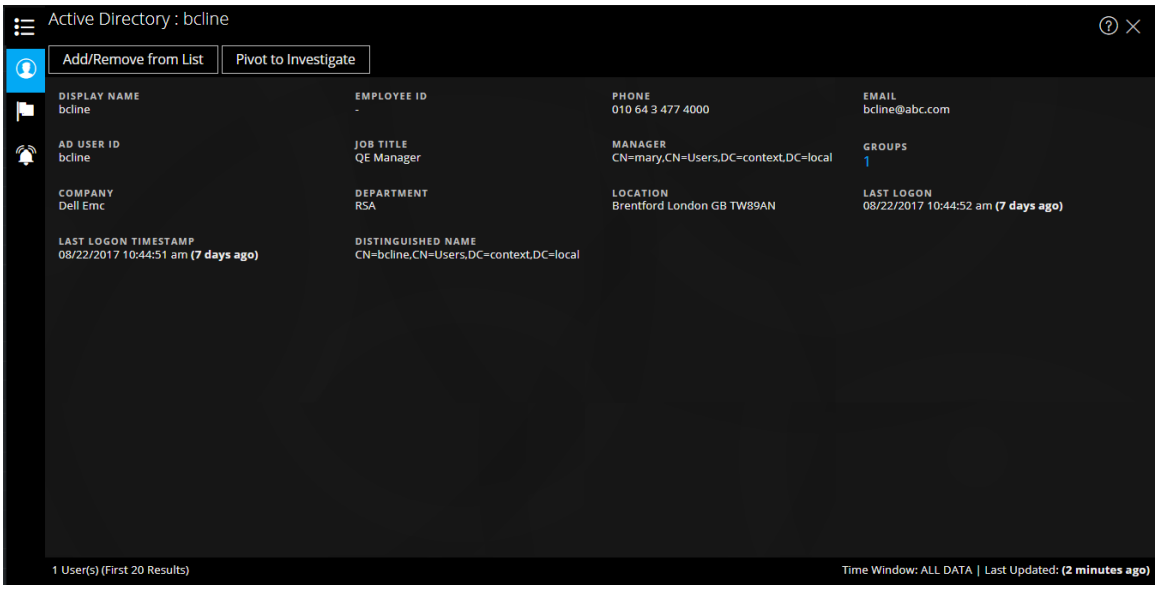
Les informations suivantes s'affichent pour Archer.

Champ	Description
Degré de criticité	Affiche le degré de criticité opérationnel du périphérique en fonction des applications que ce dernier prend en charge. La criticité peut avoir les valeurs Non évaluée, Faible, Relativement faible, Moyenne, Relativement élevée, ou Élevée.
ID du périphérique	Ce champ affiche la valeur indiquée automatiquement, qui identifie de manière unique l'enregistrement parmi toutes les applications du système.
Nom du périphérique	Affiche le nom unique du périphérique.
Propriétaire du périphérique	Affiche les propriétaires responsables du périphérique qui bénéficient des droits en lecture et mise à jour sur l'enregistrement.

Champ	Description
Nom d'hôte	Affiche le nom d'hôte du périphérique.
Sites	Ce champ fournit des liens vers les enregistrements relatifs à ce périphérique dans l'application Sites.
Entité	Fournit des liens vers les enregistrements associés à ce périphérique dans l'application Entité.
Évaluation des risques	Ce champ identifie le risque estimé pour le périphérique sur la base de la dernière évaluation, ainsi que le risque moyen pour les sites utilisant ce dernier. L'évaluation du risque peut être définie comme étant Grave, Élevée, Moyenne, Faible, ou Minimale.
Type	Affiche le type de périphérique tel que serveur, ordinateur portable, ordinateur de bureau, etc.
Adresse IP	Affiche l'adresse IP interne principale du périphérique.
Nombre	Affiche le nombre de ressources disponibles.
Période	Elle se base sur la valeur définie dans le champ « Requête dans les derniers » de la fenêtre Configurer les réponses. Par défaut, toutes les données Archer sont extraites.
Dernière mise à jour	Heure à laquelle le service Context Hub a extrait et stocké les données recherchées dans le cache.

Active Directory

La figure suivante offre un exemple du panneau contextuel d'Active Directory.



