RSA NETWITNESS® PLATFORM

RSA NetWitness UEBA Guide d'utilisation

pour la version 11.2

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

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

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

March 2019

Sommaire

Introduction

RSA NetWitness UEBA (Analytique comportementale de l'entité et de l'utilisateur) est une solution d'analyse avancée pour découvrir, étudier et surveiller les comportements à risque pour tous les utilisateurs et entités de votre environnement réseau. NetWitness UEBA est utilisé pour :

- Détecter des utilisateurs malveillants et non autorisés
- Pointer les comportements à haut risque
- Découvrir des attaques
- Enquêter sur des menaces émergentes en matière de sécurité

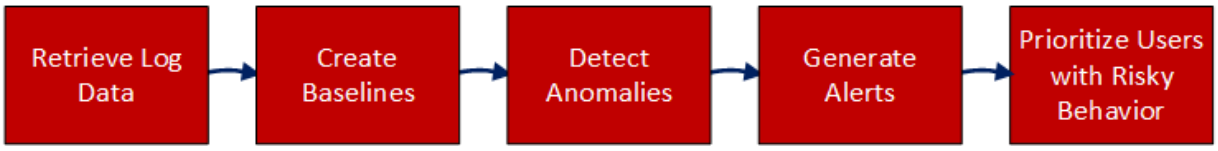
Remarque : Seuls les journaux Windows sont prêts à l'emploi. Vous pouvez ajouter des sources de log supplémentaires pour alimenter les modèles existants. Pour plus d'informations, consultez Sources de log prises en charge.

NetWitness UEBA exploite les données existantes dans les journaux NetWitness Platform et permet aux responsables du SOC et aux analystes d'entreprises d'avoir les connaissances et les capacités d'investigation nécessaires pour atténuer les cyber-menaces.

Ce guide est conçu pour les analystes et les responsables du SOC, et fournit des informations et des instructions sur l'utilisation de toutes les fonctions et fonctionnalités de NetWitness UEBA. Il décrit les méthodologies de procédure d'enquête clés, les principales capacités du système, les cas d'utilisation courants et les instructions étape par étape pour les stratégies de workflow recommandées.

Fonctionnement de NetWitness UEBA

NetWitness UEBA utilise l'analyse pour détecter les anomalies dans les données des fichiers log et en tire des résultats comportementaux. Il existe cinq étapes de base pour ce processus, comme illustré dans le schéma suivant :



Le tableau suivant fournit une brève description de chacune de ces étapes :

Étape	Description	En savoir plus
1. Récupérer les données des fichiers log	NetWitness UEBA récupère les données des fichiers log de la base de données (NWDB) NetWitness Platform et utilise les données pour créer des résultats analytiques.	Consultez Récupérer les données des fichiers log

Étape	Description	En savoir plus
2. Créer des valeurs de référence	Les valeurs de référence sont dérivées d'une analyse détaillée du comportement normal de l'utilisateur et sont utilisées pour comparer le comportement de l'utilisateur au fil du temps.	Consultez Créer des valeurs de référence
3. Détecter les anomalies	Une anomalie est une déviation par rapport au comportement de valeur de référence normal d'un utilisateur. NetWitness UEBA effectue une analyse statistique pour comparer chaque nouvelle activité à la valeur de référence. Les activités des utilisateurs qui s'écartent des valeurs de référence attendues sont notées en conséquence pour refléter la sévérité de l'écart.	Consultez Détecter les anomalies
4. Générer des alertes	Toutes les anomalies trouvées à l'étape 3 sont regroupées en lots horaires. Chaque lot est marqué en fonction du caractère unique de ses indicateurs. Si la composition de l'indicateur est unique par rapport aux compositions de lots horaires historiques d'un utilisateur, il est probable que ce lot soit transformé en alerte.	Consultez Générer des alertes
5. Hiérarchiser les utilisateurs au comportement risqué	NetWitness UEBA hiérarchise le risque potentiel d'un utilisateur à l'aide d'une formule de notation supplémentaire simplifiée. Une gravité est assignée à chaque alerte, ce qui augmente la note d'un utilisateur d'un nombre prédéfini de points. Les utilisateurs aux notes élevées ont soit plusieurs alertes qui leur sont associées, ou ont des alertes de gravité élevée qui leur sont associées.	Consultez Hiérarchiser les utilisateurs au comportement risqué

Récupérer les données des fichiers log

Le serveur NetWitness UEBA se connecte au service Broker ou Concentrator pour récupérer les données des fichiers log des Concentrators. Vous pouvez utiliser le service Broker disponible sur le serveur d'administration de NetWitness Platform si vous n'avez pas de Broker exclusif dans votre déploiement. Lors de l'installation de NetWitness UEBA, l'administrateur spécifie l'adresse IP du service Broker.

Pour plus d'informations, consultez la rubrique « (Facultatif) Tâche 2 - Installer NetWitness UEBA » dans le *Guide d'installation des hôtes physiques NetWitness Platform 11.2*.

Créer des valeurs de référence

L'UEBA de NetWitness utilise l'apprentissage automatique pour analyser plusieurs aspects des actions d'un utilisateur dans un flux des données des fichiers log et crée graduellement une valeur de référence multidimensionnelle de comportement typique pour chaque utilisateur. Par exemple, la valeur de référence peut inclure des informations sur les heures auxquelles un utilisateur se connecte en général.

Les valeurs de référence comportementales sont également créées au niveau mondial pour décrire les activités courantes observées dans tout le réseau. Si une heure de travail était anormale pour un utilisateur, mais qu'elle n'est pas anormale pour l'organisation, les algorithmes de réduction de faux positifs diminuent l'impact sur la note d'alerte.

Les modèles sont fréquemment mis à jour et s'améliorent constamment au fur et à mesure que le temps passe.

Remarque : NetWitness UEBA nécessite 28 jours de données historiques des fichiers log pour créer une valeur de référence appropriée pour tous les utilisateurs de votre réseau. Toutefois, RSA vous recommande de configurer NetWitness UEBA pour commencer à établir des valeurs de référence pour vos données deux mois avant votre date de déploiement `<today-60days>`. Les 28 premiers jours seront utilisés pour la formation de modèle et ne seront pas marqués. Les 32 jours restants sont mis à profit pour améliorer et mettre à jour le modèle, et sont également marqués pour fournir la valeur initiale.

Remarque : Pour la version 11.2, la prise en charge des environnements avec plusieurs domaines est limitée. Les valeurs de nom d'utilisateur distinctes, qui sont enregistrées sous différents domaines, seront normalisées, puis combinées en une seule entité modélisée. Par conséquent, les différents utilisateurs, qui partagent le même nom d'utilisateur dans différents domaines, seront injustement attribués à une seule entité normalisée.

Détecter les anomalies

Après avoir établi une valeur comportementale de référence pour tous les utilisateurs de votre environnement, chaque événement entrant est comparé à la valeur de référence et reçoit une note pour déterminer si le nouveau comportement est anormal, et en particulier s'il s'agit d'un écart fort par rapport à la valeur de référence. Par exemple, si les heures de travail normales d'un utilisateur sont de 9:00 à 17:00, une nouvelle activité à 18:00 ou 19:00 n'est pas une déviation forte, et n'est probablement pas marquée comme une anomalie. Cependant, une authentification à minuit est une déviation forte et est notée comme une anomalie.

Si des anomalies sont détectées, elles sont transformées en Indicateurs de compromission, décrits comme Indicateurs dans l'interface utilisateur. NetWitness UEBA utilise des indicateurs pour définir les activités anormales validées, telles que les ouvertures de session suspectes, les attaques de mots de passe forcées, les modifications utilisateur inhabituelles et l'accès anormal aux fichiers. Les indicateurs représentent soit des anomalies trouvées dans un seul événement, soit plusieurs événements mis en lots au fil du temps.

Générer des alertes

Toutes les anomalies trouvées sont regroupées en noms d'utilisateur et en lots horaires. Chaque lot est marqué en fonction du caractère unique de la composition de ses indicateurs. Si une composition est unique par rapport à l'historique de l'utilisateur, il est probable que ce lot soit transformé en alerte et les anomalies en indicateurs. Un lot d'anomalies au score élevé devient une alerte qui contient des indicateurs de compromis validés.

Par exemple, une activité anormale par elle-même, même si elle se produit des centaines de fois par jour dans un environnement de grande entreprise, ne reflète pas nécessairement une attaque de compte. Toutefois, un comportement anormal qui se produit avec un grand nombre d'autres comportements anormaux pourrait indiquer que le compte est attaqué. Ces trois comportements qui se produisent ensemble peuvent indiquer qu'une analyse supplémentaire est nécessaire.

- Authentification à partir d'un ordinateur anormal
- Plusieurs tentatives d'authentification identifiées dans une courte période de temps
- Plusieurs fichiers ont été supprimés par cet utilisateur à partir du partage de fichiers d'entreprise

Remarque : L'interface utilisateur de NetWitness UEBA peut initialement apparaître comme vide car les alertes ne sont pas générées tant que les valeurs de référence ne sont pas établies. S'il n'existe aucune donnée d'audit historique lorsque NetWitness UEBA est activé, le système commence à générer les valeurs de référence à partir du moment où il est déployé et nécessite que 28 jours complets s'écoulent avant de commencer à générer de nouvelles alertes. Si les données d'audit historiques sont traitées lorsque NetWitness UEBA est activé, les alertes apparaissent après le traitement des données historiques, généralement dans un délai de deux à quatre jours.

Hiérarchiser les utilisateurs au comportement risqué

Les notes des utilisateurs sont un outil essentiel pour la hiérarchisation des incidents. La note de l'utilisateur est basée sur un simple calcul supplémentaire des alertes de l'utilisateur. Les alertes et les commentaires des analystes sont les seuls facteurs dans le calcul de la note de l'utilisateur, avec l'impact sur les notes déterminé par leur niveau de gravité.

Un code couleur unifié est utilisé pour les notes des utilisateurs et des alertes :

Gravité	Couleur	Note
Critique	Rouge	+20
Élevée	Orange	+15
Moyenne	Jaune	+10
Faible	Verte	+1

Sources de log prises en charge

NetWitness UEBA prend en charge nativement les sources de log Windows suivantes :

- Windows Active Directory
- Activité d'ouverture de session et d'authentification Windows
- Serveurs de fichiers Windows

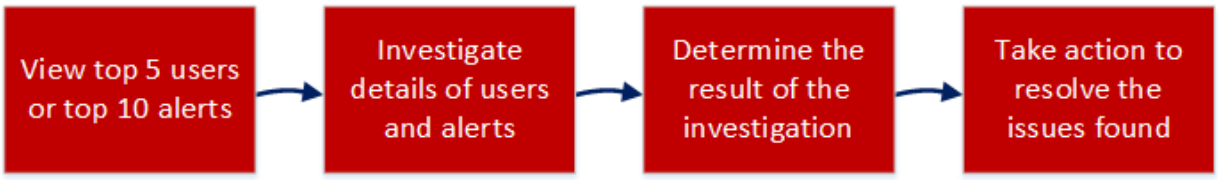
Flux de travail recommandés

Pour utiliser NetWitness UEBA le plus efficacement possible, il existe deux flux de travail ; le flux de travail de Détection et le flux de travail Légal, que vous pouvez suivre.

Flux de travail de Détection

Le flux de travail de détection vous permet d'obtenir une vue d'ensemble de l'intégrité de votre environnement, puis de vous concentrer sur l'enquête sur les principaux utilisateurs à haut risque et les alertes affichées dans l'onglet Tour d'horizon.

L'organigramme suivant illustre les étapes que vous pouvez suivre pour commencer à détecter les comportements suspects dans votre environnement.



Le tableau suivant décrit chaque étape du flux de travail.

Étape	Description	Instructions
Afficher les cinq premiers utilisateurs ou les 10 premières alertes	Dans l'onglet Tour d'horizon, notez les utilisateurs ayant les comportements les plus risqués et les alertes les plus critiques.	Enquêter sur les utilisateurs à haut risque et Enquêter sur les alertes principales
Enquêter sur les détails des utilisateurs et des alertes	Effectuez une recherche dans les informations détaillées sur les comportements d'utilisateur risqués et les alertes critiques pour essayer de déterminer la cause de ces actions et comment les résoudre.	Enquêter sur les utilisateurs à haut risque et Enquêter sur les indicateurs
Déterminer le résultat de l'enquête	Analysez les informations récapitulatives fournies dans l'interface utilisateur à partir des étapes précédentes et identifiez les zones sur lesquelles se concentrer pour résoudre les problèmes que vous avez trouvés.	Identifier les utilisateurs à haut risque et Enquêter sur les indicateurs

Étape	Description	Instructions
Prendre des mesures pour résoudre les problèmes trouvés	Ciblez les comportements et les événements spécifiques de l'utilisateur à traiter, et utilisez les résultats de cette enquête pour améliorer et affiner les enquêtes futures.	Prendre des mesures sur les utilisateurs à haut risque

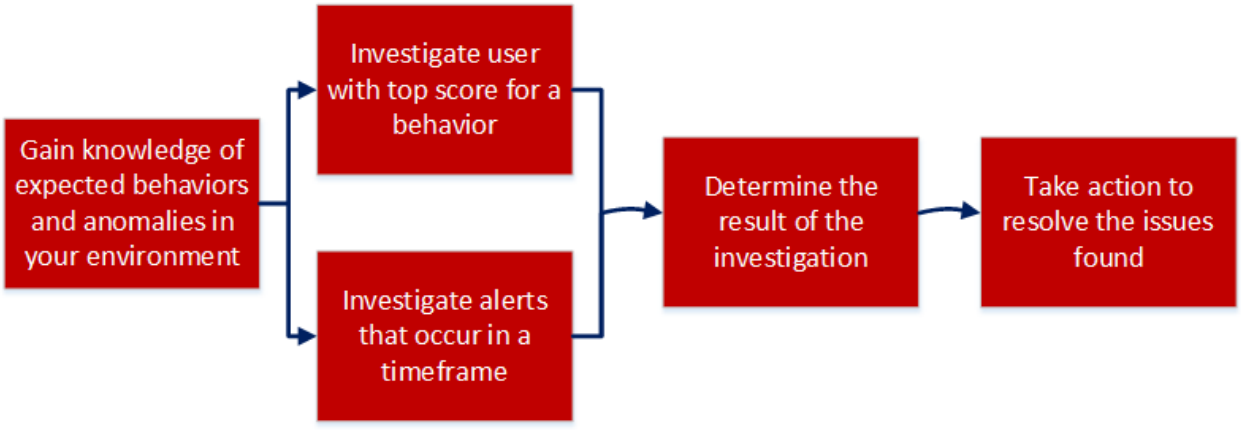
Flux de travail légal

Le flux de travail légal est recommandé lorsque vous avez acquis une compréhension des comportements utilisateur et des anomalies typiques dans votre environnement, et il vous aide à vous concentrer sur des informations légales spécifiques basées sur un comportement de l'utilisateur, ou une période de temps spécifique au cours de laquelle des événements suspects se sont produits.

À l'aide des informations légales, les analystes peuvent déterminer les actions et les comportements que l'attaquant est susceptible de tenter à l'aide des questions suivantes :

- Quelles sont les techniques et les comportements fondamentaux communs à toutes les intrusions ?
- Quelles preuves ces techniques laissent-elles derrière elles ?
- Que font les attaquants ?
- Quels sont les comportements normaux de mes comptes et entités ?
- Quelles sont mes machines sensibles et où sont-elles situées ?

L'organigramme suivant illustre comment effectuer votre enquête sur les informations légales, basée sur un comportement utilisateur spécifique, ou une période spécifique dans laquelle les événements suspects se sont produits.



Le tableau suivant décrit chaque étape du flux de travail.

Étape	Description	Instructions
Acquérir des connaissances sur les comportements et anomalies attendus dans votre environnement	Établissez une valeur de référence des comportements normaux, des anomalies attendues et des anomalies inattendues, afin que vous puissiez vous concentrer sur les anomalies significatives pour votre environnement.	Récupérer les données des fichiers log, Détecter les anomalies et Générer des alertes.
Enquêtez sur l'utilisateur avec la note la plus élevée pour un comportement spécifique	Sélectionnez un utilisateur avec une note élevée pour un comportement spécifique et rassemblez des informations détaillées.	Enquêter sur les utilisateurs à haut risque et Enquêter sur les indicateurs

Étape	Description	Instructions
Enquêter sur les alertes qui surviennent dans une période spécifique	Déterminez une période d'intérêt et, dans l'onglet Alertes, sélectionnez cette période pour afficher des informations détaillées sur les alertes qui se sont produites pendant cette durée.	Enquêter sur les indicateurs
Déterminer le résultat de l'enquête	En fonction de votre connaissance du comportement de l'utilisateur attendu, concentrez-vous sur les indicateurs affichés pendant la période spécifiée et déterminez si les anomalies découvertes doivent être résolues.	Enquêter sur les indicateurs et Identifier les utilisateurs à haut risque
Prendre des mesures pour résoudre les problèmes trouvés	Ciblez les comportements et les événements spécifiques de l'utilisateur à traiter, et utilisez les résultats de cette enquête pour améliorer et affiner les enquêtes futures.	Prendre des mesures sur les utilisateurs à haut risque

Accéder à NetWitness UEBA

Remarque : Pour accéder au service NetWitness UEBA et à l'onglet Utilisateurs, vous devez être affecté au rôle UEBA_Analyst ou aux rôle Administrateurs. Pour plus d'informations sur la façon d'assigner ces rôles, consultez la rubrique « Mode de fonctionnement du contrôle d'accès basé sur un rôle » dans le *Guide de sécurité du système et de maintenance de l'utilisateur*. Vous devez également vous assurer d'avoir correctement configuré les licences NetWitness UEBA. Pour plus d'informations sur les licences NetWitness UEBA, consultez la rubrique « Licence d'analytique comportementale de l'entité et de l'utilisateur » dans le *Guide de gestion des licences*.

Pour accéder à NetWitness UEBA, connectez-vous à NetWitness Platform et accédez à **Enquêter** > **Utilisateurs**. La vue Utilisateurs, qui contient toutes les fonctionnalités de NetWitness UEBA, s'affiche.

Indicateurs NetWitness UEBA

Les tableaux suivants répertorient les indicateurs qui s'affichent lorsqu'une activité potentiellement malveillante est détectée.

Serveurs de fichiers Windows

Indicateur	Type d'alerte	Description
Temps d'accès au fichier anormal	Heures non standard	Un utilisateur a accédé à un fichier à un moment anormal.
Modification d'autorisation d'accès aux fichiers anormale	Modifications d'autorisations en bloc	Un utilisateur a modifié plusieurs autorisations de partage.
Événement d'accès aux fichiers anormal	Accès anormal aux fichiers	Un utilisateur a accédé anormalement à un fichier.
Modifications des autorisations d'accès aux fichiers multiples	Modifications d'autorisations en bloc	Un utilisateur a modifié plusieurs autorisations de partage de fichiers.
Plusieurs événements d'accès aux fichiers	Utilisateur espion	Un utilisateur a modifié plusieurs autorisations de partage de fichiers.
Plusieurs événements d'accès aux fichiers en échec	Utilisateur espion	Un utilisateur n'est pas parvenu à plusieurs reprises à accéder à un fichier.
Plusieurs événements d'ouverture de fichier	Utilisateur espion	Un utilisateur a ouvert plusieurs fichiers.
Événements d'ouverture de plusieurs dossiers	Utilisateur espion	Un utilisateur a ouvert plusieurs dossiers.
Plusieurs événements de suppression de fichiers	Accès anormal aux fichiers	Un utilisateur a supprimé plusieurs fichiers.

Active Directory

Indicateur	Type d'alerte	Description
Heure de modification d'Active Directory anormal	Heures non standard	Un utilisateur a modifié Active Directory à une heure anormale.
Modification Active Directory anormale	Modifications AD anormales	Une modification anormale d'un attribut Active Directory a été effectuée.

