RSA NETWITNESS® UEBA

FONCTIONNALITÉS PRINCIPALES :

- *Apprentissage automatique basé sur le comportement, à la fois non surveillé, récurrent et breveté*
- *Collecte de données native*
- *Système innovant de pondération des fonctionnalités*
- *Moteur simplifié de notation des risques*
- *Étendue des cas d'utilisation*
- *Visualisation du contexte d'identité*
- *Algorithmes automatisés de réduction des faux positifs*

PRINCIPAUX AVANTAGES :

- *Réduction du MTTD et du MTTI*
- *Accélération de la réponse aux incidents*
- *Moins de faux positifs*
- *Enrichissement du contexte basé sur l'identité*
- *Identification rapide des utilisateurs risqués*

Meilleure lutte contre les menaces destructrices en constante évolution, sur tous les terrains.

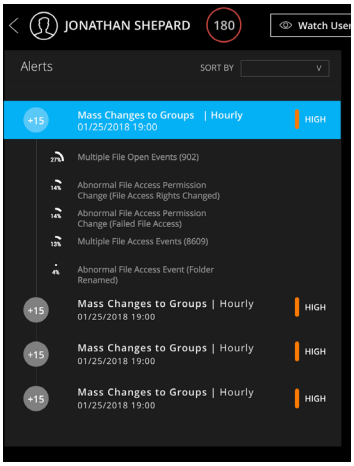
DÉTECTION PLUS RAPIDE DES MENACES. RÉDUCTION DU TEMPS D'IMPLANTATION. AUTOMATISATION DE LA RÉPONSE.

À l'heure où les surfaces d'attaque se multiplient, il est devenu de plus en plus complexe de se protéger contre les attaquants, qu'il s'agisse de logiciels malveillants courants, de menaces et de logiciels criminels provenant de personnel interne jusqu'aux attaques parrainées par l'état, ou encore d'attaques d'hacktivistes et de terroristes. Toutes les menaces ne naissent pas égales, pourtant des silos de technologies non connectées pour la prévention, la surveillance et l'investigation restent inefficaces pour permettre aux centres d'opérations de sécurité (SOC, Security Operations Centers) d'éliminer rapidement les faux positifs et de fournir des indicateurs ciblés (par opposition aux alertes cloisonnées libres). Ce qu'il faut, c'est une solution complète et collaborative permettant aux analystes de la sécurité de détecter et de répondre aux menaces réellement importantes pour leur organisation.

RSA NetWitness® UEBA est une solution d'analytique du comportest une solution spécialement conçue pour l'analytique du comportement des utilisateurs et des entités, **axée sur le Big Data** et intégrée en tant que partie centrale de RSA NetWitness Platform. En tirant parti des algorithmes d'apprentissage automatique non surveillés pour de nombreux cas d'utilisation, la solution RSA NetWitness UEBA fournit une détection complète des menaces inconnues basée sur le comportement, sans nécessiter de réglages de la part d'un analyste. La solution RSA NetWitness UEBA augmente la capacité de votre équipe de sécurité existante grâce à une détection rapide et des renseignements exploitables à chaque étape du cycle de vie de l'attaque. RSA NetWitness UEBA est un élément clé de RSA NetWitness Platform et vous aide à découvrir le cycle de vie complet des attaques et à résoudre les violations.

DÉTECTION DES MENACES SUR TOUS LES TERRAINS

RSA NetWitness UEBA optimise les fonctionnalités de détection des menaces, automatisées et clé en main, proposées par RSA NetWitness Platform. Les analystes de la sécurité mettent les attaquants (internes ou externes) hors d'état de nuire via des alertes claires et ciblées. Ils tirent parti des fonctionnalités natives clés de capture réseau de RSA NetWitness Platform, mais aussi de la collecte de journaux, de la visibilité sur les points de terminaison et d'un enrichissement unifié des métadonnées à la vitesse de l'apprentissage automatique. La solution RSA NetWitness UEBA exploite l'intelligence artificielle et l'approche mathématique supérieure de l'apprentissage automatique pour établir des références en matière d'utilisateurs, de groupes d'utilisateurs, d'entités et de comportements à l'échelle de l'organisation, ce qui permet de dissocier les activités normales et bénignes des écarts malveillants pour une réponse aux incidents à la fois juste et exploitable.