Le panneau Recherche contextuelle d'Active Directory affiche l'ensemble des informations, incidents et alertes connexes pour un utilisateur. Vous pouvez effectuer la recherche à l'aide des formats suivants :

- userPrincipalName
- Domain\UserName
- sAMAccountName

Si l'utilisateur existe dans plusieurs domaines ou plusieurs forêts, toutes les informations de contexte associées sont affichées pour l'utilisateur spécifique.

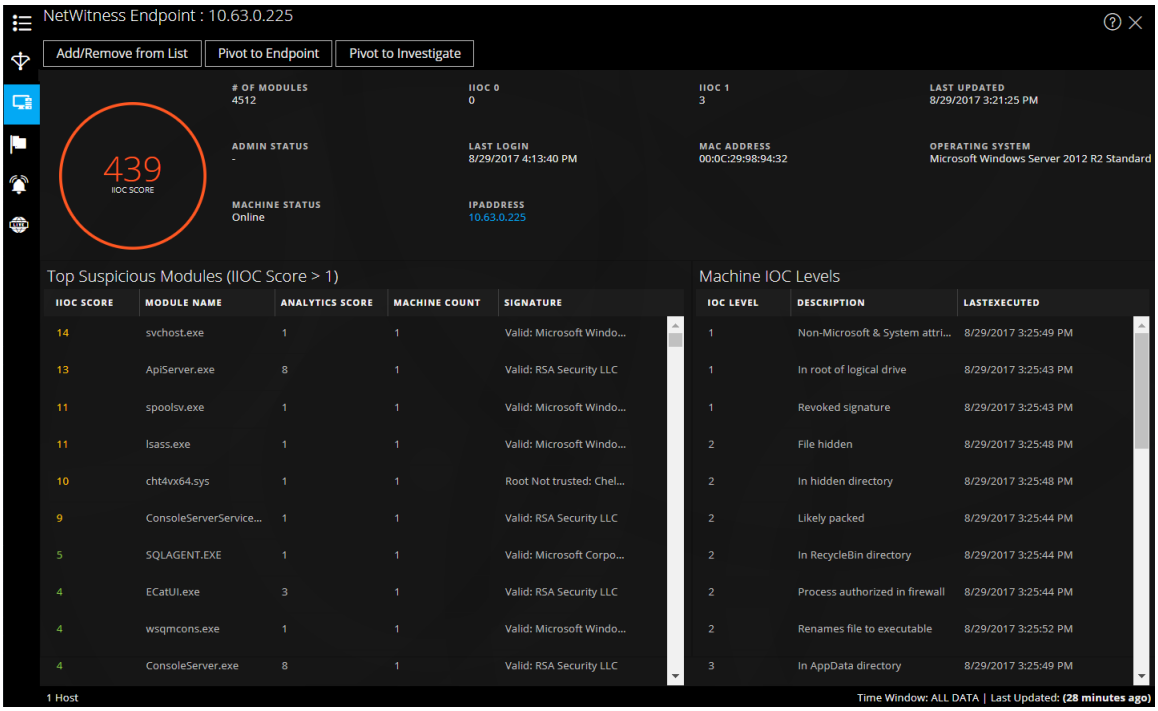
Les informations suivantes s'affichent pour Active Directory.

Champ	Description
Nom d'affichage	Affiche le nom de l'utilisateur.
ID de l'employé	Affiche l'ID d'employé de l'utilisateur.
Téléphone	Affiche le numéro de téléphone de l'utilisateur.
E-mail	Affiche l'ID e-mail de l'utilisateur.
ID utilisateur AD	Affiche l'identification unique de l'utilisateur spécifique au sein d'une organisation.
Poste	Affiche la désignation de l'utilisateur.
Gestionnaire	Affiche le nom du responsable de
Groupes	Affiche la liste des groupes dont l'utilisateur est membre.

Champ	Description
Entreprise	Affiche le nom de l'entreprise à laquelle appartient l'utilisateur spécifique.
Département	Affiche le nom du département de l'organisation auquel appartient l'utilisateur spécifique.
Emplacement	Affiche l'emplacement de l'utilisateur.
Dernière connexion	Affiche l'heure à laquelle l'utilisateur spécifique s'est connecté au système, uniquement si le Catalogue global est défini.
Horodatage de la dernière connexion	Affiche l'heure à laquelle l'utilisateur spécifique s'est connecté au système.
Nom unique	Affiche le nom unique attribué à l'utilisateur.
Nombre	Affiche le nombre d'utilisateurs.
Période	Elle se base sur la valeur définie dans le champ « Requête dans les derniers » de la fenêtre Configurer les paramètres des sources de données. Par défaut, toutes les données Active Directory sont extraites.
Dernière mise à jour	Heure à laquelle le service Context Hub a extrait et stocké les données recherchées dans le cache.