Indicateur	Type d'alerte	Description
Modifications de l'appartenance à plusieurs groupes	Modifications importantes sur les groupes	Un utilisateur a apporté avec succès plusieurs modifications aux groupes.
Modifications de gestion de compte multiple	Modifications AD anormales	Un utilisateur a procédé avec succès à plusieurs modifications sur Active Directory.
Modifications de gestion de compte utilisateur multiple	Modifications AD anormales	Un utilisateur a procédé avec succès à plusieurs modifications sensible sur Active Directory.
Plusieurs modifications de gestion des comptes ont échoué	Modifications AD anormales	Un utilisateur n'est pas parvenu à effectuer plusieurs modifications sur Active Directory.
Mot de passe administrateur modifié	Modification du mot de passe administrateur	Le mot de passe d'un administrateur a été modifié.
Compte utilisateur activé	Changements d'état d'utilisateur sensibles	Le compte d'un utilisateur a été activé.
Compte utilisateur désactivé.	Changements d'état d'utilisateur sensibles	Le compte d'un utilisateur a été désactivé.
Compte utilisateur déverrouillé	Changements d'état d'utilisateur sensibles	Le compte d'un utilisateur a été déverrouillé.
Type de compte d'utilisateur modifié	Changements d'état d'utilisateur sensibles	Le type d'un utilisateur a été modifié.
Compte utilisateur verrouillé	Changements d'état d'utilisateur sensibles	Un compte utilisateur a été verrouillé.
Mot de passe utilisateur modifié	Changements d'état d'utilisateur sensibles	Le mot de passe d'un utilisateur a été modifié.

Activité d'ouverture de session

Indicateur	Type d'alerte	Description
Temps d'ouverture de session anormal	Heures non standard	Un utilisateur connecté à un moment anormal.
Ordinateur anormal	Connexion utilisateur à un hôte anormal	Un utilisateur a tenté d'accéder à un ordinateur anormal.
Plusieurs authentifications réussies	Plusieurs ouvertures de session par utilisateur	Un utilisateur connecté plusieurs fois.

Indicateur	Type d'alerte	Description
Plusieurs authentifications échouées	Plusieurs ouvertures de session échouées	Un utilisateur a échoué plusieurs tentatives d'authentification.
Connecté sur plusieurs ordinateurs	Utilisateur connecté à plusieurs hôtes	Un utilisateur a tenté de se connecter à partir de plusieurs ordinateurs.

Cas d'utilisation de NetWitness UEBA pour les journaux Windows

NetWitness UEBA se concentre sur la fourniture de capacités de détection avancées pour protéger les entreprises contre les menaces d'initiés. Ceux-ci peuvent être des utilisateurs de confiance du réseau qui ont été compromis, ou bien, il peut s'agir d'un attaquant externe exploitant les informations d'identification acquises à l'aide des techniques avancées d'usurpation de compte.

Le vol d'identité commence généralement par le vol d'informations d'identification, qui sont ensuite utilisées pour obtenir un accès non autorisé aux ressources et pour prendre le contrôle sur le réseau. Les attaquants peuvent également exploiter des utilisateurs non-administrateurs compromis pour obtenir l'accès aux ressources pour lesquelles ils ont des droits d'administration, puis procéder à une escalade de privilèges.

Un attaquant utilisant des informations d'identification usurpées peut déclencher des événements réseau suspects tout en accédant aux ressources. Il est possible de détecter toute utilisation illicite des identifiants, mais vous devez faire la distinction entre les activités des attaquants et les nombreux événements légitimes. NetWitness UEBA vous aide à faire la distinction entre les activités éventuellement malveillantes de celles qui sont anormales, sans être dangereuses.

Les cas d'utilisation suivants définissent certains types de risques ainsi que les capacités système correspondantes utilisées afin de les détecter. Vous pouvez examiner les cas d'utilisation, représentés par leur type d'alerte et leur description, afin de mieux comprendre le comportement à risque lié à chacun d'eux. NetWitness UEBA vous permet d'effectuer une recherche approfondie en utlisant les indicateurs des activités utilisateur éventuellement à risque et d'en savoir plus. Pour en savoir plus sur les indicateurs pris en charge par NetWitness UEBA, voir Indicateurs NetWitness UEBA.

Type d'alerte	Description
Modifications importantes sur les groupes	Un nombre anormal de modifications ont été apportées aux groupes. Examinez les éléments qui ont été modifiés et déterminez si ces modifications sont légitimes ou si elles pourraient être le fruit d'un comportement risqué ou malveillant. Cette activité est généralement associée à l'indicateur **Modifications de l'appartenance à plusieurs groupes**.
Privilèges élevés accordés	Des privilèges de compte élevés ont été délégués à un utilisateur. Les attaquants utilisent souvent des comptes d'utilisateurs normaux et leur accordent des privilèges élevés, pour exploiter le réseau. Examinez l'utilisateur qui a reçu les privilèges élevés et déterminez si ces modifications étaient légitimes ou pourraient résulter d'un comportement risqué ou malveillant. Cette activité est généralement associée aux indicateurs **Membre imbriqué ajouté à un groupe d'entreprise critique** et **Membre ajouté à un groupe d'entreprise critique**.

Type d'alerte	Description
Plusieurs ouvertures de session échouées	Dans une tentative classique d'usurpation de mot de passe, l'attaquant tente d'obtenir un mot de passe en le devinant ou à l'aide d'autres méthodes peu sophistiquées afin d'obtenir un accès initial. Il est possible que l'attaquant soit détecté ou que le compte se bloque après qu'il essaie de s'authentifier, toutefois s'il connaît l'historique des mots de passe de la victime, il peut réussir à s'authentifier. Restez à l'affût de tout signe d'activité anormale, indiquant qu'une personne autre que le propriétaire du compte tente d'y accéder. Cette activité est généralement associée à l'indicateur indicateur **Plusieurs authentifications échouées**.
Connexions utilisateur à plusieurs sites AD	Les contrôleurs de domaine stockent les hachages de mot de passe de tous les comptes du domaine ; par conséquent, ils sont des cibles de choix pour les pirates informatiques. Les contrôleurs de domaine qui ne sont pas rigoureusement mis à jour et sécurisés sont exposés à des attaques et à des usurpations d'identité, conduisant ainsi à une vulnérabilité du domaine. Des privilèges d'utilisateur sur plusieurs domaines peuvent indiquer qu'un domaine parent a été compromis. Déterminez si l'accès des utilisateurs depuis et vers plusieurs sites est légitime ou si elle est le signe d'une attaque éventuelle. Cette activité est généralement associée à l'indicateur **Connecté à plusieurs domaines**.
Connexion utilisateur à un hôte anormal	Les attaquants ont souvent besoin de réacquérir des informations d'identification et d'effectuer d'autres activités sensibles, comme l'accès à distance. Le fait de remonter la chaîne d'accès peut permettre d'identifier d'autres ordinateurs utilisés pour des activités éventuellement à risque. Si la présence d'un attaquant se limite à un seul hôte compromis ou à de nombreux hôtes compromis, cette activité peut être associée l'indicateur **Ordinateur anormal**.
Exfiltration de données	L'exfiltration des données désignz la copie, le transfert ou la récupération non autorisé(e) de données à partir d'un ordinateur ou d'un serveur. L'exfiltration des données est une activité malveillante réalisée grâce à diverses techniques, généralement par des cybercriminels sur Internet ou un autre réseau. Cette activité peut être associée aux indicateurs **Nombre excessif d'événements de renommage de fichiers**, **Nombre excessif de fichiers déplacés à partir du système de fichiers** et **Nombre excessif de fichiers déplacés vers le système de fichier**.
Renommage en masse de fichiers	Le rançongiciel est un type de logiciel malveillant qui crypte les fichiers de bureau et système, les rendant ainsi inaccessibles. Certains rançonligiciels, par exemple, tel que le programme malveillant Locky, chiffre et renomme les fichiers dès sa première exécution. Utilisez cette indicateur de renommage massif de fichiers pour déterminer si votre système de fichiers a été infecté par un rançongiciel. Cette activité peut être associée à l'indicateur **Événements de renommage de fichiers multiples**.

Type d'alerte	Description
Utilisateur espion	Le snooping est un accès non autorisé aux données d'une personne ou d'une entreprise. Le snooping peut également désigner le fait de regarder simplement un e-mail sur un autre ordinateur, ou d'observer une personne en train de saisir un message. Les techniques de snooping plus sophistiquées utilise des programmes logiciels permettant de surveiller à distance l'activité sur un ordinateur ou un périphérique réseau. Cette activité peut être associée aux indicateurs **Plusieurs événements d'accès aux fichiers**, **Plusieurs événements d'accès aux fichiers en échec**, **Plusieurs événements d'ouverture de fichier**, et **Événements d'ouverture de plusieurs dossiers**.
Plusieurs ouvertures de session par utilisateur	Toutes les activités d'authentification, malveillantes ou non, apparaissent comme des ouvertures de session normales. Par conséquent, les administrateurs doivent surveiller toute activité autorisée inattendue. Les pirates utilisent ces informations d'identification usurpées pour accéder aux données d'une manière non autorisée, ce qui peut fournir une possibilité de détection. Lorsqu'un compte est utilisé pour des activités inhabituelles, par exemple pour effectuer des tentatives d'authentification en nombre inhabituel, la sécurité du compte peut être compromise. Cette activité peut être associée à l'indicateur **Plusieurs authentifications réussies**.
Utilisateur connecté à plusieurs hôtes	Les pirates doivent généralement réacquérir les informations d'identification périodiquement. En effet, leur trousseau d'identifiants usurpés se dégrade naturellement au fil du temps, en raison des modifications et des réinitialisations de mot de passe. Par conséquent, les pirates maintiennent fréquemment un ancrage dans l'organisation compromise en installant des accès contournés et en conservant les informations d'identification de nombreux ordinateurs dans l'environnement. Cette activité peut être associée à l'indicateur **Connecté sur plusieurs ordinateurs**.
Modification du mot de passe administrateur	Les secrets partagés à long terme, par exemple les mots de passe de compte privilégié, sont fréquemment utilisés pour accéder à des ressources, depuis des serveurs d'impression aux contrôleurs de domaine. Pour identifier les pirates qui cherchent à utiliser ces comptes, faites particulièrement attention aux modifications de mot de passe effectuées par les administrateurs, et assurez-vous qu'elles ont été réalisées par des parties de confiance et qu'aucun comportement anormal ne leur est associé. Cette activité peut être associée à l'indicateur **Modification de mot de passe administrateur**.

Type d'alerte	Description
Modifications d’autorisations en bloc	Certaines techniques d’usurpation d'informations d'identification, par exemple, Pass-The-hash, utilisent un processus itératif à deux étapes. Tout d'abord, un pirate obtient une autorisation de lecture-écriture élevée dans les zones privilégiées de la mémoire volatile et des systèmes de fichiers, qui sont généralement accessibles uniquement aux processus du système sur au moins un ordinateur. En outre, le pirate tente d'augmenter l'accès à d'autres ordinateurs sur le réseau. Déterminez si des modifications d'autorisation anormales ont été effectuées sur les systèmes de fichiers pour vous assurer qu'ils n'ont pas été compromis par un pirate. Cette activité peut être associée aux indicateurs **Modifications des autorisations d'accès aux fichiers multiplesModifications multiples des autorisations d’accès aux fichiers** et **Modification d'autorisation d'accès aux fichiers anormale**.
Modifications AD anormales	Si un pirate obtient un accès hautement privilégié à un domaine ou à un contrôleur de domaine Active Directory, cet accès peut être exploité afin d’accéder, de contrôler ou même de détruire toute la forêt. Si un contrôleur de domaine unique est compromis et qu'un pirate modifie la base de données AD, ces modifications sont répliquées sur tous les autres contrôleurs de domaine du domaine, et selon la partition dans laquelle les modifications sont apportées, la forêt le sera aussi. Examinez les modifications anormales réalisées par les administrateurs et les non-administrateurs dans AD pour déterminer si elles représentent un éventuel compromis réel pour le domaine. Cette activité peut être associée aux indicateurs **Modification anormale d'Active Directory**, **Modifications multiples de la gestion de compte**, **Modifications multiples de la gestion de compte utilisateur** et **Modifications multiples de compte en échec**.
Changements d'état d'utilisateur sensibles	Un compte d'administrateur de domaine ou d'entreprise a la capacité par défaut de contrôler toutes les ressources d'un domaine, qu'il ait de bonnes ou de mauvaises intentions. Ce contrôle inclut la possibilité de créer et de modifier des comptes, de lire, écrire ou supprimer des données, d’installer ou de modifier des applications et d’effacer les systèmes d'exploitation. Certaines de ces activités se déclenchent de manière organique dans le cadre du cycle de vie naturel du compte. Examinez ces modifications de compte utilisateur sensibles à la sécurité et déterminez si celui-ci a été compromis. Cette activité peut être associée aux indications **Compte utilisateur activé**, **Compte utilisateur désactivé**, **Compte utilisateur débloqué**, **Type de compte utilisateur modifié**, **Compte utilisateur verrouillé**, **Modification de l’option Le mot de passe de l’utilisateur ne s’expire jamais**, **Mot de passe utilisateur modifié par un non propriétaire** et **Modification par un mot de passe utilisateur**.

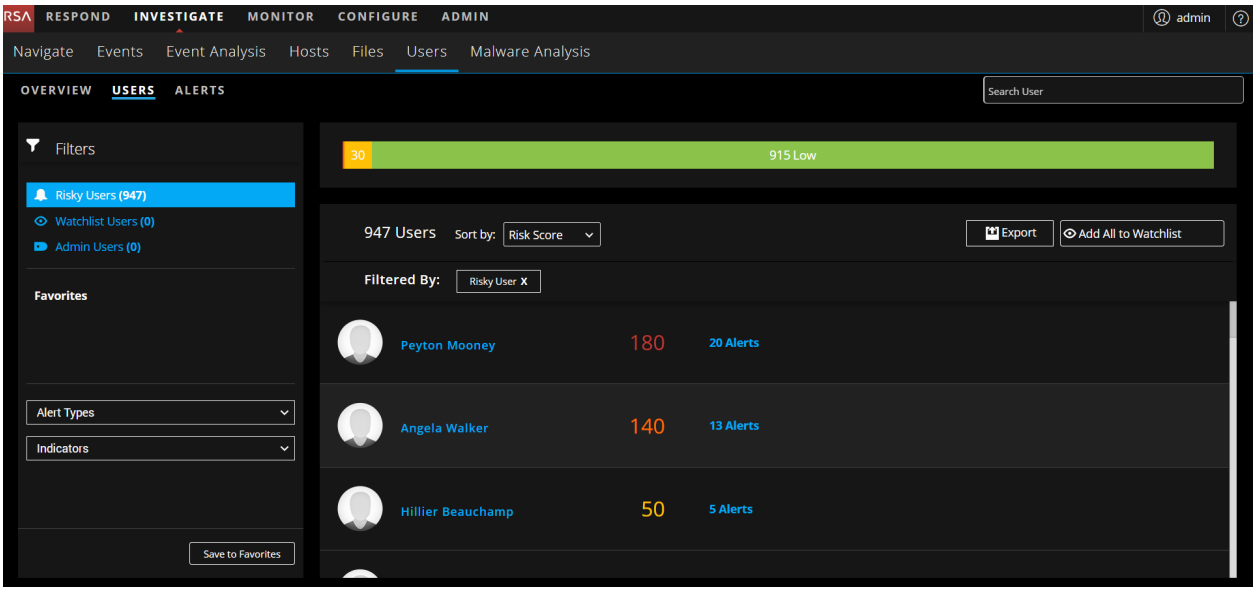
Type d'alerte	Description
Accès anormal aux fichiers	Surveillez tout accès aux fichiers anormale afin d'empêcher un accès inapproprié aux fichiers confidentiels et tout vol de données sensibles. En surveillant les vues, les modification et les suppressions des fichiers de manière sélective, vous pouvez détecter les modifications éventuellement non autorisées des fichiers sensibles, qu'elles soient causées par une attaque ou qu'elle soit le fruit d'une erreur de gestion des modifications. Cette activité peut être associée à l'indicateur **Événement d'accès aux fichiers** et **Événements multiples de suppression de fichiers**.
Heures non standard	Toutes les activités d'authentification, malveillantes ou non, apparaissent comme des ouvertures de session normales. Par conséquent, les administrateurs doivent surveiller toute activité autorisée inattendue. Les pirates utilisent ces informations d'identification usurpées pour accéder aux données d'une manière non autorisée, ce qui peut fournir une possibilité de détection. Lorsqu'un compte est utilisé pour des activités inhabituelles, par exemple pour effectuer des tentatives d'authentification en nombre inhabituel, la sécurité du compte peut être compromise. Utilisez l'indicateur d'heure d'activité anormale pour déterminer si le compte a été usurpé par un acteur externe. Cette activité peut être associée aux indicateurs**Heure d'accès aux fichiers anormale**, **Heure de modification Active Directory anormale**et **Heure de connexion anormale**.

Enquêter sur les utilisateurs à haut risque

Une note de l'utilisateur est générée en fonction du score d'alerte et de la gravité de l'alerte. En utilisant la note de l'utilisateur, vous pouvez identifier les utilisateurs nécessitant une attention immédiate, effectuer une recherche plus approfondie et prendre les mesures nécessaires. Vous pouvez identifier les utilisateurs à haut risque à partir de l'onglet **Tour d'horizon** ou de l'onglet **Utilisateurs**.

La figure suivante est un exemple des cinq principaux utilisateurs à haut risque dans l'onglet **Tour d'horizon**.

La figure suivante est un exemple de tous les utilisateurs à risque dans votre environnement dans l'onglet **Utilisateurs**.



Ce qui suit est un processus général pour enquêter sur les utilisateurs à haut risque dans votre environnement.

1. Identifiez les utilisateurs à haut risque. Vous pouvez identifier les utilisateurs à haut risque à l'aide des méthodes suivantes :

   - L'onglet **Tour d'horizon** affiche les cinq principaux utilisateurs à risque dans votre environnement. Parmi les utilisateurs répertoriés, identifiez les utilisateurs présentant une gravité critique ou une note d'utilisateur supérieure à 100.
   - L'onglet **Utilisateur** affiche tous les utilisateurs à risque dans votre environnement, triés par valeur de risque. Identifiez le nombre d'utilisateurs marqués comme Critiques, Élevés et Moyens ou selon les enquêtes scientifiques, identifiez les comportements d'utilisateurs malveillants et générez des listes d'utilisateurs cibles axées sur les cas d'utilisation à l'aide de filtres comportementaux. En outre, vous pouvez également utiliser différents types de filtres (Risqué, Admin ou Liste de surveillance) pour identifier un groupe ciblé d'utilisateurs à haut risque.

   Remarque : L'enquête devrait surtout se concentrer sur les gravités Critiques, Hautes et Moyennes. Les utilisateurs à faible score ne valent généralement pas beaucoup de procédure d'enquête.

   Survolez le nombre d'alertes associées aux utilisateurs à risque pour voir rapidement ce qu'ils sont et déterminer s'il existe un bon mélange.

   Remarque : Le nombre d'alertes n'est pas toujours corrélé aux scores les plus élevés, car certaines alertes ne contribuent qu'à de petits scores par rapport à la note globale de l'utilisateur, mais plus il y a d'alertes, plus il est facile de démontrer une chronologie de l'activité qui a abouti au score élevé.

   Pour plus d'informations, consultez la rubrique Identifier les utilisateurs à haut risque.

2. Dans la vue **Profil utilisateur**, examinez les alertes et les indicateurs de l'utilisateur.

   a. Révisez la liste des alertes associées à l'utilisateur et le score d'alerte pour chaque alerte, trié par gravité.

   b. Développez les noms des alertes pour identifier un récit de menace. L'indicateur de contribution le plus élevé détermine le nom de l'alerte qui suggère pourquoi cette heure est marquée.

   c. Utilisez la chronologie de flux d'alerte pour comprendre les activités anormales.

   d. Examinez chaque indicateur associé à l'alerte pour voir les informations de l'indicateur, y compris la chronologie dans laquelle l'anomalie s'est produite. En outre, vous pouvez approfondir l'enquête sur l'incident à l'aide de ressources externes telles que SIEM, le système de détection d'intrusions réseau, en contactant directement l'utilisateur ou un directeur général et ainsi de suite.