DES RÉPONSES PRÉCISES

La solution RSA NetWitness UEBA aide les analystes de la sécurité à identifier les sources de compromis et les activités de données isolées suspectes via une visualisation chronologique basée sur les identités, en mettant en évidence les indicateurs suspects alignés sur le cadre MITRE ATT&CK™, pour une réponse aux incidents plus efficace et plus complète.

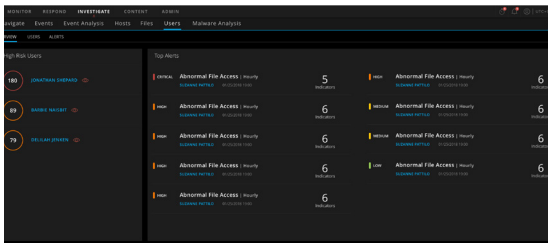
RSA

EXEMPLES D'UTILISATION DE UEBA :

- *Menace interne*
- *Attaque par force brute*
- *Usurpation de compte*
- *Compromission de compte*
- *Utilisation erronée et abusive de comptes dotés de privilèges*
- *Privilèges élevés*
- *Utilisateur espion (snooping)*
- *Exfiltration de données*
- *Accès anormal au système*
- *Mouvement latéral*
- *Activité malveillante*
- *Comportement suspect*

La solution RSA NetWitness UEBA vous fait bénéficier de son intelligence supérieure dès son activation : elle révèle les comportements anormaux de manière rapide et précise sans exiger constamment votre attention pour peaufiner les réglages.

DÉTECTION PUISSANTE ET AUTOMATISÉE



La surveillance automatisée et continue accélère le temps de détection des utilisateurs internes malveillants et des cybercriminels qui utilisent des comptes corrompus, sans règles, signatures ou analyses manuelles. La solution RSA NetWitness UEBA est dotée de modèles de science de données puissants pour renforcer la capacité des organisations à détecter des outils, techniques et processus (TTP, Tools, Techniques and Processes) inédits, et fournit des enquêtes de bout en bout qui permettent aux analystes de passer des résultats de l'analytique brute à l'approche de risques globale de leur organisation.

En tirant profit d'une architecture technologique évolutive de Big Data, la solution RSA NetWitness UEBA offre un puissant moteur de détection des menaces capable de révéler des événements indépendants comme étant des activités anormales et des menaces utilisateur jusque-là inconnues, le tout dans une interface utilisateur unique.

UEBA : L'ANALYTIQUE CLÉ DE LA PLATE-FORME

Des alertes ciblées, exploitables et contextuelles attirent l'attention sur les comportements d'utilisateurs potentiellement synonymes d'activité suspecte. Au final, ce sont des outils puissants pour les analystes de la sécurité. RSA NetWitness Platform propose une analytique adaptative du comportement des utilisateurs et des entités qui peut fonctionner avec la même agilité et rapidité que les menaces en constante évolution. RSA NetWitness Platform est capable de capturer des données de journaux sans surveillance afin de permettre aux analystes de la sécurité de démasquer les pirates, en tirant profit d'algorithmes de détection dynamiques et non déterministes, de l'élaboration de référentiels, de la modélisation des comportements et de l'analytique des groupes de pairs.

RSA NetWitness UEBA et UEBA Essentials révèlent des événements dont la priorité est plus élevée, corrélés en temps réel grâce aux événements de journaux, au trafic réseau et à la visibilité sur les points de terminaison pour permettre aux équipes SOC de réduire le temps moyen de détection (MTTD, Mean Time To Detect) et le temps moyen d'investigation (MTTI, Mean Time To Investigate), diminuer la lassitude face aux alertes et les faux positifs, et proposer des prévisions et une analytique prédictive plus précise.

RSA NETWITNESS PLATFORM

Avec plus de 30 ans d'expertise en matière de sécurité, RSA continue à diriger le marché à l'aide de solutions innovantes qui répondent aux défis les plus importants des opérations de sécurité dans le monde entier. Le nouveau produit RSA NetWitness UEBA complète RSA NetWitness Platform et ses offres avancées en termes de SIEM et de défense contre les menaces, et tire profit de sa visibilité généralisée sur les journaux, le réseau et les points de terminaison.

Consultez notre site web RSA.com/fr-fr/Domore pour connaître toutes les dernières intégrations, études de cas et meilleures pratiques.

09/20 Fiche produit H17297-1 W386667.