NetWitness Endpoint

Le panneau Recherche contextuelle de NetWitness Endpoint affiche les informations suivantes.



Les informations suivantes s'affichent pour IIOC.

Champ	Description
Nbre de modules	Affiche le nombre de modules sur lesquels porte la recherche.
État admin	Affiche l'état admin (le cas échéant).
Dernière mise à jour	Affiche l'heure de la dernière actualisation des données.
Dernière connexion	Affiche l'heure à laquelle l'utilisateur s'est connecté pour la dernière fois.
Adresse MAC	Adresse MAC de la machine.
Système d'exploitation	Version du système d'exploitation utilisé par la machine NetWitness Endpoint.
État de l'ordinateur	Indique si le module consulté est En ligne, Hors ligne, Actif ou Inactif.
Adresse IP	Affiche l'adresse IP du module spécifique.

Les informations suivantes s'affichent pour les modules.

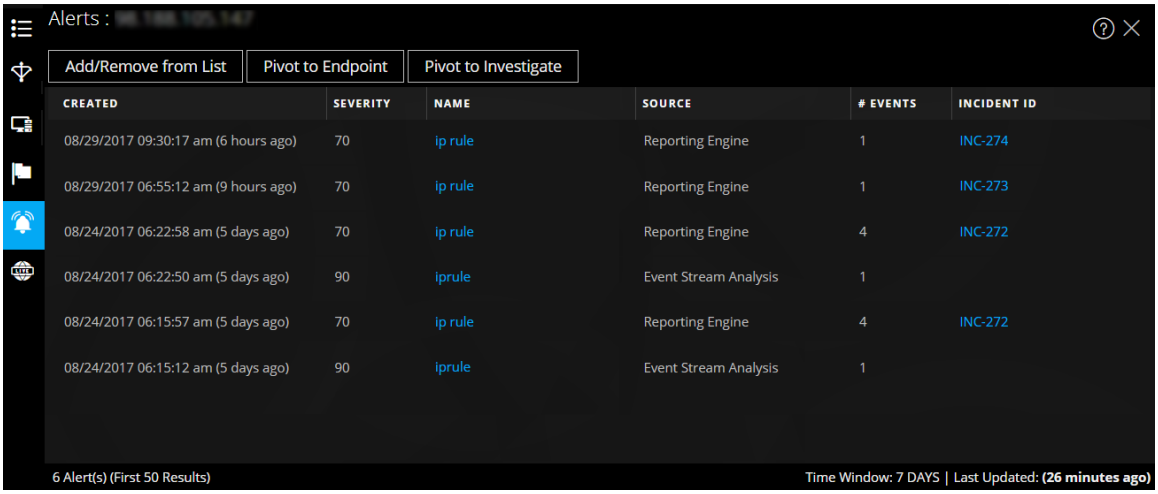
Champ	Description
Score IIOC	Le score IIOC de la machine est un score agrégé basé sur les scores des modules. Cela dépend de la valeur définie pour le champ « Valeur IIOC minimale » dans les paramètres de source de données pour Context Hub. La valeur par défaut pour « Valeur IIOC minimale » est 500. Consultez la rubrique « Configurer les paramètres de source de données pour Context Hub » du *Guide de configuration de Context Hub*.
Nom du module	Nom du module qui est consulté.
Score d'analyse	Nombre de fichiers actifs pour la machine sélectionnée.
Nombre de machines	Indique le moment de la dernière mise à jour des résultats de l'analyse dans la base de données NetWitness Endpoint.
Signature	Indique si le fichier est signé ou non signé, valide ou non valide et fournit des informations relatives aux signataires. Par exemple, Google, Apple, etc.

Les informations suivantes s'affichent pour les machines.