   Pour plus d'informations, consultez la rubrique Commencer une investigation sur les utilisateurs à haut risque.

3. À la fin de l'enquête, vous pouvez enregistrer votre observation comme suit :

a. Spécifier si une alerte n'est pas un risque

b. Enregistrer le profil comportemental pour le cas d'utilisation trouvé dans votre environnement

c. Si vous souhaitez conserver une trace de l'activité utilisateur, vous pouvez ajouter des utilisateurs à la liste de surveillance et regarder le profil utilisateur

Pour plus d'informations, consultez la rubrique Prendre des mesures sur les utilisateurs à haut risque.

Identifier les utilisateurs à haut risque

Vous pouvez identifier un utilisateur à haut risque dans votre environnement de la manière suivante :

- Afficher les cinq principaux utilisateurs à haut risque
- Afficher tous les utilisateurs à haut risque
- Afficher les utilisateurs d'un groupe spécifique
- Afficher les utilisateurs sur la base de l'enquête légale

Afficher les cinq principaux utilisateurs à risque

Dans l'onglet **Tour d'horizon**, vous pouvez afficher la liste des cinq principaux utilisateurs à haut risque dans votre environnement ainsi que la note de l'utilisateur.

Pour afficher les cinq principaux utilisateurs à risque :

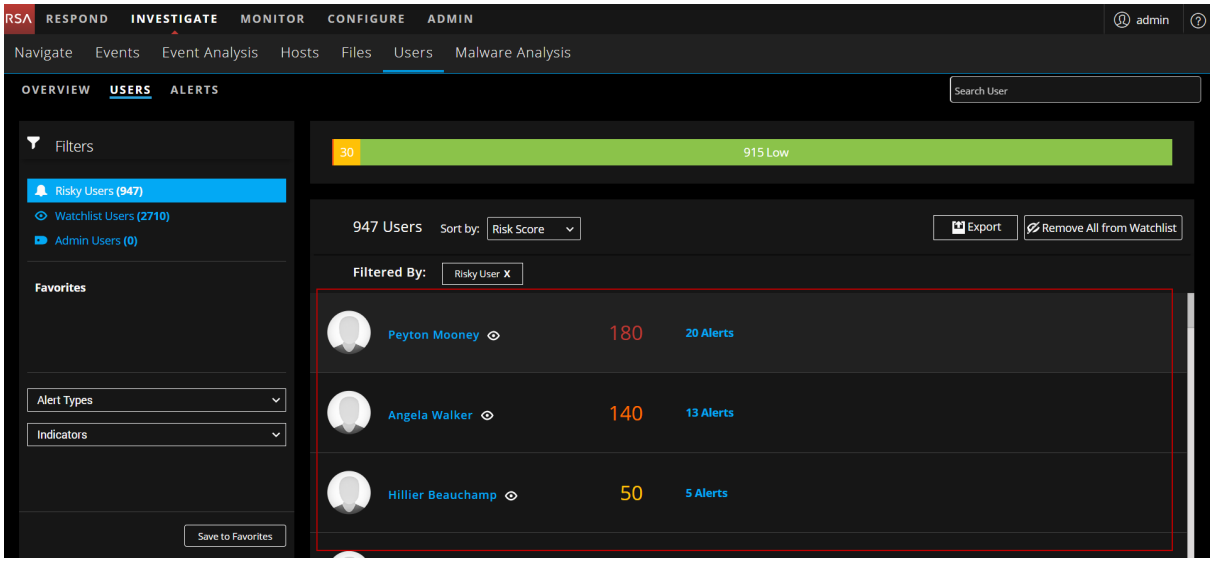
Connectez-vous à **NetWitness Platform** et accédez à **Enquêter** > **Utilisateurs**.
L'onglet Tour d'horizon s'affiche avec les utilisateurs à haut risque affichés dans le panneau Utilisateurs à haut risque.

Afficher tous les utilisateurs à haut risque

Dans l'onglet **Utilisateurs**, vous pouvez afficher la liste de tous les utilisateurs à haut risque dans votre environnement, ainsi que la note d'utilisateur et le nombre total d'alertes associées aux utilisateurs.

Pour afficher tous les utilisateurs à haut risque :

1. Connectez-vous à **NetWitness Platform** et accédez à **Enquêter** > **Utilisateurs**.
   L'onglet Tour d'horizon s'affiche.
2. Cliquez sur l'onglet **Utilisateurs**.
   La liste de tous les utilisateurs à haut risque s'affiche.

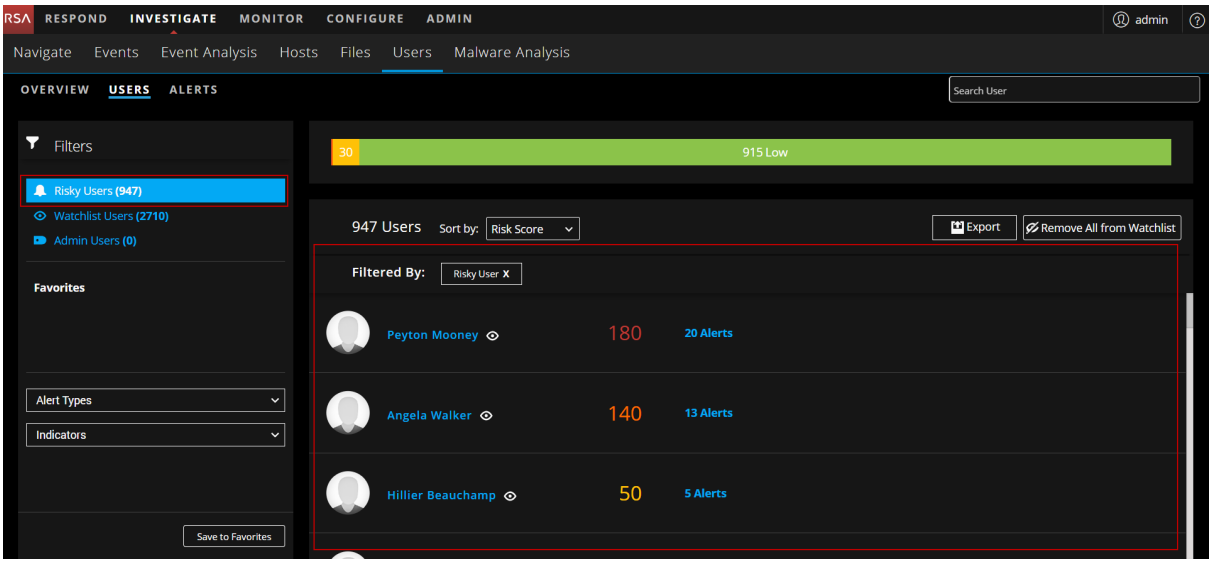


Afficher les utilisateurs d'un groupe spécifique

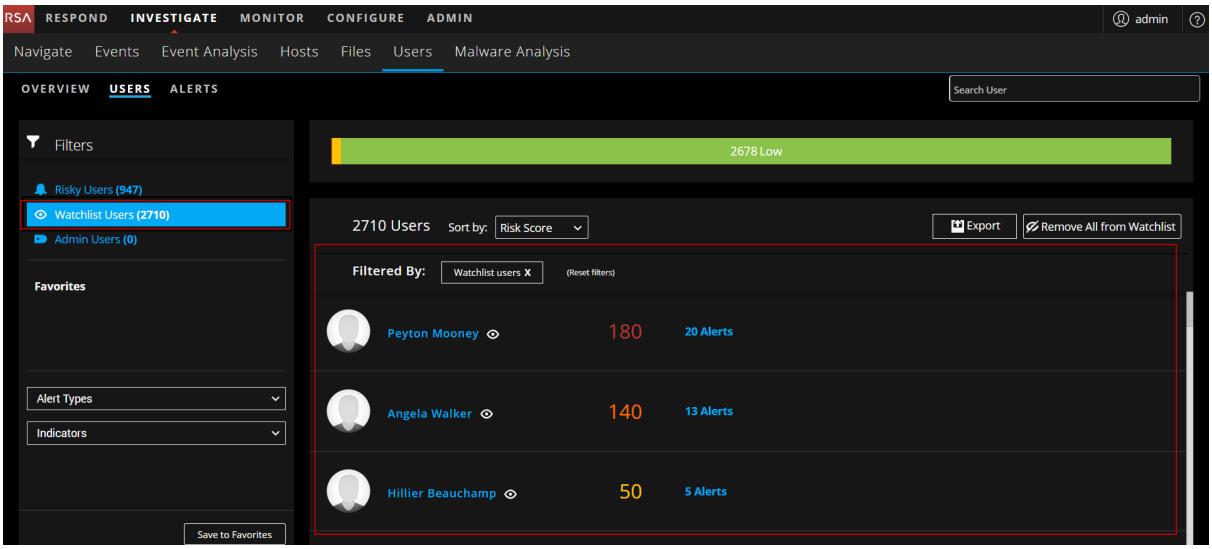
Dans l'onglet **Utilisateurs**, vous pouvez utiliser différents types de filtres pour identifier le groupe ciblé d'utilisateurs à haut risque.

Pour afficher les utilisateurs d'un groupe spécifique :

1. Connectez-vous à **NetWitness Platform** et accédez à **Enquêter** > **Utilisateurs**.
   L'onglet Tour d'horizon s'affiche.
2. Cliquez sur l'onglet **Utilisateurs**.
3. Dans le panneau **Filtres**, effectuez l'une des opérations suivantes :
   - **Utilisateurs à risque** : Pour afficher tous les utilisateurs à risque dans votre environnement, sélectionnez **Utilisateurs à risque**. Par défaut, les utilisateurs à risque ainsi que leur note utilisateur sont affichés.



- **Utilisateurs de la liste de surveillance** : Pour afficher la liste des utilisateurs que vous avez ajoutés à la liste de surveillance pour surveiller des modifications spécifiques, sélectionnez **Utilisateurs de la liste de surveillance**.



- **Utilisateurs administrateurs** : Pour afficher tous les utilisateurs marqués comme administrateurs dans les événements, sélectionnez **Utilisateurs administrateurs**.

Remarque : Vous pouvez afficher les utilisateurs d'un ou de plusieurs groupes en sélectionnant un ou plusieurs filtres. Par exemple, si vous souhaitez afficher la liste des utilisateurs administrateurs qui sont des utilisateurs à risque, sélectionnez les filtres **Utilisateurs administrateurs** et **Utilisateurs à risque**.

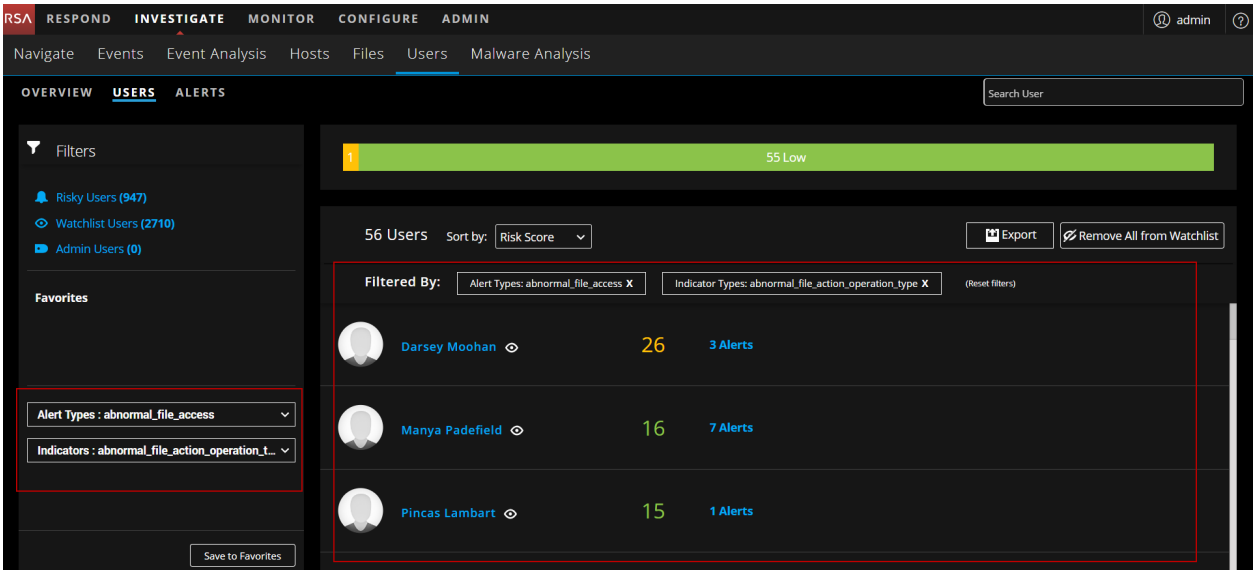
Afficher les utilisateurs sur la base de l'enquête légale

Dans l'onglet **Utilisateurs**, vous pouvez utiliser Types d'alerte et Indicateurs qui sont des filtres comportementaux pour afficher les utilisateurs à haut risque basé sur l'enquête légale. Pour plus d'informations sur l'enquête légale, consultez *Flux de travail légal* dans la rubrique Introduction.

Pour afficher les utilisateurs sur la base d'une enquête légale spécifique :

1. Connectez-vous à **NetWitness Platform** et accédez à **Enquêter** > **Utilisateurs**. L'onglet Tour d'horizon s'affiche.
2. Cliquez sur l'onglet **Utilisateurs**.
3. Pour créer un filtre comportemental à l'aide des types d'alerte, sélectionnez une ou plusieurs alertes dans la liste déroulante **Types d'alerte**.
4. Pour créer un filtre comportemental à l'aide d'indicateurs, sélectionnez un ou plusieurs indicateurs dans la liste déroulante **Indicateurs**.

Remarque : Vous pouvez sélectionner une combinaison d'un ou plusieurs types d'alertes et d'indicateurs pour créer un filtre comportemental en fonction de vos besoins. Par exemple, pour surveiller l'accès anormal aux fichiers confidentiels et le vol de données sensibles, vous pouvez créer un filtre comportemental avec Types d'alertes = **Accès anormal aux fichiers** et Indicateurs = **Type d'opération d'action de fichier anormal**.



Vous enregistrez ces filtres comportementaux comme favoris pour une enquête future.

Commencer une investigation sur les utilisateurs à haut risque

Après avoir identifié les utilisateurs à haut risque, vous pouvez commencer l'investigation des utilisateurs à haut risque.

Pour enquêter sur les utilisateurs à haut risque :

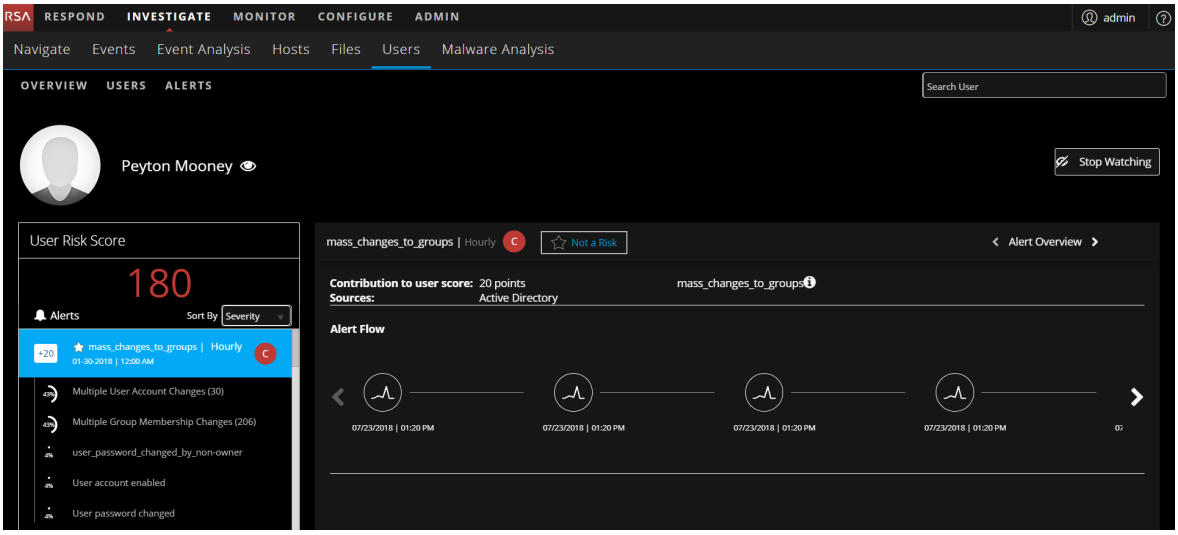
1. Connectez-vous à **NetWitness Platform** et accédez à **ENQUÊTER** > **Utilisateurs**. Effectuez l'une des opérations suivantes :

   a. Dans l'onglet **Tour d'horizon**, dans le panneau **Utilisateurs à risque élevé**, sélectionnez un utilisateur sur lequel vous souhaitez enquêter, puis cliquez sur le nom d'utilisateur ou sa note.

   b. Dans l'onglet **UTILISATEURS**, sélectionnez l'utilisateur sur lequel vous souhaitez enquêter et cliquez sur le nom d'utilisateur.
   La vue Profil d'utilisateur s'affiche.

2. Pour enquêter sur les alertes de l'utilisateur, cliquez sur le nom de l'alerte dans le panneau **Valeur de risque de l'utilisateur**. Les informations suivantes s'affichent :

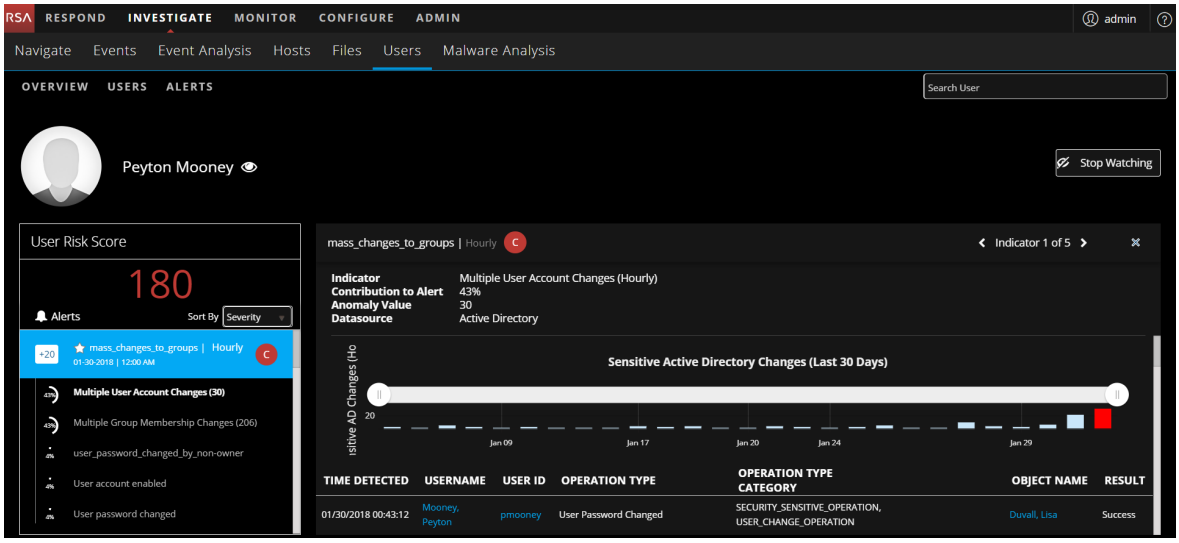
   - Le nom de l'alerte
   - Le délai de l'alerte (horaire ou journalier)
   - L'icône de niveau de gravité
   - La contribution à la valeur de score de l'utilisateur (par exemple, +20)
   - Les sources de données pour l'alerte (par exemple, Connexion)
     Le panneau du milieu est le panneau Flux d'alerte. Ce panneau fournit une chronologie des événements liés à la formation de l'alerte. La chronologie des événements peut aider à déterminer si l'alerte constitue un risque réel.



3. Pour enquêter sur les indicateurs associés à l'alerte d'un utilisateur, dans le panneau **Valeur de risque de l'utilisateur**, sélectionnez une alerte, puis sélectionnez un indicateur. Les informations suivantes s'affichent :

   - Le nom de l'indicateur et une description du type d'indicateur
   - La contribution à Alerte
   - Les valeurs d'anomalie

- La source de données des événements trouvés dans l'indicateur
  L'affichage du panneau central change en fonction de l'indicateur sélectionné.



Prendre des mesures sur les utilisateurs à haut risque

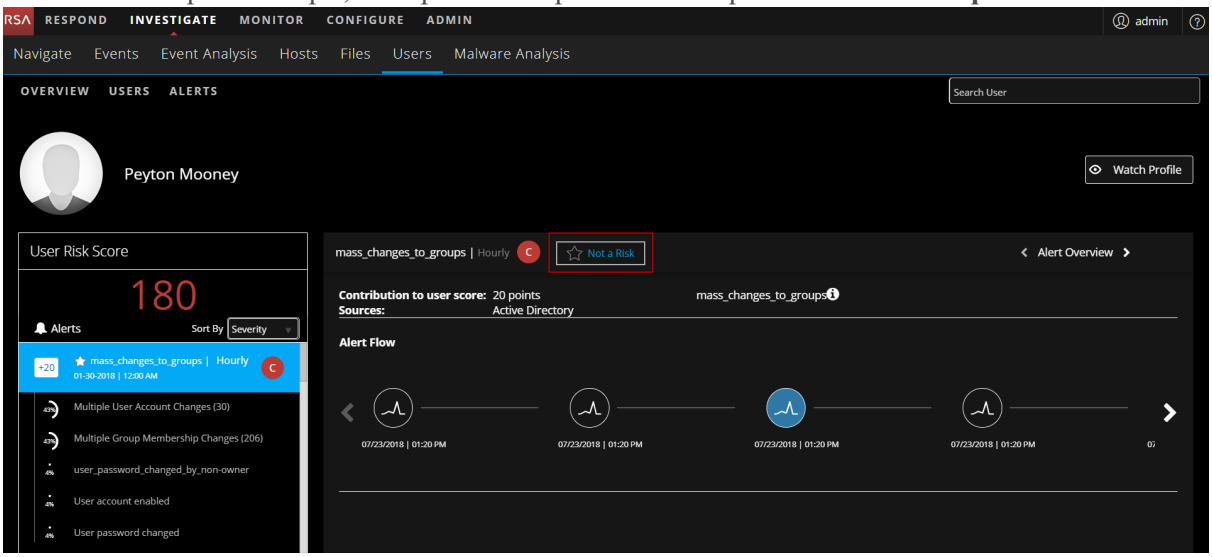
Après l'enquête, vous pouvez prendre des mesures sur les utilisateurs à risque pour réduire ou prévenir d'autres dommages causés par des attaquants malveillants dans votre organisation. Vous pouvez effectuer l'une des actions suivantes :

- Spécifier si l'alerte n'est pas un risque
- Enregistrer le profil comportemental pour le cas d'utilisation trouvé dans votre environnement
- Ajouter des utilisateurs à la liste de surveillance et regarder le profil utilisateur si vous souhaitez conserver une trace de l'activité utilisateur.

Spécifier si l’alerte n'est pas un risque.

Pour spécifier si l’alerte n'est pas un risque :

1. Connectez-vous à **NetWitness Platform** et accédez à **ENQUÊTER** > **Utilisateurs**.
2. Prendre des mesures sur les utilisateurs à partir de l'un des onglets suivants :
   a. Dans l'onglet **Tour d'horizon**, dans le panneau **Utilisateurs à risque élevé**, sélectionnez un utilisateur, puis cliquez sur le nom d'utilisateur ou sa note utilisateur.
   b. Sous l'onglet **Utilisateurs**, sélectionnez un utilisateur, puis cliquez sur le nom d'utilisateur. La vue Profil d’utilisateur s'affiche.
3. Si l'alerte n'est pas un risque, vous pouvez le spécifier en cliquant sur **Pas un risque**.



Lorsqu'une alerte est marquée comme n’étant **Pas un risque**, la note de l'utilisateur est automatiquement réduite.

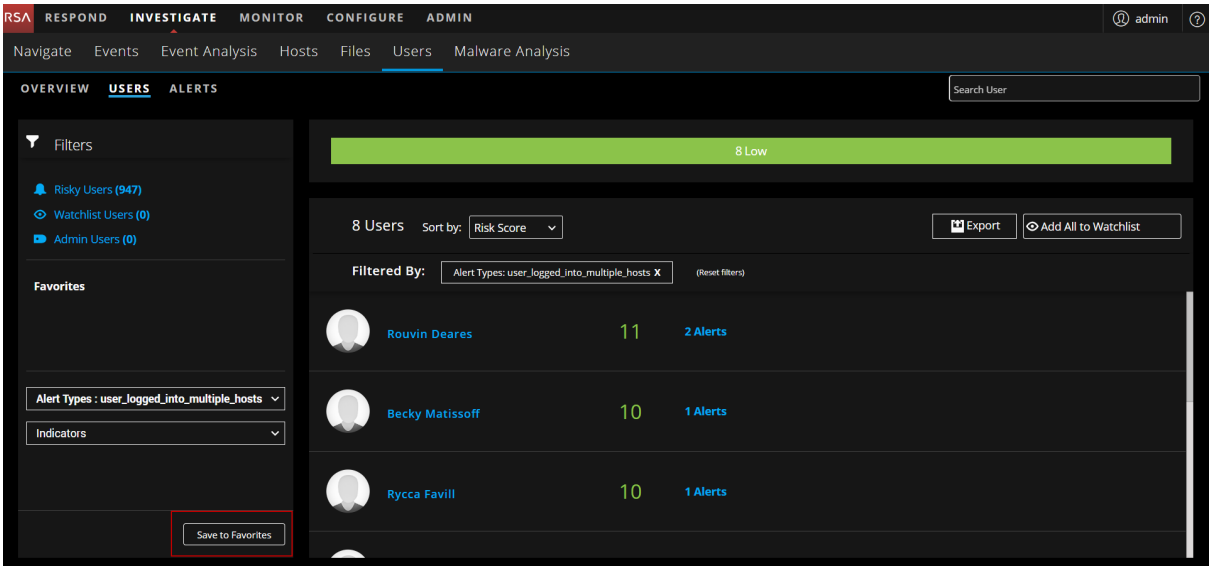
Enregistrer le profil comportemental

La combinaison des types d'alerte et des indicateurs que vous sélectionnez lors de l'enquête légale est un profil comportemental. Vous pouvez enregistrer le profil comportemental, de sorte que vous pouvez surveiller ce cas d'utilisation à l'avenir.

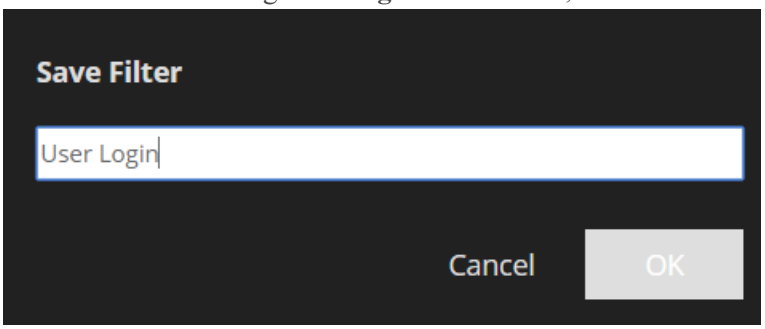
Par exemple, si votre organisation est attaquée et que les attaquants ont pénétrés par des comptes utilisateurs forcés, vous pouvez sélectionner des filtres à l'aide du type d'alerte en force. Cela peut être enregistré comme favori. Vous pouvez surveiller de manière proactive les futures attaques en force. Pour ce faire, vous pouvez cliquer sur le favori pour voir si les nouveaux utilisateurs ont été soumis à ce type d'attaque.

Pour enregistrer le profil comportemental :

1. Connectez-vous à **NetWitness Platform** et accédez à **ENQUÊTER** > **Utilisateurs**. L'onglet Tour d'horizon s'affiche.
2. Cliquez sur l'onglet **Utilisateurs**.
3. Dans le panneau **Filtres**, sélectionnez le l'alerte dans la liste déroulante **Type d'alerte** et les indicateurs dans la liste déroulante **Indicateurs**.
4. Cliquez sur **Enregistrer dans les favoris**.



5. Dans la boîte de dialogue **Enregistrer le filtre**, saisissez le nom du filtre et cliquez sur **OK**.



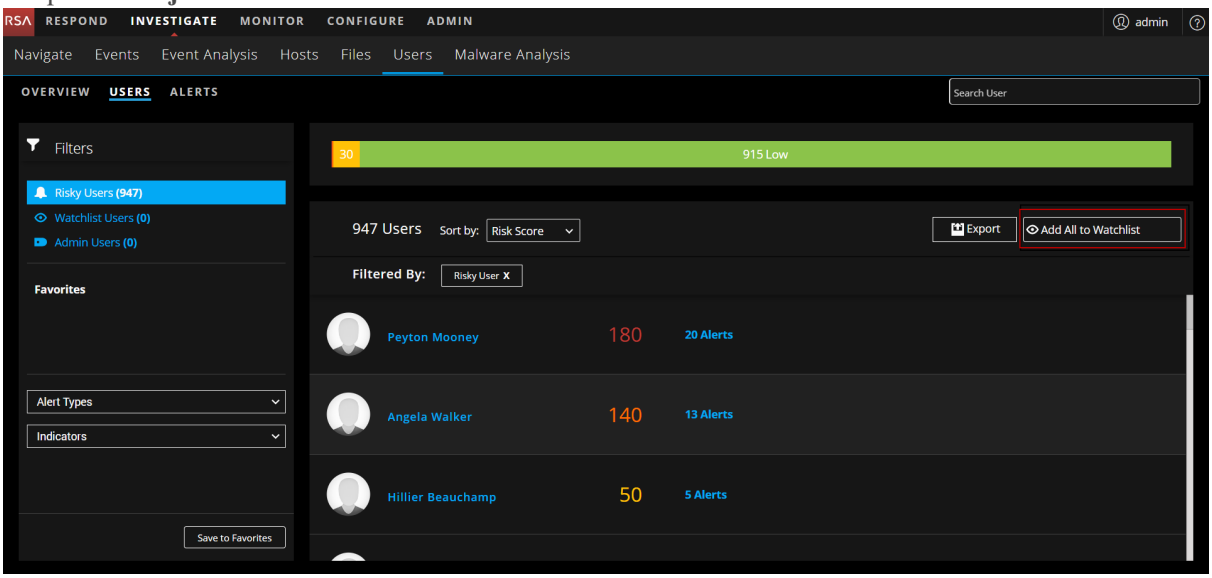
Le profil de recherche est enregistré et affiché dans le panneau Favoris. Vous pouvez cliquer sur le profil dans les Favoris pour surveiller les utilisateurs.

Ajouter tous les utilisateurs à la liste de surveillance

Si vous voulez garder une trace des utilisateurs avec une activité récente, mais que vous ne voulez pas de suivi avec une enquête immédiate, vous pouvez ajouter les utilisateurs à la liste de surveillance et la revoir au fil du temps pour voir si la valeur de risque est élevée.

Ajouter tous les utilisateurs à la liste de surveillance :

1. Connectez-vous à **NetWitness Platform** et accédez à **ENQUÊTER** > **Utilisateurs**. L'onglet Tour d'horizon s'affiche.
2. Sélectionnez l'onglet **Utilisateurs**.
3. Sélectionnez les utilisateurs de catégories spécifiques à l'aide de filtres.
4. Cliquez sur **Ajouter tous les utilisateurs à la liste de surveillance**.



La liste des utilisateurs est ajoutée à la liste de surveillance.

Surveiller le profil utilisateur

Surveiller le profil utilisateur est une liste d'utilisateurs que vous souhaitez surveiller par rapport aux menaces potentielles. Surveiller le profil utilisateur marque un utilisateur afin que les utilisateurs puissent être rapidement référencés sur le tableau de bord. Il s'agit essentiellement d'un signet pour surveiller les utilisateurs suspects.

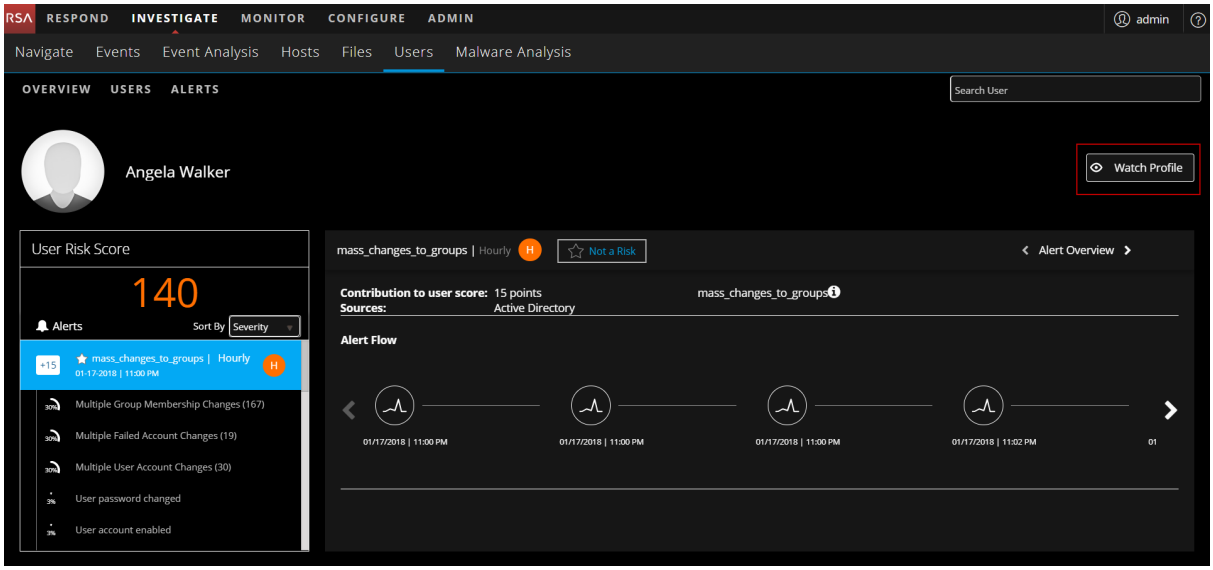
Pour surveiller le profil utilisateur :

1. Connectez-vous à **NetWitness Platform** et accédez à **ENQUÊTER** > **Utilisateurs**. Effectuez l'une des opérations suivantes :

   a. Dans l'onglet **Tour d'horizon**, sous le volet **Utilisateurs à risque élevé**, sélectionnez un utilisateur, puis cliquez sur le nom d'utilisateur ou sa note utilisateur.

   b. Sous l'onglet **Utilisateurs**, sélectionnez un utilisateur, puis cliquez sur le nom d'utilisateur.
   La vue Profil d'utilisateur s'affiche.

2. Cliquez sur **Surveiller le profil** dans le coin supérieur droit du profil utilisateur.



   L'utilisateur est ajouté à la liste de surveillance.

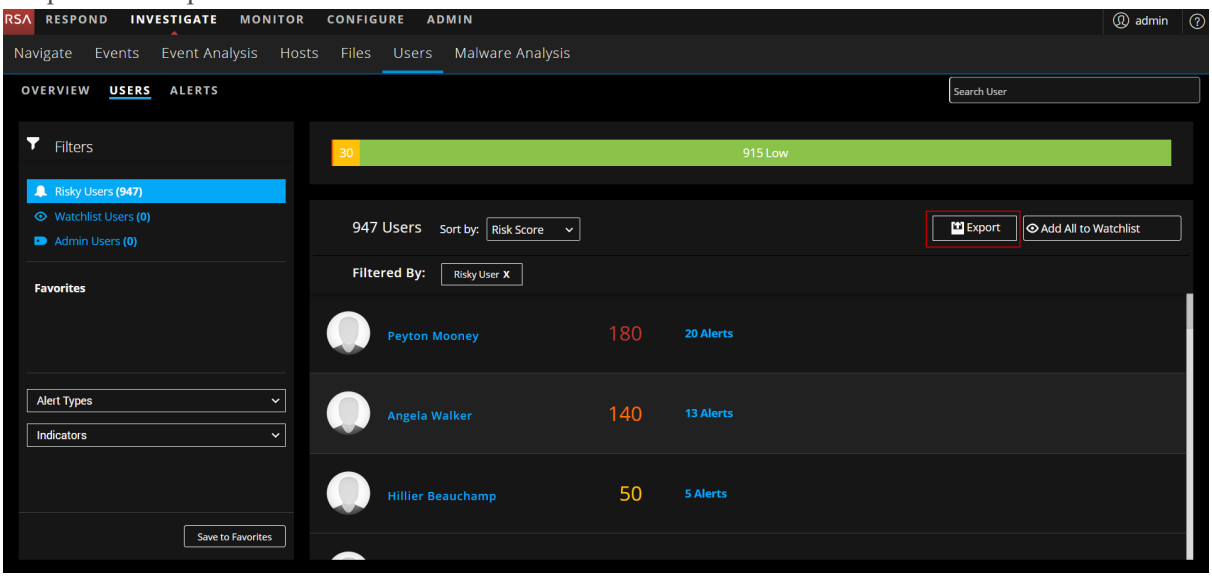
Exporter des utilisateurs à haut risque

Vous pouvez exporter une liste de tous les utilisateurs et leurs notes dans un format de fichier. csv. Vous pouvez utiliser ces informations pour les comparer avec d'autres outils d'analyse de données tels que tableau, powerbi et zeppelin.

Exporter des utilisateurs à haut risque :

1. Accédez à **ENQUÊTER** > **Utilisateurs**.
   L'onglet Tour d'horizon s'affiche.
2. Sélectionnez l'onglet **Utilisateurs**.

3. Cliquez sur Exporter.



La liste de tous les utilisateurs et la note d'utilisateur associée sont téléchargés au format de fichier. csv.

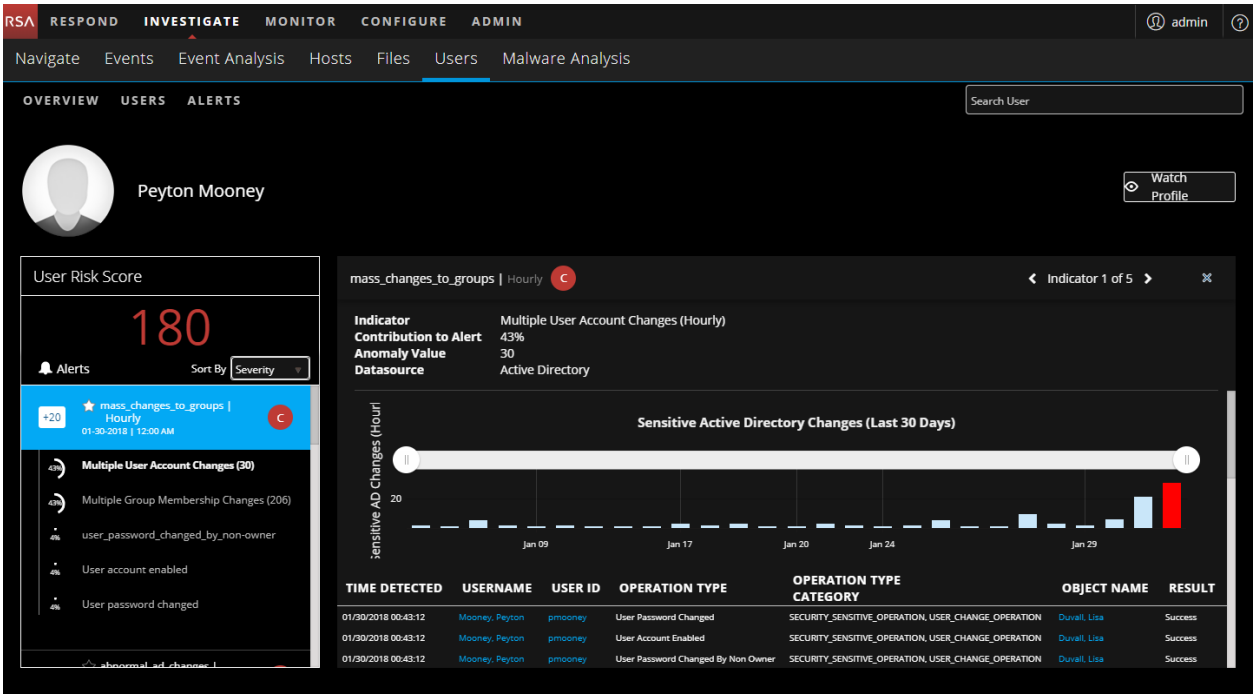
Enquêter sur les alertes principales

Les anomalies qui sont trouvées comme des événements entrants sont comparées à la valeur de référence et sont compilées en alertes horaires. Des écarts relativement importants par rapport à la valeur de référence, ainsi qu'une composition unique d'anomalies, sont plus susceptibles d'obtenir une note d'alerte plus élevée.