Champ	Description
Niveaux IOC	Affiche les niveaux IOC.
Description	Affiche la description les niveaux IOC, le cas échéant.
Dernière exécution	Affiche l'heure à laquelle la tâche a été exécutée.
Nombre	Affiche le nombre d'hôtes sur lesquels porte la recherche.
Période	Elle se base sur la valeur définie dans le champ « Requête dans les derniers » de la fenêtre Configurer les paramètres des sources de données. Par défaut, toutes les données NetWitness Endpointsont extraites.
Dernière mise à jour	Indique le moment de la dernière mise à jour des résultats de l'analyse dans la base de données NetWitness Endpoint.

Alertes

La figure suivante est un exemple du panneau contextuel pour Alertes qui s'affiche en fonction de l'heure (du plus récent au plus ancien), puis de l'état de gravité.



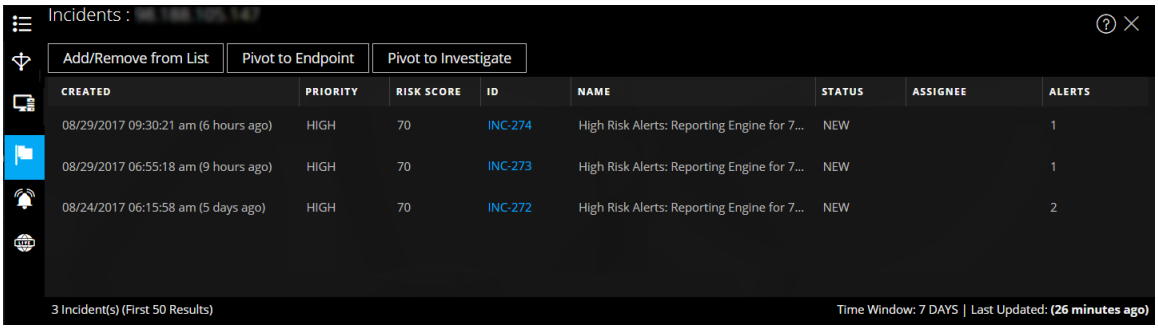
Le panneau Recherche contextuelle des alertes affiche les informations suivantes.

Champ	Description
Créé	Date et heure de création de l'alerte.
Gravité	Gravité de l'alerte
Nom	Nom de l'alerte. Cliquez sur le nom pour afficher les détails d'une alerte spécifique.
Source	Nom de la source de l'alerte à partir du déclenchement de l'alerte.
Événements	Nombre d'événements associés à l'alerte.
ID d'incident	ID de l'incident associé à l'alerte (le cas échéant). Cliquez sur l'ID pour afficher les détails d'une alerte spécifique.
Nombre	Affiche le nombre d'alertes. Par défaut, seules les 100 premières alertes sont affichées. Pour plus d'informations sur la façon de configurer les paramètres, consultez la rubrique « Configurer les paramètres de source de données pour Context Hub » du *Guide de configuration de Context Hub*.

Champ	Description
Période	Elle se base sur la valeur définie dans le champ « Requête dans les derniers » de la fenêtre Configurer les paramètres des sources de données. Par défaut, les données d'alerte pour les 7 derniers jours sont extraites.
Dernière mise à jour	Indique lorsque les données contextuelles ont été extraites de la source de données pour la dernière fois.

Incidents

La figure suivante est un exemple du panneau contextuel des incidents qui s'affiche en fonction de l'heure (du plus récent au plus ancien), puis de l'état de priorité.