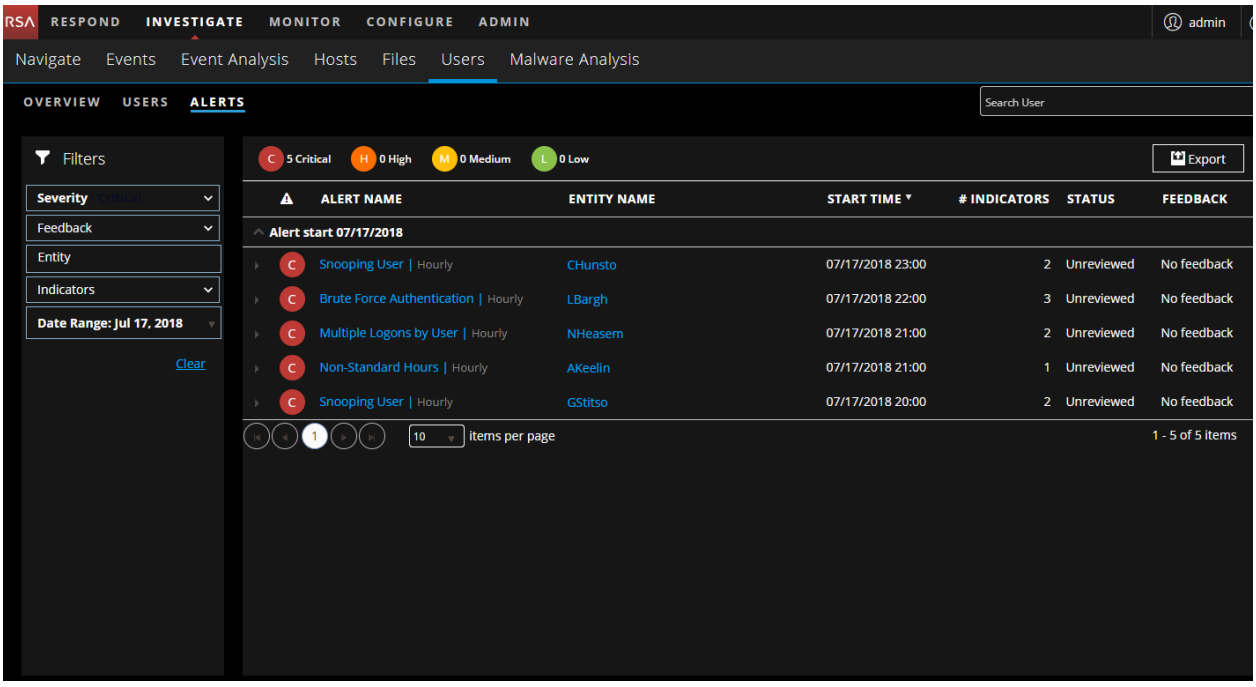
Vous pouvez rapidement afficher les alertes les plus critiques dans votre environnement et commencer à enquêter dessus à partir de l'onglet TOUR D'HORIZON ou de l'onglet ALERTES. La figure suivante est un exemple des principales alertes dans l'onglet TOUR D'HORIZON. Les alertes sont répertoriées par ordre de gravité et le nombre d'utilisateurs qui génèrent les alertes.

Pour enquêter sur une alerte sur cette page, cliquez sur une alerte dans la section **Alertes principales** pour afficher les détails sur l'alerte.

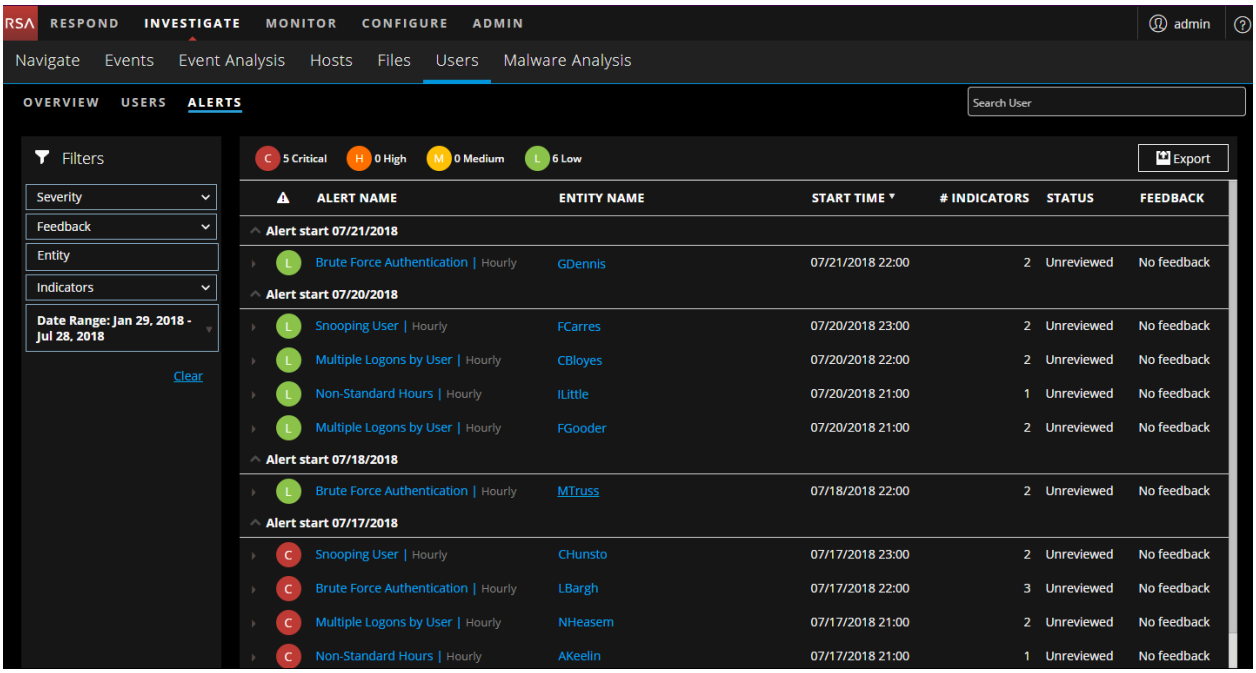
La figure suivante montre des détails sur l'événement ayant provoqué l'alerte et la période dans laquelle il s'est produit.



Dans l'onglet TOUR D'HORIZON, dans le panneau Gravité des alertes, vous pouvez cliquer sur une barre du graphique pour consulter les alertes principales dans l'onglet ALERTES, comme illustré dans la figure suivante.



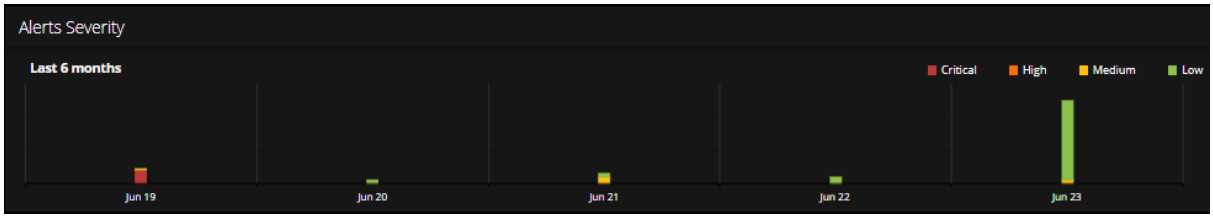
Enquêter sur les alertes est particulièrement utile lorsque vous souhaitez vous concentrer sur une période pendant laquelle vous pensez que vos systèmes ont été compromis. Vous pouvez afficher les informations légales en fonction d'une période et collecter des informations détaillées sur les événements survenus pendant cette période dans l'onglet Alertes.



Commencer une enquête sur les alertes critiques

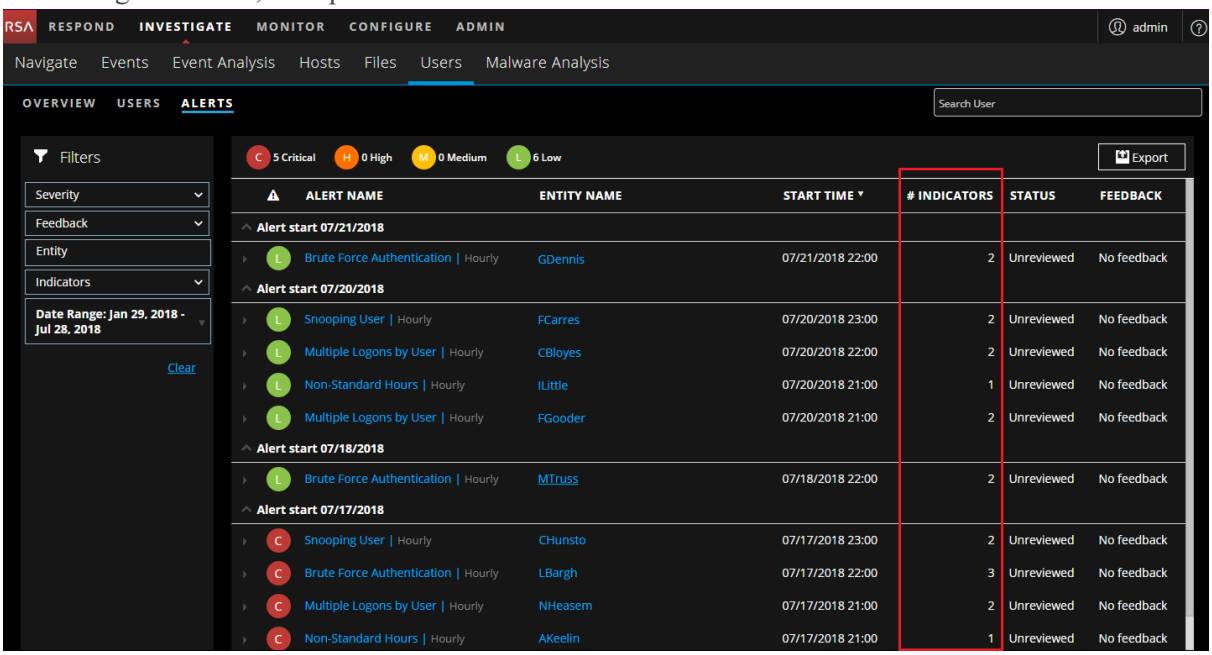
Vous pouvez commencer votre enquête sur les alertes critiques de la manière suivante :

1. Sous l'onglet Tour d'horizon, examinez la gravité des alertes.



La distribution des alertes est-elle uniforme ou un pic peut-il être observé pour quelques jours ? Un pic pourrait indiquer quelque chose de suspect comme un malware. Prenez note de ces jours afin que vous puissiez inspecter les alertes (la barre à partir du graphique est directement liée aux alertes pour ce jour spécifique).

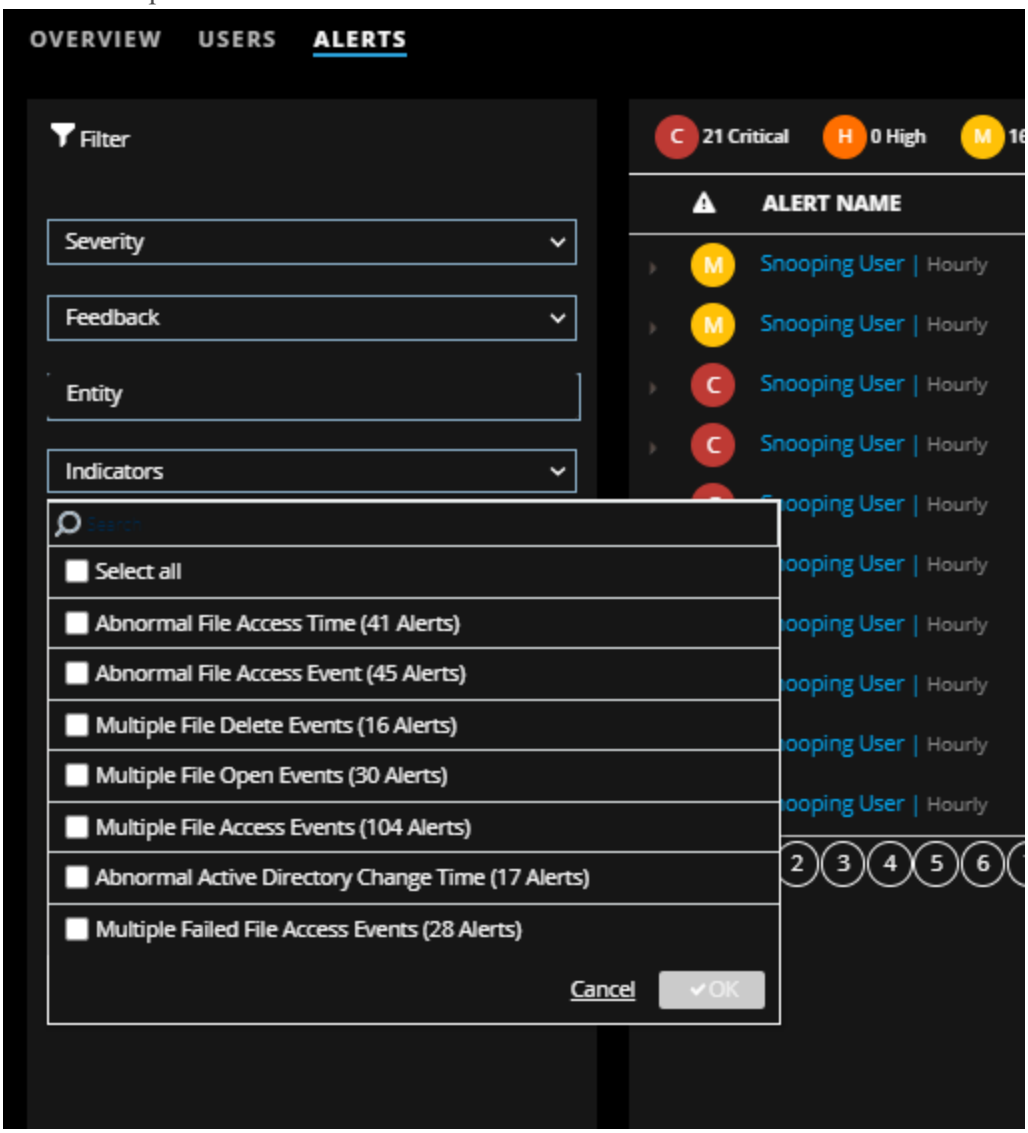
2. Dans l'onglet Alertes, trier par le nombre d'indicateurs :



Assurez-vous que les alertes ayant regroupé le plus grand nombre d'indicateurs apparaissent en haut de la liste. Comme pour identifier les utilisateurs avec le plus grand nombre d'alertes, plus d'indicateurs aident à illustrer une histoire plus intéressante et vous fournir une chronologie plus solide que vous pouvez suivre.

3. Développez les alertes principales dans la liste :
   - Recherchez les alertes qui ont des sources de données variées. Celles-ci montrent un profil de comportement plus large.
   - Recherchez une variété d'indicateurs différents.
   - Recherchez des indicateurs avec des valeurs numériques élevées, en particulier des valeurs élevées qui n'indiquent pas une activité qu'un être humain puisse effectuer manuellement (par exemple, un utilisateur a accédé à 8 000 fichiers).
4. Recherchez des types d'événements Windows uniques que les utilisateurs ne changent généralement pas car ils peuvent indiquer une activité administrative suspecte.

5. Rechercher par indicateurs :



La liste indique le nombre d'alertes soulevées qui contiennent chaque indicateur.

- Recherchez les plus importants indicateurs de volume ; utilisez un filtre de volume et révisez par utilisateur pour trouver les utilisateurs qui ont connu le plus grand nombre de ces indicateurs.
- En général, vous pouvez ignorer les alertes temporelles (par exemple, temps d'ouverture de session anormal) car elles sont très fréquentes. Cependant, ils fournissent un bon contexte lorsqu'ils sont combinés avec des indicateurs d'intérêt plus élevés.

6. Effectuer une recherche en détail :

- Tirez parti des noms d'alerte pour commencer à établir un récit de menace. Utilisez le fait que l'indicateur de contribution le plus fort détermine généralement le nom de l'alerte pour commencer à expliquer pourquoi cet utilisateur est marqué.
- Utilisez la chronologie pour mettre en page les activités trouvées et essayez de comprendre ce qui pourrait expliquer les comportements observés.

- Poursuivez en examinant chaque indicateur et en démontrant comment les informations de support, sous forme de graphiques et d'événements, peuvent aider les analystes à vérifier un incident. Suggérez les prochaines étapes de l'enquête à l'aide de ressources externes (par exemple, SIEM, analyse légale du réseau, et toucher directement l'utilisateur ou un administrateur délégué).
- Terminez l'enquête en demandant des réactions et en laissant un commentaire.

7. Prenez des mesures pour contrer les menaces déterminées par votre enquête sur les alertes. Pour plus d'informations, consultez Prendre des mesures sur les utilisateurs à haut risque.

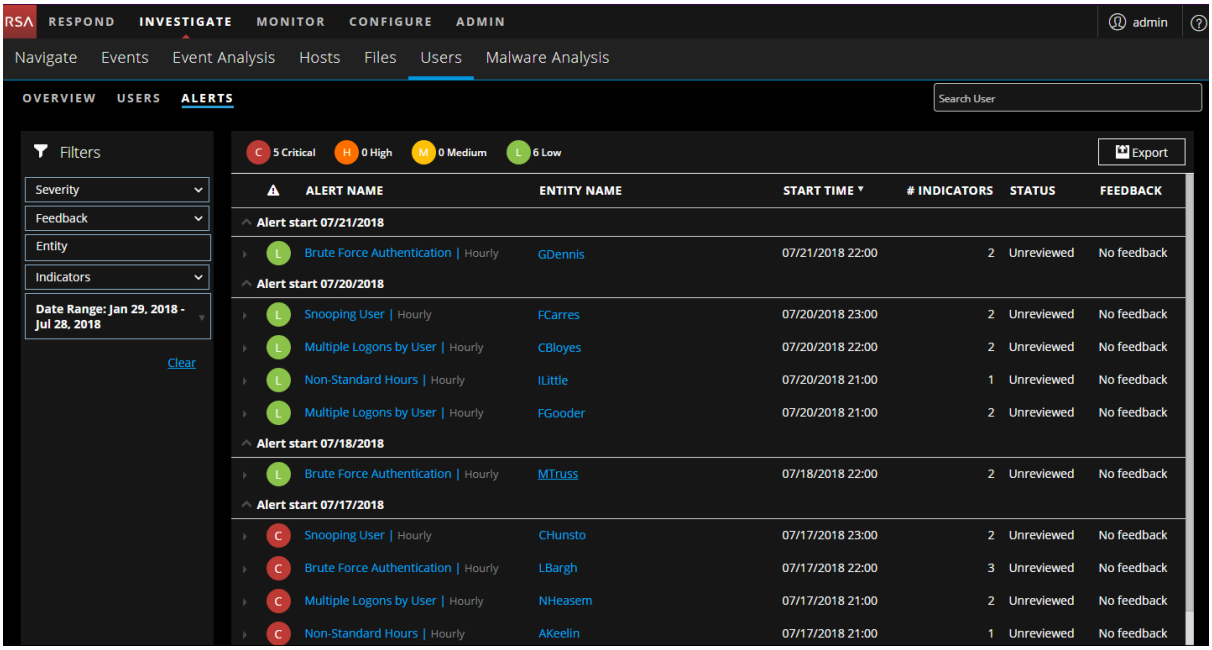
Les rubriques suivantes expliquent différentes façons d'enquêter sur les alertes.

- Filtrer les alertes
- Enquêter sur les indicateurs
- Gérer les alertes principales
- Voir les mesures NetWitness UEBA dans Intégrité

Filtrer les alertes

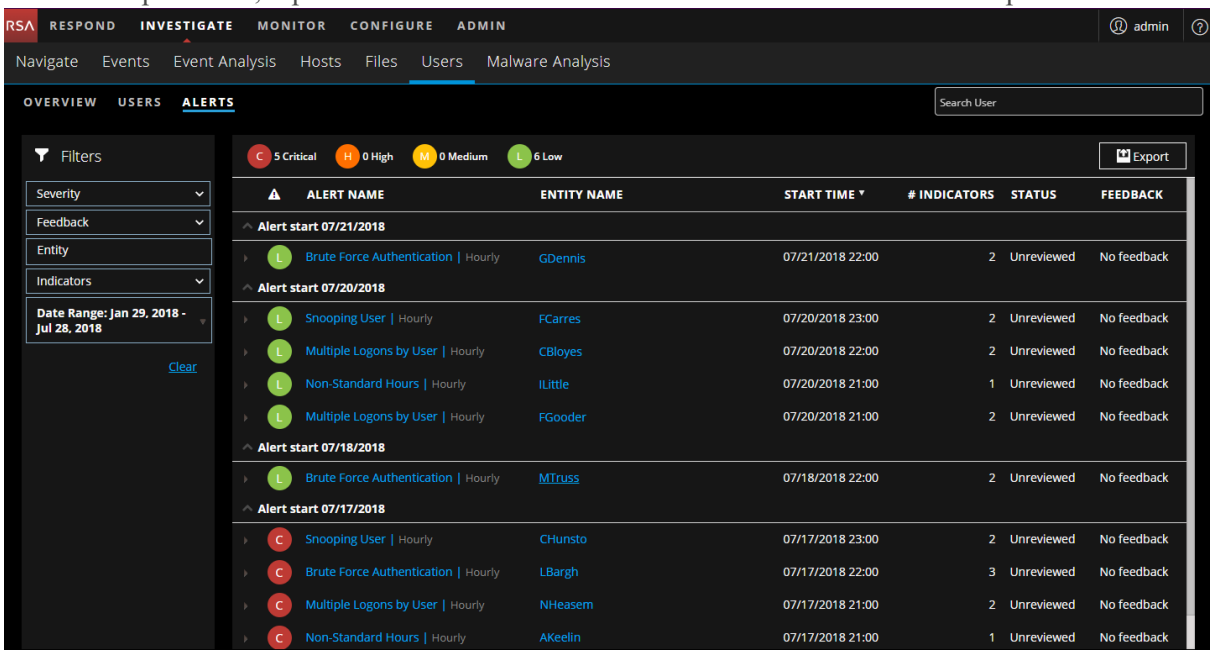
Vous pouvez filtrer les alertes affichées dans l'onglet Alertes par gravité, rétroaction, entité, indicateurs et plage de dates.

1. Connectez-vous à NetWitness Platform et cliquez sur **ENQUÊTER** > **Utilisateurs** > **Alertes**. L'onglet Alerte s'affiche.



2. Pour filtrer par gravité, cliquez sur **Gravité** dans le panneau **Filtrer les alertes**, sélectionnez une ou plusieurs options, puis cliquez sur **OK**. Les options sont Sélectionner tout, Critique, Élevée, Moyenne et Faible.

3. Pour filtrer par commentaires, cliquez sur la flèche vers le bas sous **Commentaires**, sélectionnez une ou plusieurs options, puis cliquez sur **OK**. Les options sont Sélectionner tout, Pas de rétroaction, et Pas un risque.
4. Pour filtrer par entité, tapez un nom d'utilisateur ou le nom d'une entité dans le champ **Entité**.



5. Pour filtrer par plage de dates, cliquez sur la flèche vers le bas **Période**, sélectionnez une option, puis cliquez sur **OK**. Les options sont Semaine dernière, Mois dernier et Sélectionner la plage.

Les alertes sont affichées dans le volet droit en fonction du filtre que vous avez sélectionné. Pour effacer les filtres, dans le volet gauche, cliquez sur **Effacer**.

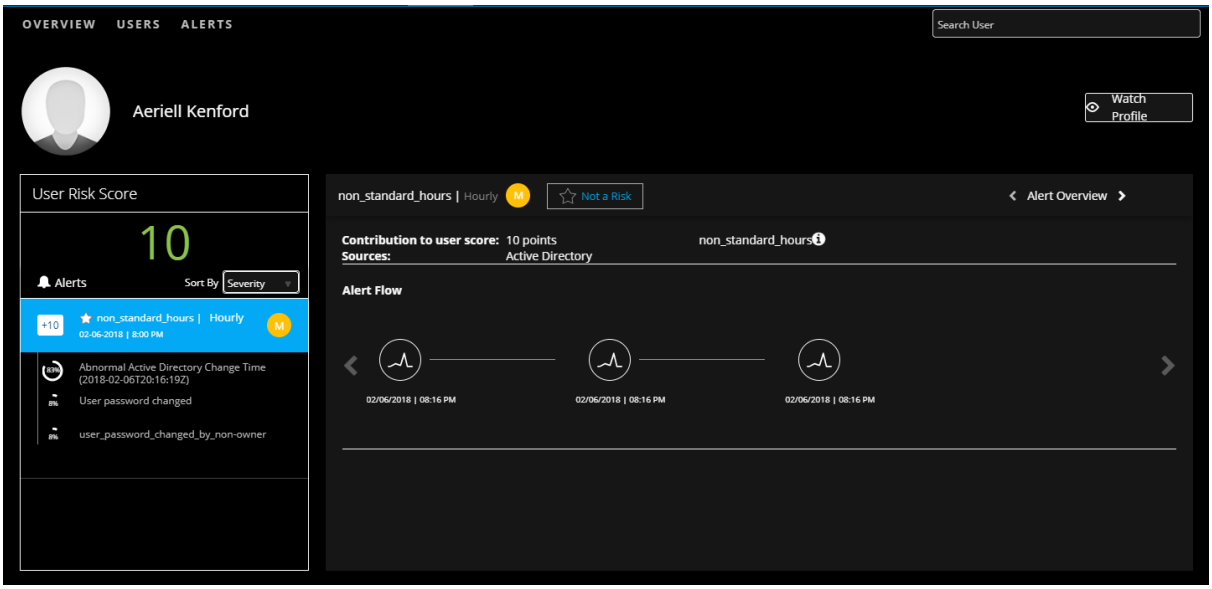
Enquêter sur les indicateurs

Vous pouvez afficher tous les indicateurs qui forment une alerte dans l'onglet ALERTES. Chaque indicateur affiche également sa valeur d'anomalie entre parenthèses. Vous pouvez trouver le nom de l'indicateur et une description du type d'indicateur, les valeurs d'anomalie et la source de données des événements trouvés dans l'indicateur. Vous pouvez également afficher un graphique qui montre les détails d'un indicateur spécifique. Vous pouvez rechercher un indicateur pour rechercher une activité connexe dans une plage de temps en pivotant vers la vue **ENQUÊTER** > **Événements**. Dans la vue Utilisateurs, les valeurs qui activent le pivot sont mises en surbrillance en bleu clair, et vous pouvez cliquer sur une valeur pour ouvrir la vue Événement. Une fois dans la vue Événement, la valeur sélectionnée est définie dans toutes les clés méta et la plage de temps est définie sur un jour. Il est possible de modifier la plage horaire.

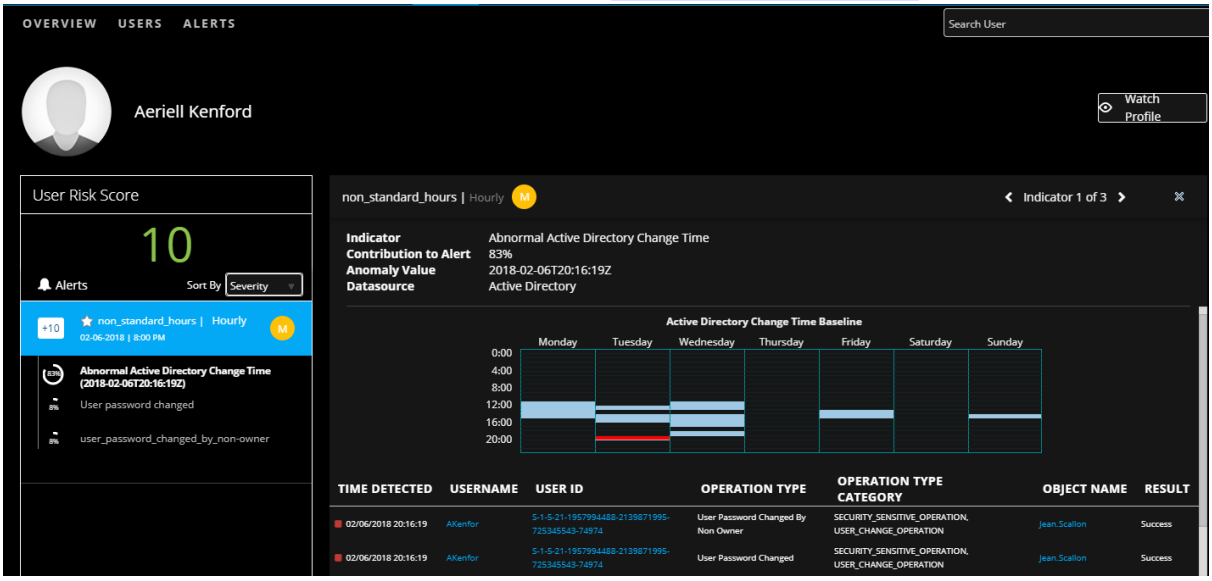
Pour voir tous les indicateurs de menace qui composent une alerte :

1. Connectez-vous à NetWitness Platform et cliquez sur **ENQUÊTER** > **Utilisateurs** > **ALERTES**.
2. Sous **NOM DE L'ALERTE**, cliquez sur un nom d'alerte.
   Les indicateurs sont affichés, ainsi que la valeur de l'anomalie, la source de données et l'heure de

début.



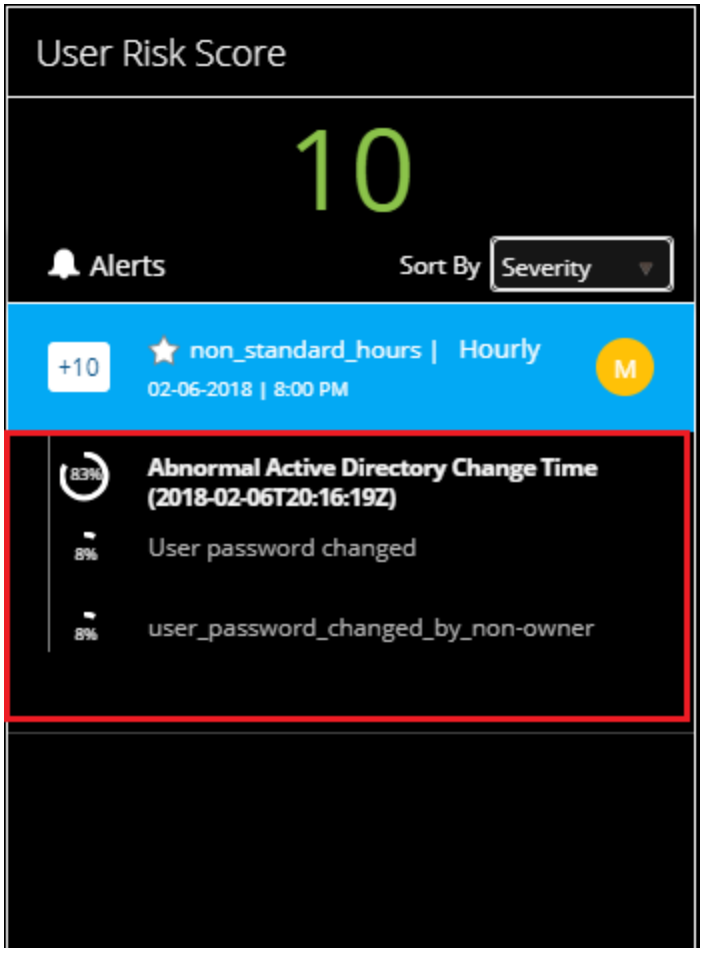
3. Sous **Flux d'alerte**, cliquez sur l'icône du graphique.
   Un graphique affiche des détails sur un indicateur spécifique, y compris la chronologie dans laquelle l'anomalie s'est produite et l'utilisateur associé à l'indicateur. La figure ci-dessous présente un exemple du graphique. Le type de graphique peut varier, selon le type d'analyse effectué par NetWitness UEBA. Pour en savoir plus, consultez Vue du profil d'utilisateur.



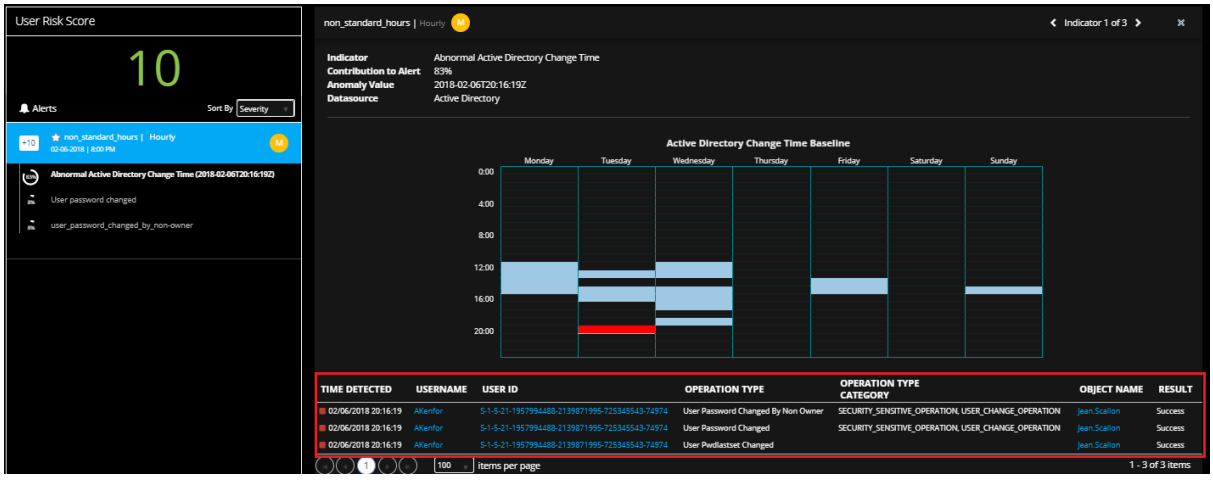
Pour pivoter vers la vue Événements :

1. Accédez à **ENQUÊTER** > **Utilisateurs**, puis sélectionnez une alerte ou un utilisateur.

2. Sous **Valeur de risque de l'utilisateur**, sélectionnez un nom d'alerte.
   Les indicateurs sont affichés sous l'alerte.



3. Sélectionnez un indicateur d'intérêt.
   Les valeurs qui peuvent être utilisées pour pivoter sont mises en surbrillance en bleu clair au bas du panneau.



4. Cliquez sur un élément indicateur surligné en bleu.
   La vue Événements s'ouvre et des détails sur l'élément indicateur s'affichent.

La date dans la vue Événements est le jour où l'alerte s'est produite. Le texte dans le champ de recherche est la valeur que vous avez sélectionnée. Les événements qui sont affichés sont tous les événements liés à la valeur sélectionnée.

Pour plus d'informations sur la recherche d'éléments présentant un intérêt dans la vue Événements, consultez « Procédure d'enquête relative aux événements bruts dans la vue Événements » dans le *Guide d'utilisation de NetWitness Investigate*.

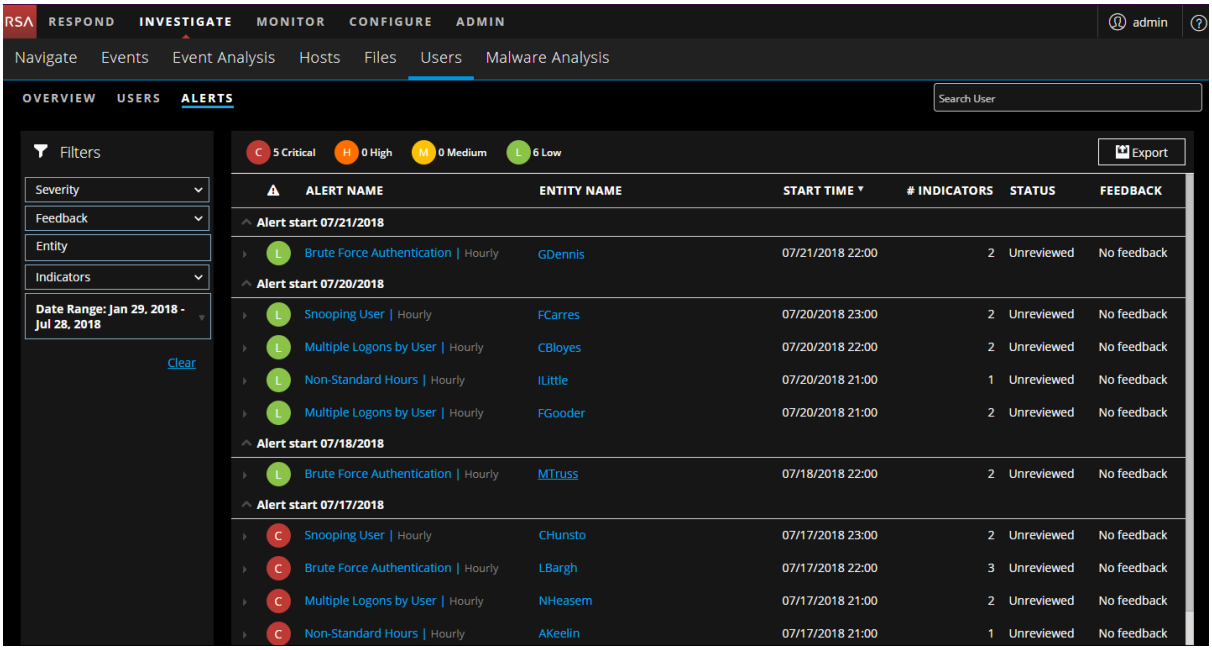
Pour plus d'informations sur les indicateurs de menace, consultez la section Indicateurs de menace dans Introduction

Gérer les alertes principales

Vous pouvez exporter une liste de toutes les alertes vers un format de fichier. csv. Un analyste peut utiliser ces informations pour comparer les données provenant d'autres sources dans d'autres outils d'analyse des données comme tableau, powerbi et zeppelin.

Pour exporter des données d'alerte vers un fichier. csv :

1. Connectez-vous à NetWitness Platform et cliquez sur **ENQUÊTER** > **Utilisateurs** > **ALERTES**. L'onglet Alerte s'affiche.