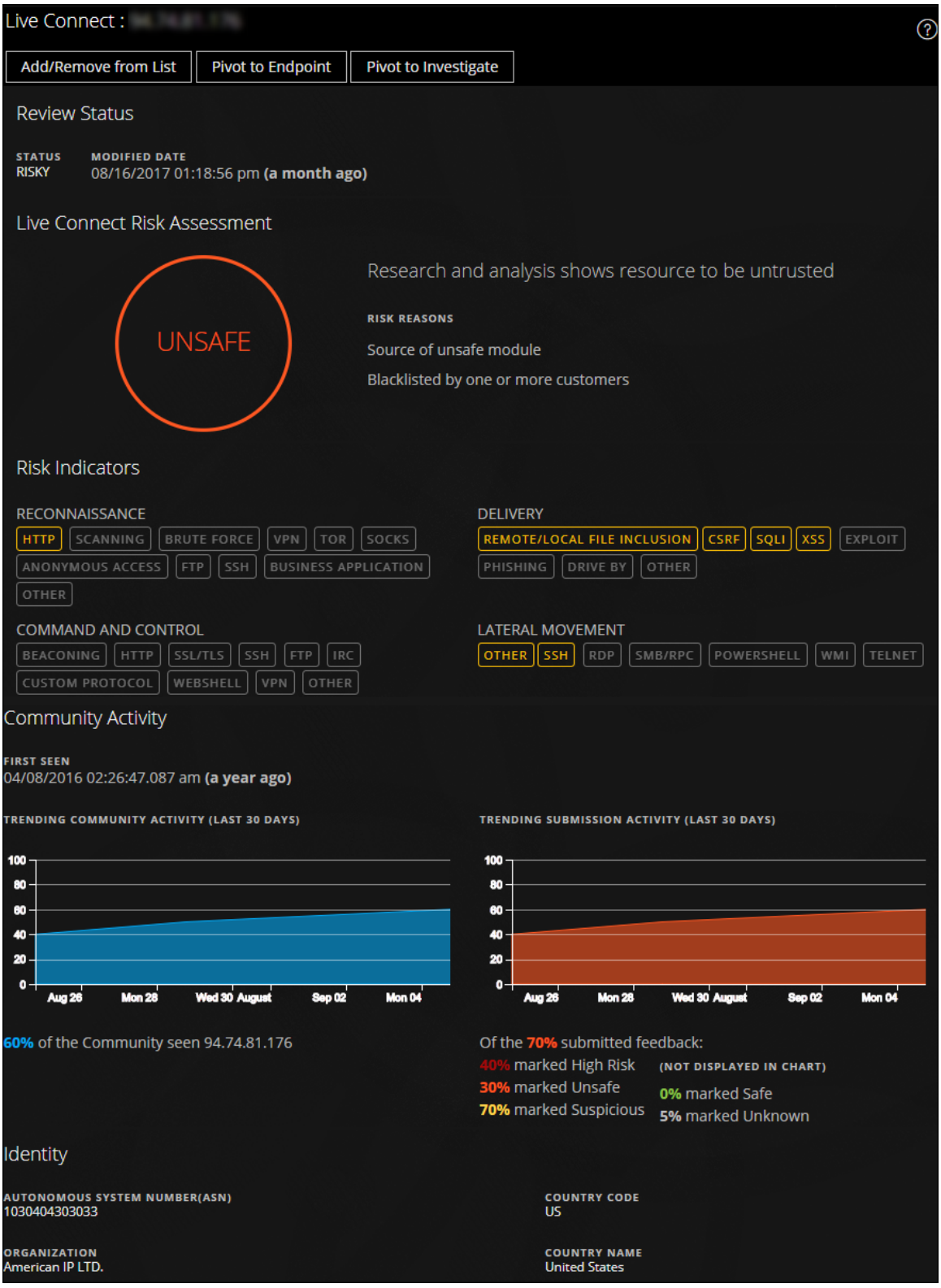
Le panneau Recherche contextuelle des incidents affiche les informations suivantes.

Champ	Description
Créé	Date de création de l'incident
Priorité	Priorité des incidents
Score de risque	Score de risque des incidents
ID	ID d'incident de l'incident. Si vous cliquez dessus, plus de détails sur l'incident s'affichent.
Nom	Nom de l'incident
État	État de l'incident
Personne affectée	Propriétaire actuel de l'incident
Alertes	Nombre d'alertes associées à l'incident

Champ	Description
Nombre	Affiche le nombre d'incidents. Par défaut, seules les 100 premières alertes sont affichées. Pour plus d'informations sur la façon de configurer les paramètres, consultez la rubrique « Configurer les paramètres de source de données pour Context Hub » du *Guide de configuration de Context Hub*.
Période	Elle se base sur la valeur définie dans le champ « Requête dans les derniers » de la fenêtre Configurer les paramètres des sources de données. Par défaut, les données d'alerte pour les 7 derniers jours sont extraites.
Dernière mise à jour	Indique lorsque les données contextuelles ont été extraites de la source de données pour la dernière fois.

Live Connect

La figure suivante est un exemple du panneau contextuel de Live Connect.