2. En haut à droite, cliquez sur **Exporter**.
   Toutes les données d'alerte sont téléchargées dans un format de fichier. csv. Voici un exemple des données d'alerte exportées au format. csv :

	A	B	C	D	E	F	G
1	Alert Name	Entity Name	Start Time	# of Indicators	Status	Feedback	Severity
2	Brute Force Au	presidio_4769_u	Jul 21 2018 22:0	2	Reviewed	No Feedback	Low
3	Snooping User	4769_user122	Jul 20 2018 23:0	2	Reviewed	No Feedback	Low
4	Multiple Logon	presidio_4769_u	Jul 20 2018 22:0	2	Reviewed	No Feedback	Low
5	Non-Standard I	4769_user122	Jul 20 2018 21:0	1	Reviewed	No Feedback	Low
6	Multiple Logon	PRESIDIO_USER:	Jul 20 2018 21:0	2	Reviewed	No Feedback	Low
7	Brute Force Au	presidio_4769_u	Jul 18 2018 22:0	2	Reviewed	No Feedback	Low
8	Snooping User	4769_user122	Jul 17 2018 23:0	2	Reviewed	No Feedback	Critical
9	Brute Force Au	presidio_4769_u	Jul 17 2018 22:0	3	Reviewed	No Feedback	Critical
10	Multiple Logon	PRESIDIO_USER:	Jul 17 2018 21:0	2	Reviewed	No Feedback	Critical
11	Non-Standard I	4769_user122	Jul 17 2018 21:0	1	Reviewed	No Feedback	Critical
12							

Voir les mesures NetWitness UEBA dans Intégrité

RSA NetWitness UEBA envoie les mesures à l'onglet Navigateur de statistiques système **ADMIN** > **Intégrité**. En plus des informations de base sur l'utilisation du système, les mesures spécifiques aux utilisateurs, les alertes et événements de NetWitness UEBA sont fournies.

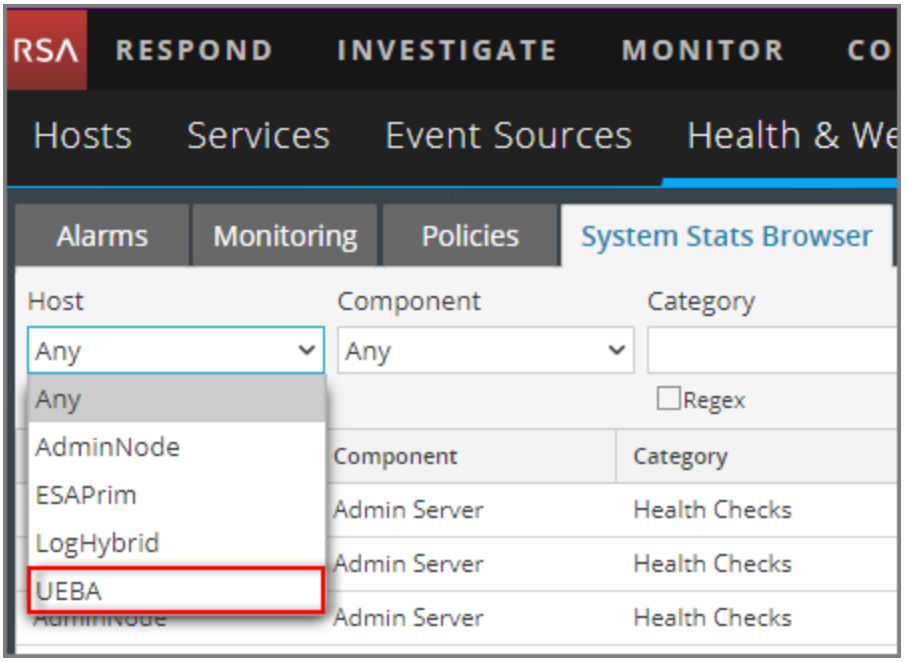
Les analystes peuvent utiliser ces métriques de la manière suivante :

- Confirmer que la licence actuellement acquise est conforme à leurs contrats de licence, et combien par jour.
- Déterminer si le système fonctionne comme prévu.
- Surveiller activement les nouveaux événements.
- Surveiller la création de nouveaux indicateurs et alertes.

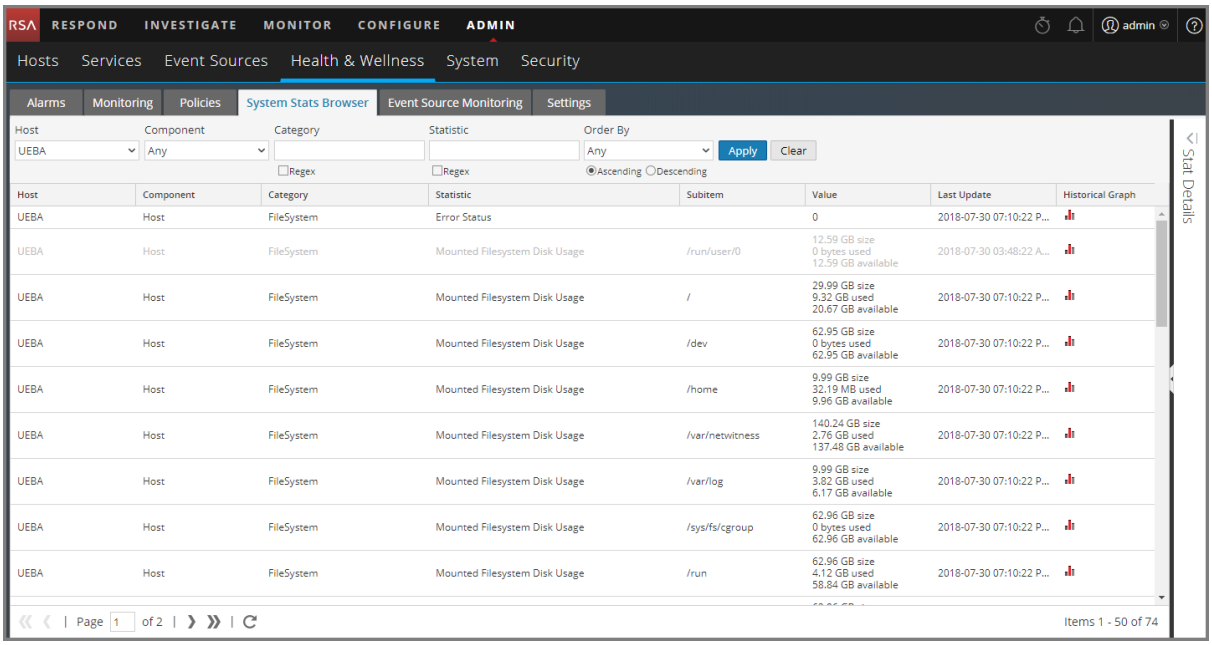
Si ces mesures critiques sont signalées comme « 0 », cela peut indiquer un dysfonctionnement du système.

Pour afficher les mesures NetWitness UEBA dans le navigateur de statistiques système dans Intégrité :

1. Connectez-vous NetWitness Platform et accédez à **ADMIN** > **Santé et bien être**.
2. Cliquez sur l'onglet Navigateur Stat. système.
   Le Navigateur Stat. système s'affiche.
3. Sous Hôte, sélectionnez **UEBA**, puis cliquez sur **Appliquer**.

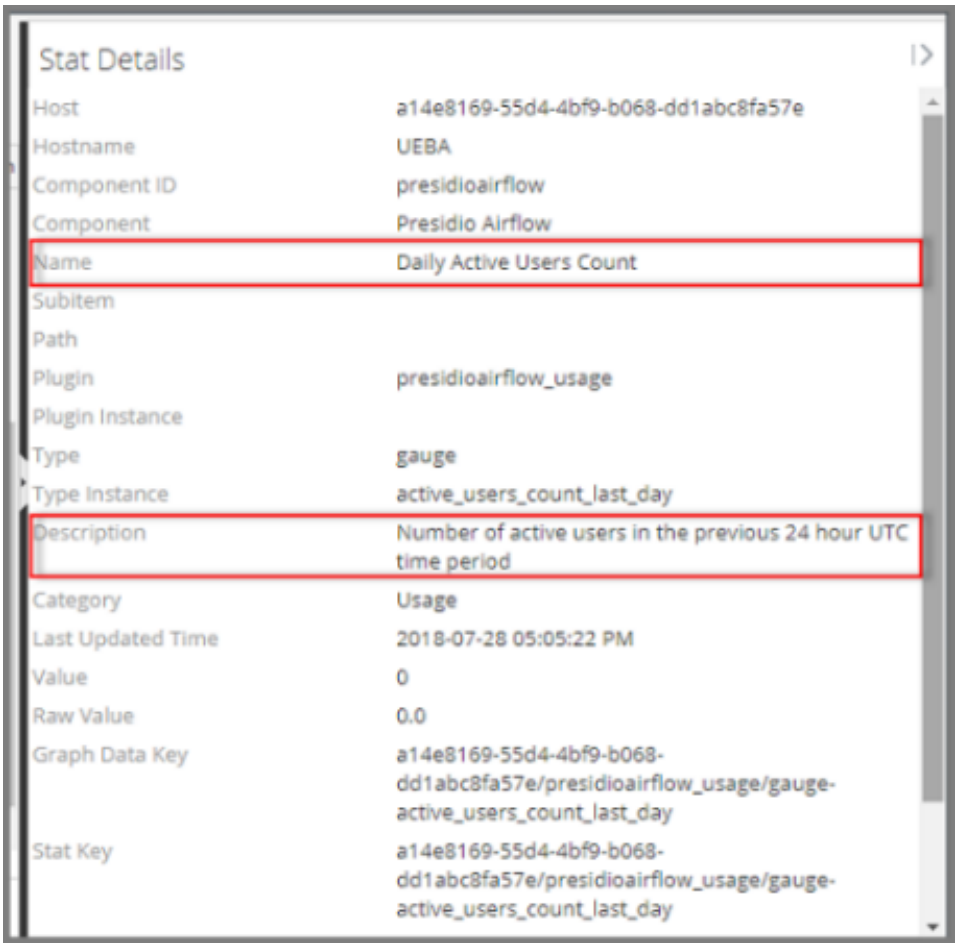


Les résultats de NetWitness UEBA sont affichés.



4. Pour afficher les détails d'une statistique, **cliquez sur** Détails sur les statistiques.

Les détails sur les statistiques sont affichés.



Les champs **Nom** et **Description** fournissent un résumé des mesures affichées.

Pour plus d'informations sur Intégrité et sur l'onglet Navigateur de statistiques système, consultez la rubrique « Surveiller les statistiques système » dans le *du système» dans le Guide de maintenance du système.*. Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

Référence

Cette section fournit des informations sur l'interface utilisateur RSA NetWitness UEBA.

Onglet Overview

L'onglet **Vue d'ensemble** fournit une vue initiale sur les activités utilisateur récentes et les plus importantes dans l'environnement. Chaque panneau indique soit des incidents prioritaires pour l'enquête, soit des mesures consolidées reflétant les risques potentiels pour l'entreprise.

Workflow

Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Documentation
Analyste UEBA	Afficher les cinq principaux utilisateurs à haut risque*.	Identifier les utilisateurs à haut risque
Analyste UEBA	Afficher les utilisateurs, les utilisateurs de liste et les utilisateurs admin à risque*.	Identifier les utilisateurs à haut risque
Analyste UEBA	Afficher l'utilisateur en fonction du type d'alerte et de l'indicateur.	Identifier les utilisateurs à haut risque
Analyste UEBA	Examiner les alertes dans mon environnement.	Enquêter sur les alertes principales
Analyste UEBA	Commencer une enquête sur les alertes critiques	Enquêter sur les alertes principales
Analyste UEBA	Trier les alertes pour concentrer mon enquête.	Filtrer les alertes
Analyste UEBA	Enquêter sur les indicateurs de menace.	Enquêter sur les indicateurs
Analyste UEBA	Exporter les données d'alerte	Gérer les alertes principales

*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

- Commencer une investigation sur les utilisateurs à haut risque
- Enquêter sur les alertes principales
- Filtrer les alertes
- Gérer les alertes principales

Aperçu rapide

La figure ci-dessous présente l'onglet Vue d'ensemble.

Pour accéder à cette vue, accédez à **ENQUÊTER** > **Utilisateurs**.

L'onglet Vue d'ensemble comprend les panneaux suivants :

1. Panneau Utilisateurs à haut risque
2. Panneau Alertes principales
3. Panneau Tous les utilisateurs
4. Panneau Gravité des alertes

Panneau Utilisateurs à haut risque

Le panneau Utilisateurs à haut risque répertorie les cinq principaux utilisateurs à haut risque ainsi que le score de l'utilisateur.

Le tableau ci-dessous décrit les éléments du panneau des utilisateurs à rique élevé.

Nom	Description
Nom d'utilisateur	Nom de l'utilisateur.

Nom	Description
Score utilisateur	Le score d'utilisateur de l'utilisateur, avec la couleur indiquant la gravité du score. Le rouge signifie critique, l'orange indique un risque élevé, le jaune un risque moyen et le vert un risque faible.

Panneau Alertes principales

Le panneau Alertes principales affiche une liste d'alertes pour l'utilisateur, la gravité, la date de création d'alerte et le nombre d'indicateurs associés. La liste se compose des dix principales alertes survenues au cours des 7 derniers jours.

Le tableau suivant décrit les principaux éléments du panneau d'alerte.

Nom	Description
Icône de gravité	L'icône de gravité de l'alerte. Les options sont Critique, Élevée, Moyenne et Faible.
Nom de l'alerte	Nom de l'alerte.
Date de création d'alerte	Date à laquelle une alerte est générée.
Nombre d'indicateurs	Le nombre d'indicateurs associés à l'alerte.

Panneau Tous les utilisateurs

Le panneau Tous les utilisateurs affiche le nombre d'utilisateurs présents dans chacun des groupes prédéfinis NetWitness UEBA.

Le tableau ci-dessous décrit les éléments du panneau d'utilisateurs

Groupe	Description
C'est risqué	Tous les utilisateurs dont le score de risque est supérieur à 0.
Surveillé	Tous les utilisateurs qui sont actuellement marqués comme étant sous surveillance.
Administrateur	Tous les utilisateurs qui ont été précédemment marqués comme Admin.

Panneau Gravité des alertes

Le panneau Gravité des alertes affiche graphiquement le nombre d'alertes, par niveau de gravité, générées au cours de la dernière année.

Le tableau suivant décrit les éléments du panneau Gravité des alertes.

Nom	Description
Last Year	Nombre d'alertes générées au cours de l'année dernière.

Nom	Description
Niveau de gravité	La criticité est également désignée par un code couleur où le rouge signifie critique, l'orange indique un risque élevé, le jaune un risque moyen et le vert un risque faible. Par exemple : 

Onglet Utilisateurs

L'onglet **Utilisateurs** est une console de chasse aux menaces proactive. Vous pouvez utiliser des filtres comportementaux pour créer des listes cibles pilotées par cas d'utilisation et pour surveiller en permanence l'environnement afin de détecter des modèles de comportement à risque spécifiques.

Workflow

Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Documentation
Analyste UEBA	Afficher tous les utilisateurs à haut risque*.	Identifier les utilisateurs à haut risque
Analyste UEBA	Afficher l'utilisateur en fonction du type d'alerte et de l'indicateur*.	Identifier les utilisateurs à haut risque
Analyste UEBA	Commencer une investigation sur les utilisateurs à haut risque	Commencer une investigation sur les utilisateurs à haut risque
Analyste UEBA	Prendre des mesures sur les utilisateurs à haut risque	Prendre des mesures sur les utilisateurs à haut risque
Analyste UEBA	Exporter des utilisateurs à haut risque*.	Exporter des utilisateurs à haut risque
Analyste UEBA	Commencer une enquête sur les alertes critiques	Enquêter sur les alertes principales
Analyste UEBA	Enquêter sur les indicateurs de menace.	Enquêter sur les indicateurs

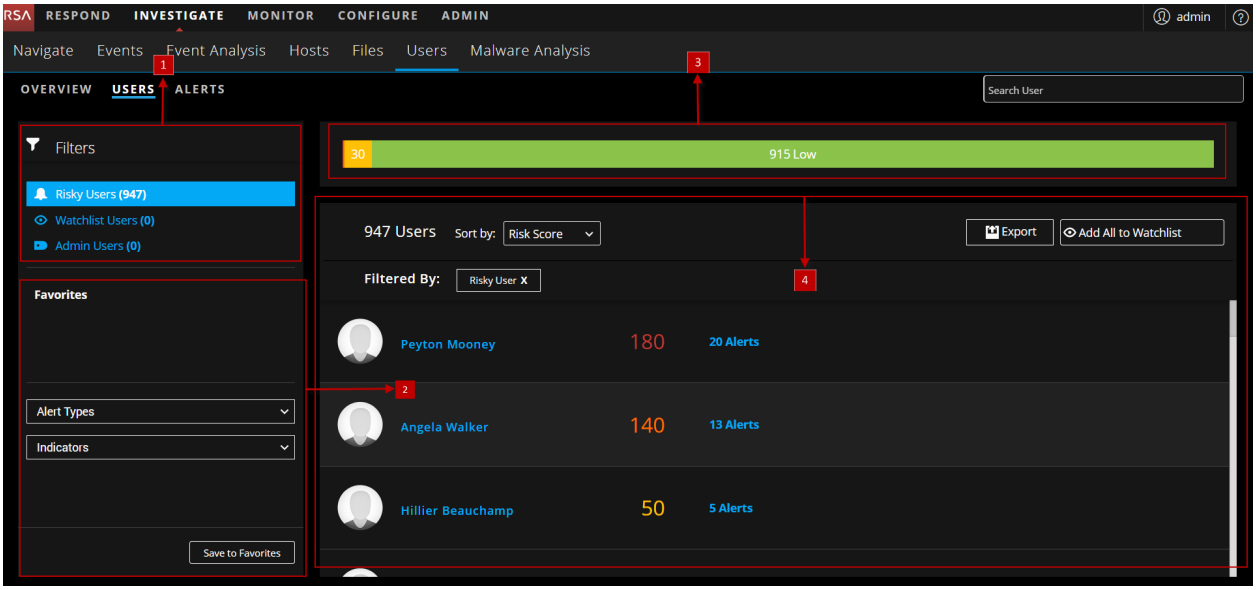
*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

- Commencer une investigation sur les utilisateurs à haut risque
- Enquêter sur les alertes principales
- Filtrer les alertes
- Enquêter sur les indicateurs
- Exporter des utilisateurs à haut risque

Aperçu rapide

La figure suivante montre l'onglet Utilisateurs.



Pour accéder à cette vue :

1. Accédez à **ENQUÊTER** > **Utilisateurs**.

   L'onglet Tour d'horizon s’affiche.

2. Cliquez sur **Utilisateurs**.

Cet onglet Utilisateurs comprend les panneaux suivants :

1	Panneau Filtres
2	Panneau Favoris
3	Panneau d’indicateur de risque
4	Volet Liste d'utilisateurs

Filtre du panneau Filtres

Le panneau Filtres répertorie trois filtres prédéfinis, avec le nombre d'utilisateurs associés entre parenthèses.

Le tableau suivant décrit les types de filtre.

Type de filtre	Description
Utilisateurs à risque	Tous les utilisateurs ayant un score de risque supérieur à 0.
Utilisateurs de la liste de surveillance	Tous les utilisateurs qui sont actuellement marqués comme surveillés.
Utilisateurs administrateurs	Tous les utilisateurs qui ont été précédemment marqués comme Admin.

Panneau Favoris

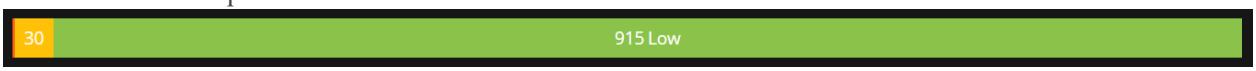
Le panneau Favoris affiche la liste des profils comportementaux enregistrés en tant que favoris.

Le tableau suivant présente les différents types de filtres de profil comportementaux.