Live Connect :
Add/Remove from List
Pivot to Endpoint
Pivot to Investigate
Review Status
STATUS
RISKY
MODIFIED DATE
08/16/2017 01:18:56 pm (a month ago)
Live Connect Risk Assessment
UNSAFE
Research and analysis shows resource to be untrusted
RISK REASONS
Source of unsafe module
Blacklisted by one or more customers
Risk Indicators
RECONNAISSANCE
HTTP
SCANNING
BRUTE FORCE
VPN
TOR
SOCKS
ANONYMOUS ACCESS
FTP
SSH
BUSINESS APPLICATION
OTHER
DELIVERY
REMOTE/LOCAL FILE INCLUSION
CSRF
SQLI
XSS
EXPLOIT
PHISHING
DRIVE BY
OTHER
COMMAND AND CONTROL
BEACONING
HTTP
SSL/TLS
SSH
FTP
IRC
CUSTOM PROTOCOL
WEBSHELL
VPN
OTHER
LATERAL MOVEMENT
OTHER
SSH
RDP
SMB/RPC
POWERSHELL
WMI
TELNET
Community Activity
FIRST SEEN
04/08/2016 02:26:47.087 am (a year ago)
TRENDING COMMUNITY ACTIVITY (LAST 30 DAYS)
100
80
60
40
20
0
Aug 26
Mon 28
Wed 30 August
Sep 02
Mon 04
TRENDING SUBMISSION ACTIVITY (LAST 30 DAYS)
100
80
60
40
20
0
Aug 26
Mon 28
Wed 30 August
Sep 02
Mon 04
60% of the Community seen 94.74.81.176
Of the 70% submitted feedback:
40% marked High Risk
(NOT DISPLAYED IN CHART)
30% marked Unsafe
0% marked Safe
70% marked Suspicious
5% marked Unknown
Identity
AUTONOMOUS SYSTEM NUMBER(ASN)
1030404303033
COUNTRY CODE
US
ORGANIZATION
American IP LTD.
COUNTRY NAME
United States

Le panneau Live Connect affiche les informations suivantes :

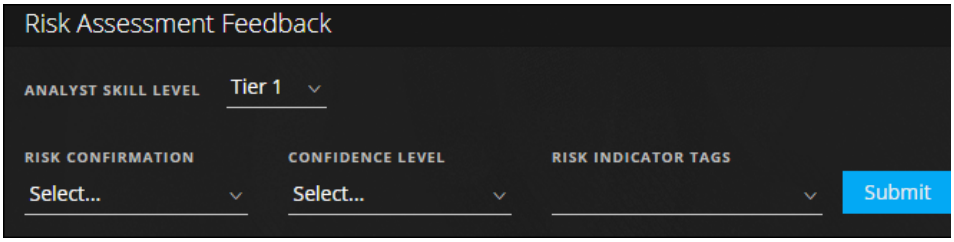
- État de révision
- Évaluation des risques Live Connect
- Indicateurs de risque
- Activité de la communauté
- WHOIS
- Fichiers, domaines et adresses IP connexes
- Identité
- Informations sur le certificat

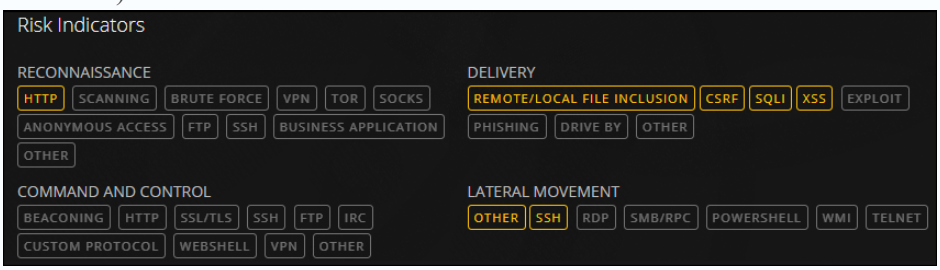
Le panneau Recherche contextuelle de Live Connect affiche les informations suivantes.

Champ	Description
État de révision	Affiche l'état de révision de l'entité Live Connect sélectionnée (IP, fichier ou domaine) en fonction de l'activité des analystes. Cela permet d'avoir une visibilité sur l'activité des analystes au sein d'une organisation. **État** Les types d'état sont les suivants : • **Nouveau :** Si les résultats d'une recherche pour une adresse IP sont affichés pour la première fois au sein de l'organisation. • **Affiché :** Si un analyste de l'organisation a déjà affiché les résultats d'une recherche pour une adresse IP. • **Marqué comme étant Sûr :** Si un analyste de l'organisation a déjà affiché les résultats d'une recherche et marqué l'adresse IP comme étant sûre. • **Marqué comme étant Risqué :** Si un analyste de l'organisation a déjà affiché les résultats d'une recherche et marqué l'adresse IP comme étant risquée.

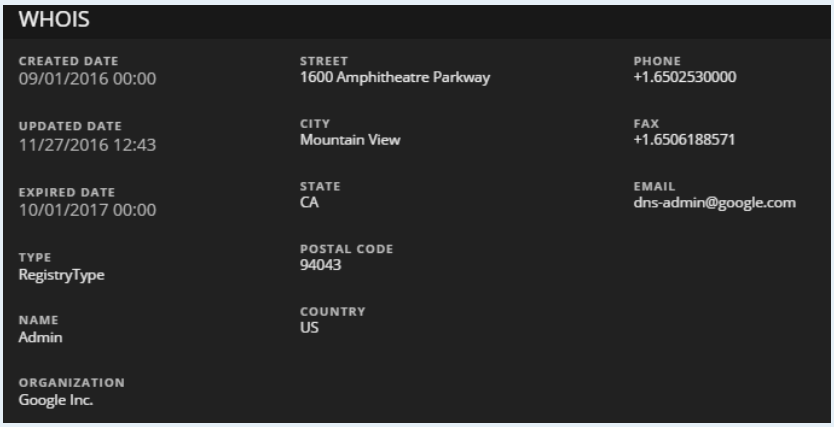
Champ	Description
Évaluation des risques	Affiche l'évaluation des risques concernant l'entité Live Connect sélectionnée (IP, fichier ou domaine) en fonction des commentaires des analystes et de l'analyse Live Connect. Les catégories d'évaluation des risques sont les suivantes : • **Sûr :** L'entité Live Connect est considérée comme sûre. • **Inconnu :** Live Connect ne dispose pas de suffisamment d'informations relatives à cette entité pour calculer le risque. • **Risque élevé** : Évaluation basée sur l'analyse et les raisons du risque fournies par la communauté. Les entités marquées comme étant à « Risque élevé » requièrent votre attention immédiate. • **Suspect** : Évaluation basée sur l'analyse et les raisons du risque fournies par la communauté. L'analyse indique une activité potentiellement menaçante qui nécessite une action. • **Dangereux :** Évaluation basée sur l'analyse et les raisons du risque fournies par la communauté. L'entité est classée comme étant à risque élevé, suspecte ou dangereuse et affiche les motifs de risque associés en conséquence.

Champ	Description
Commentaires sur l'évaluation des risques	Commentaires sur l'évaluation des risques permettant à l'analyste d'envoyer des commentaires de renseignements sur les menaces concernant une entité au serveur Live Connect. • **Niveau de compétence de l'analyste** Vous trouverez ci-dessous des options relatives au niveau de compétence de l'analyste : ◦ **Niveau 1** - Les analystes de ce niveau définissent généralement les procédures de correction et décident si un incident doit être transféré à d'autres zones d'un SOC (Centre des opérations de sécurité). Il s'agit de la valeur par défaut. ◦ **Niveau 2** - Les analystes examinent les incidents et capturent les renseignements à partir d'une procédure d'enquête pour générer des commentaires dans différents flux de travail d'un SOC. ◦ **Niveau 3** - Les analystes partagent les résultats d'une procédure d'enquête avec l'organisation du SOC. En général, ils gèrent les incidents et disposent d'un large éventail de compétences et d'outils nécessaires pour répondre aux incidents. **Remarque :** Lors de la création d'un nouvel utilisateur pour NetWitness Suite (analyste), un administrateur doit être en mesure d'identifier l'utilisateur comme étant de niveau 1, de niveau 2 ou de niveau 3. • **Confirmation du risque** - Confirmation du risque pour l'entité Live Connect sélectionnée (IP, fichier ou domaine). Les catégories de confirmation du risque sont les suivantes : ◦ **Sûr** : L'entité Live Connect est considérée comme sûre. ◦ **Inconnu** : L'analyste n'a pas suffisamment d'informations pour fournir une confirmation de risque ◦ **Risque élevé** : Évaluation basée sur l'analyse et les raisons du risque fournies par la communauté. Les entités marquées comme étant à « Risque élevé » requièrent votre attention immédiate. ◦ **Suspect** : Évaluation basée sur l'analyse et les raisons du risque fournies par la communauté. L'analyse indique une activité potentiellement menaçante qui nécessite une action.