Filtres	Description
Types d'alertes	Tous les types d'alerte existants qui décrivent les cas d'utilisation distincts pris en charge (par exemple, tentative de force brute, utilisateur espion, modification anormale AD, exfiltration des données).
Indicateurs	Toutes les fonctions comportementales existantes modélisées par NetWitness UEBA. Vous pouvez utiliser ce filtre pour cibler des alertes associées à une source de données ou une application spécifique.

Panneau d'indicateur de risque

L'indicateur de risque fournit une ventilation basée sur la sévérité des utilisateurs cibles.



Le tableau suivant décrit les éléments du panneau de l'indicateur de risque.

Couleur	Gravité
Rouge	Critique
orange	Élevé
Jaune	Medium
Vert	Low

Volet Liste d'utilisateurs

Le panneau Liste d'utilisateurs affiche la liste de tous les utilisateurs de votre environnement, ainsi que la note d'utilisateur et le nombre total d'alertes associées aux utilisateurs.

Le tableau ci-dessous décrit les éléments de la liste d'utilisateurs.

Données utilisateur	Description
Nom d'utilisateur	Nom de l'utilisateur.
Score	Le score utilisateur de l'utilisateur
Nombre d'alertes	Nombre total d'alertes générées pour l'utilisateur.
Trier par	Le menu déroulant Trier par vous permet de sélectionner la méthode de tri de la liste. Les options sont les suivantes : Score de risque, nom, alertes.
Exportation	Exporter une liste de tous les utilisateurs et leurs notes dans un format de fichier. csv.
Tout ajouter à la liste de surveillance	Ajoute tous les utilisateurs dans la vue filtrée à la liste de surveillance.
Utilisateur de la recherche	Recherche un nom d'utilisateur que vous avez saisi pour le sélectionner dans la liste correspondant à votre entrée.

Onglet Alertes

L'onglet Alertes affiche des détails sur toutes les alertes de votre environnement. Vous pouvez afficher des informations approfondies sur l'activité suspecte survenue dans votre environnement selon une période spécifique.

Workflow

Que voulez-vous faire ?

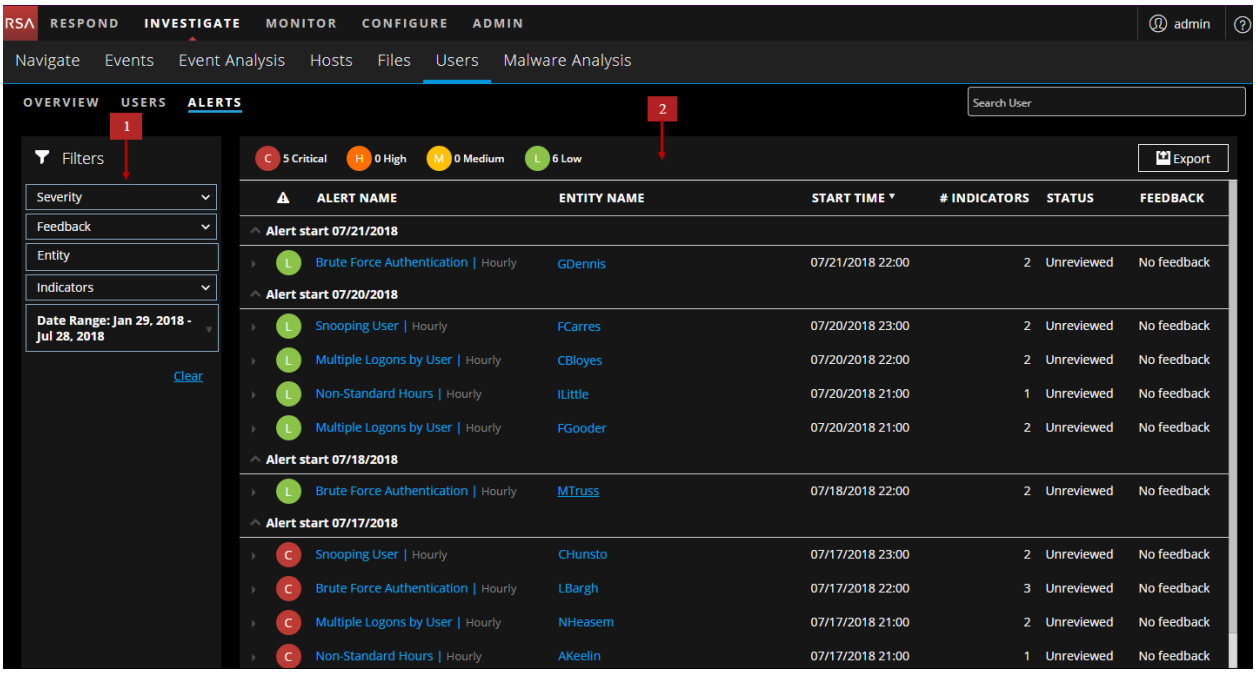
Rôle d'utilisateur	Je souhaite...	Documentation
Analyste UEBA	Examiner les alertes dans mon environnement*.	Enquêter sur les alertes principales
Analyste UEBA	Trier les alertes pour concentrer mon enquête *.	Filtrer les alertes
Analyste UEBA	Enquêter sur les incidents selon des indicateurs de menace*.	Enquêter sur les indicateurs
Analyste UEBA	Partager les données d'alerte au format tableur.	Gérer les alertes principales
Analyste UEBA	Consulter rapidement un récapitulatif des alertes utilisateur.	Afficher les récapitulatifs des alertes

*Vous pouvez effectuer ces tâches ici.

Rubriques connexes

- Enquêter sur les alertes principales
- Filtrer les alertes
- Enquêter sur les indicateurs
- Gérer les alertes principales

Aperçu rapide



Pour accéder à cette vue :

1. Accédez à **ENQUÊTER** > **Utilisateurs**.

   L'onglet Tour d'horizon s’affiche.

2. Cliquez sur **Alertes**.

L’onglet Alertes comprend les panneaux suivants :

1 Panneau Filtres
2 Panneau Alerts

Panneau Filtres

Utilisez le panneau Filtres pour affiner votre recherche d'alertes. Les filtres sont automatiquement appliqués lorsque vous effectuez vos sélections. Vous pouvez effacer tous les filtres actuellement définis en cliquant sur **Effacer**.

Le tableau suivant présente les différents types de filtres.

Filter Name	Description	Options
Gravité	Filtre la liste des alertes pour inclure des alertes associées à un ou plusieurs niveaux de gravité.	Critique, Élevé, Moyen ou Faible.
Commentaires	Filtre la liste des alertes pour inclure des alertes associées à un ou plusieurs types de commentaires.	Sélectionnez tout, Aucune rétroaction ou Aucun risque.

Filter Name	Description	Options
Entity	Filtre la liste des alertes pour inclure uniquement des alertes associées à un nom d'utilisateur spécifique.	NA.
Indicateurs	Filtre la liste des alertes pour inclure des alertes associées à un ou plusieurs indicateurs.	Exemples d'indicateurs : • Active Directory - Temps d'ouverture de session anormal • Authentification - Connecté sur plusieurs ordinateurs • Plusieurs échecs d'accès aux fichiers
Période	Filtre la liste des alertes pour inclure les alertes créées pendant une plage de temps spécifique.	La semaine dernière, le mois dernier ou une plage spécifiée

Panneau Alertes

Le panneau des alertes affiche les informations suivantes pour chaque alerte :

- Icône de gravité : Une icône à côté du nom de l'alerte qui indique le niveau de gravité de l'alerte
- Nom de l'alerte Le nom de l'alerte et la période d'alerte
- Nom de l'entité Nom de l'entité (compte d'utilisateur) ayant généré l'alerte
- Heure de début : Date et heure de la première détection de cette alerte
- Indicateurs : Le nombre d'anomalies de comportement uniques (indicateurs) associées à l'alerte
- État : Indique si l'alerte a été marquée comme Non examinée ou Sans risque
- Commentaires Indique si une valeur de rétroaction a été affectée à l'alerte

Au début de chaque ligne d'alerte se trouve une icône qui développe l'alerte pour afficher des détails supplémentaires. Une fois développée, les champs suivants sont affichés :

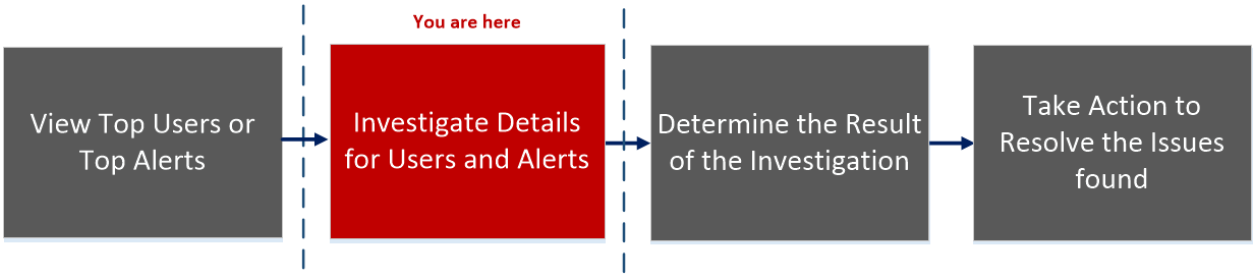
- Nom de l'indicateur – Le nom de chaque indicateur unique associé à l'alerte
- Valeur de l'anomalie – La valeur de l'indicateur, représentant le montant ou la valeur de déviation car il diffère du comportement normal de l'utilisateur
- Source de données – Le type de données où l'indicateur a été trouvé
- Heure de début – La date et l'heure de la première détection de cet indicateur
- # d'événements – Le nombre d'événements dans l'indicateur

Les données actuellement affichées dans le volet central peuvent être exportées vers un fichier. csv en cliquant sur Exporter en haut à droite du volet.

Vue du profil d'utilisateur

La vue **Profil d'utilisateur** fournit des informations détaillées sur toutes les alertes et les indicateurs associés d'un utilisateur.

Workflow



Que voulez-vous faire ?

Rôle d'utilisateur	Je souhaite...	Documentation
Analyste UEBA	Afficher les utilisateurs à haut risque	Identifier les utilisateurs à haut risque
Analyste UEBA	Commencer une investigation sur les utilisateurs à haut risque*	Commencer une investigation sur les utilisateurs à haut risque
Analyste UEBA	Prendre des mesures sur les utilisateurs à haut risque	Prendre des mesures sur les utilisateurs à haut risque
Analyste UEBA	Exporter des utilisateurs à haut risque	Exporter des utilisateurs à haut risque
Analyste UEBA	Commencer une enquête sur les alertes critiques*	Enquêter sur les alertes principales
Analyste UEBA	Enquêter sur les indicateurs de menace	Enquêter sur les indicateurs

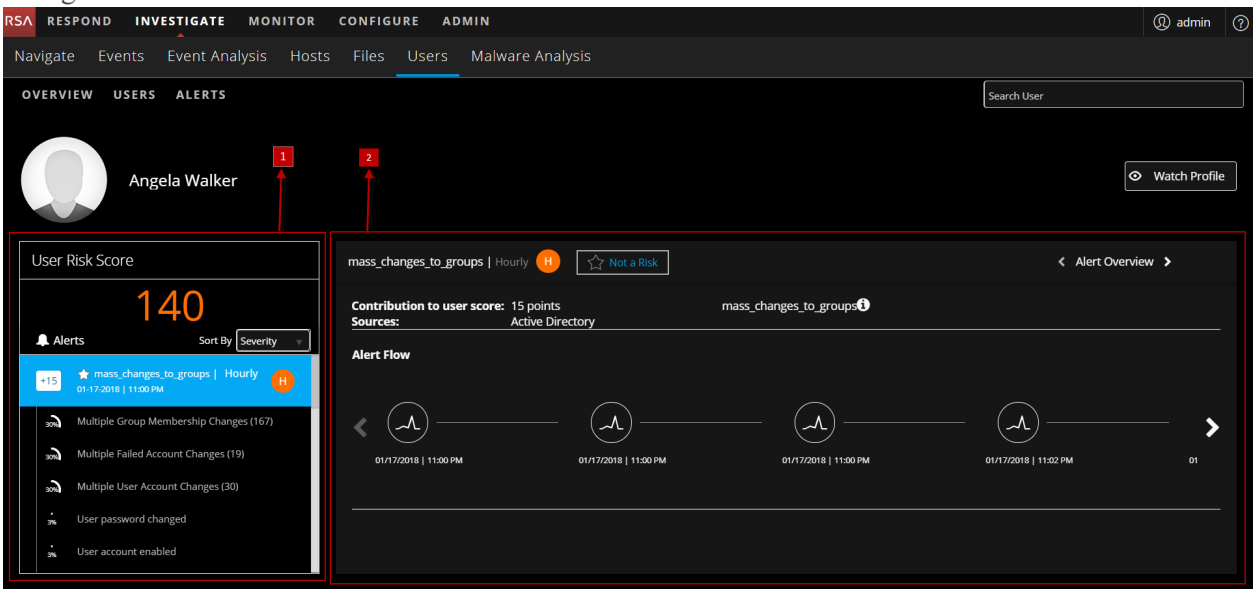
*Vous pouvez effectuer ces tâches ici.

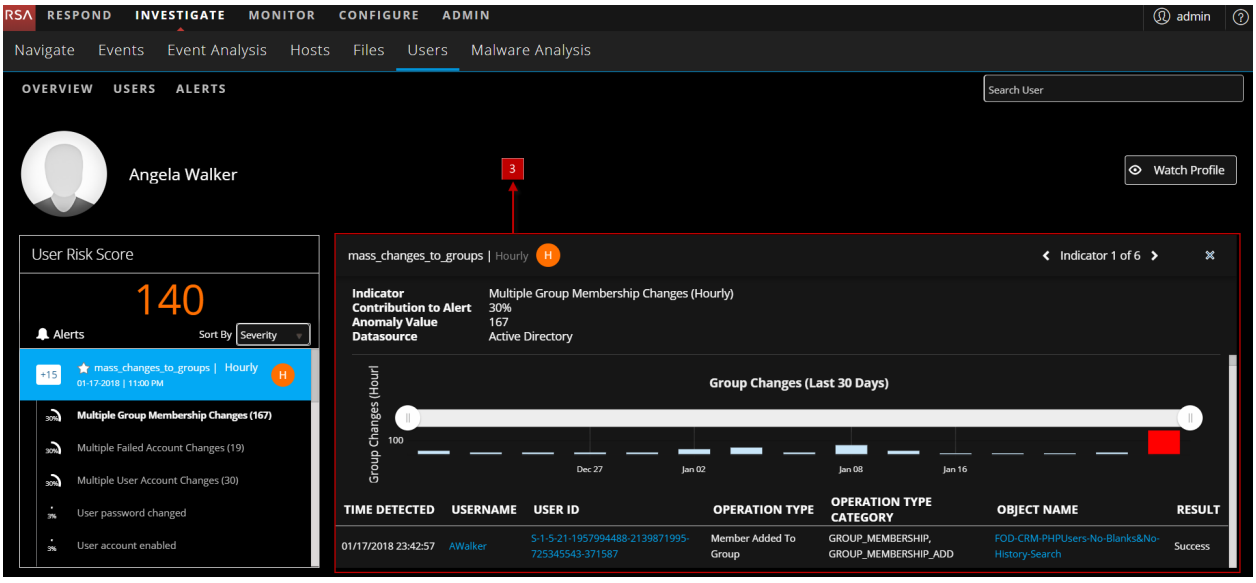
Rubriques connexes

- Commencer une investigation sur les utilisateurs à haut risque
- Enquêter sur les alertes principales
- Filtrer les alertes
- Enquêter sur les indicateurs
- Exporter des utilisateurs à haut risque

Aperçu rapide

La figure ci-dessous montre la vue Profil d'utilisateur.





Pour accéder à cette vue :

1. Accédez à **ENQUÊTER** > **utilisateurs**. Effectuez l'une des opérations suivantes :
   a. Dans l'onglet **TOUR D'HORIZON**, sous le volet **Utilisateurs à risque élevé**, sélectionnez un utilisateur, puis cliquez sur le nom d'utilisateur ou sa note utilisateur.
   b. Sous l'onglet **UTILISATEURS**, sélectionnez un utilisateur, puis cliquez sur le nom d'utilisateur.
   c. Dans l'onglet **ALERTES**, sélectionnez un nom d'alerte ou un nom d'entité.

Le profil des utilisateurs se compose des panneaux suivants :

1 Panneau Score de risque utilisateur
2 Panneau Flux d'alertes
3 Panneau Indicateurs

Panneau Score de risque utilisateur

Le panneau Score de risque utilisateur contient les informations suivantes :

Nom	Description
Score utilisateur	Le score utilisateur de l'utilisateur mis en surbrillance en fonction de la gravité.
Alertes	Les informations suivantes s'affichent : • Les noms de l'alerte • L'icône de niveau de gravité • La date et heure de début de l'alerte. • Le délai de l'alerte (horaire ou journalier) • Le score de risque de l'alerte (+20) • Une liste des noms d'indicateurs d'alerte et le nombre de fois où les événements d'indicateur se sont produits.
Trier par	Les alertes sont triées en fonction de la gravité et de la date. Par défaut, elles sont est triées par gravité.

Panneau Flux des alertes

Le panneau Flux des alertes affiche les informations suivantes :

Nom	Description
Nom de l'alerte	Nom de l'alerte.
Période	Le délai de l'alerte (horaire ou journalier)
Niveau de gravité	La gravité de l'alerte.

Nom	Description
Contribution au score utilisateur	La contribution à la valeur de score de l'utilisateur (par exemple, + 20)
Sources	Les sources de données pour l'alerte (par exemple Active Directory).
Graphique chronologique	La chronologie des événements liés à la formation de l'alerte.

Panneau Indicateurs

Cliquez sur une icône de graphique dans le panneau Flux d'alertes pour ouvrir le panneau Indicateur. Le tableau suivant décrit les éléments du panneau de l'indicateur :

Nom	Description
Indicateur	Le nom de l'indicateur avec la période de l'indicateur entre parenthèses. Par exemple, les modifications de l'appartenance à plusieurs groupes (toutes les heures).
La contribution à Alerte	Pourcentage de contribution d'alerte.
Valeur de l'anomalie	La valeur Anomalie.
dataSource	Source de données où l'alerte est déclenchée.
Moment détecté	La date et l'heure de déclenchement d'un indicateur.
Nom d'utilisateur	Nom de l'utilisateur pour lequel un indicateur est déclenché.
User ID	ID utilisateur de l'utilisateur pour lequel un indicateur est déclenché.
Type d'opération	L'action réalisée par l'utilisateur. Par exemple, Membre ajouté au groupe.
Type de la catégorie d'opération	Le type de la catégorie d'opération Par exemple, GROUP_MEMBERSHIP.
Résultat	L'état de l'action réalisée par l'utilisateur.

Annexe : Stratégie d'audit Windows de NetWitness UEBA

Afin d'obtenir le maximum d'avantages de RSA NetWitness UEBA, RSA vous recommande d'implémenter les stratégies d'audit Windows décrites ici.

Pour un ensemble de stratégies de base à auditer, reportez-vous à la section « Recommandations des paramètres d'audit pour Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 et Windows Server 2008 » de cet article de Microsoft : Recommandations de la stratégie d'audit.

Les stratégies sous « recommandation renforcée » sont requises, ainsi que les stratégies suivantes, pour s'assurer que tous les événements d'authentification et Active Directory requis sont soumis à l'audit :

- Partage de fichiers d'audit détaillé
- Partage de fichiers d'audit
- Système de fichiers d'audit

RSA vous recommande d'activer l'audit pour les réussites et les échecs.

Les événements Windows suivants doivent être vérifiés :

Pour les modèles d'authentification :

4624	4625	4769

Pour les modèles AD :

4670	4717	4720	4722	4723	4724	4725	4726
4727	4728	4729	4730	4731	4732	4733	4734
4735	4737	4738	4739	4740	4741	4742	4743
4754	4755	4756	4757	4758	4764	4767	4794
5136	5376	5377					

Pour les modèles d'accès aux fichiers :

4660	4663	4670	5145