Champ	Description
	◦ **Dangereux** : Évaluation basée sur l'analyse et les raisons du risque fournies par la communauté. • **Niveau de confiance** - Le niveau de confiance d'un analyste fournissant des commentaires sur l'entité Live Connect. Les catégories de niveau de confiance sont les suivantes : ◦ Élevé ◦ Moyen ◦ Faible. • **Balises d'indication des risques** - Permet de sélectionner une catégorie de balise en fonction de l'analyse. 
Activité de la communauté	Activités de la communauté, telles que : • Date du premier affichage dans la communauté. • Heure du premier affichage de l'adresse IP/du fichier/du domaine (heure actuelle - heure du premier affichage). **Tendance de l'activité de la communauté :** Si l'adresse IP est connue au sein de la communauté RSA, une représentation graphique de la tendance de l'activité de la communauté s'affiche pour les éléments suivants : • Utilisateurs (en %) ayant consulté l'adresse IP dans la communauté Live Connect. • Utilisateurs (en %) ayant envoyé des commentaires pour l'adresse IP. • Utilisateurs (en %) ayant marqué l'adresse IP comme dangereuse.

Champ	Description
Indicateurs de risque	Les indicateurs de risque sont mis en surbrillance en fonction des balises qui sont affectées par la communauté aux entités (adresses IP, fichiers ou domaines).  Les balises sont classées comme suit : • Reconnaissance • Livraison • Commande et contrôle • Déplacement latéral • Escalade des privilèges • Emballage et exfiltration Ces balises sont des exemples et varient selon les entrées reçues de la communauté sur le serveur Live Connect. L'analyste peut choisir les balises d'indication des risques appropriées tout en fournissant les commentaires de révision. Les balises mises en surbrillance indiquent que l'entité sélectionnée est associée à cette catégorie et à cette balise en particulier. Le fait de cliquer sur les balises mises en surbrillance affiche la description de la balise.

Champ	Description
Identité	Fournit les informations d'identité suivantes pour l'entité ou la métadonnée sélectionnée : Pour l'adresse IP : • Numéro de système autonome (ASN) • Préfixe • Code et nom du pays • Personne enregistrée (organisation) • Date Pour le hachage de fichier : • Nom du fichier • Taille du fichier • MD5 • SH1 • SH256 • Heure de compilation • Type Mime Pour le domaine : • Nom du domaine • Adresse IP associée
Informations sur le certificat	Fournit les informations suivantes sur le certificat pour le hachage de fichier sélectionné : • Émetteur de certificat • Validité du certificat • Algorithme de signature • Numéro de série du certificat

Champ	Description
Informations WHO IS	Les informations **WHO IS** fournissent les détails de la propriété d'un domaine donné.  Les informations suivantes concernant le propriétaire du domaine s'affichent : • Date de création • Date de mise à jour • Date d'expiration • Type (type d'enregistrement) • Nom • Organisation • Adresse avec le code postal • Pays • Téléphone • Fax • E-mail

Champ	Description
Fichiers associés	Les fichiers associés sont affichés pour les types d'entités IP et domaine. Une liste de fichiers associés connus est affichée, avec les informations suivantes : • Évaluation des risques Live Connect (Sûr, Risqué ou Inconnu) • Nom du fichier • MD5 • Date et heure de la compilation • Hachage importation - Fonction API • Type Mime
Domaines connexes	Les domaines associés sont affichés pour les types d'entités IP et domaine. Une liste de domaines associés connus est affichée, avec les informations suivantes : • Évaluation des risques Live Connect (Sûr, Risqué ou Inconnu) • Nom du domaine • Pays • Date enregistrée • Date d'expiration • E-mail de la personne enregistrée

Champ	Description
Adresses IP connexes	Les adresses IP associées sont affichées pour les types d'entités Domaine et Fichiers. Une liste d'adresses IP associées connues est affichée, avec les informations suivantes : • Évaluation des risques Live Connect (Sûr, Risqué ou Inconnu) • Adresse IP • Nom du domaine • Code et nom du pays • Pays • Date enregistrée • Date d'expiration • E-mail de la personne enregistrée