CAS D'UTILISATION RSA NETWITNESS® UEBA

DÉTECTION PUISSANTE DES MENACES BASÉES SUR L'UTILISATEUR

RSA NetWitness UEBA est 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 de la détection non surveillée des anomalies statistiques et de l'apprentissage automatique, RSA NetWitness UEBA propose une détection complète et basée sur les comportements des menaces inconnues afin de répondre à un large éventail de cas d'utilisation. 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.

Lors de l'évaluation des solutions d'analytique du comportement des utilisateurs et des entités (UEBA, User and Entity Behavior Analytics) recherchez les fonctionnalités et capacités stratégiques suivantes :

- Détection et surveillance des menaces entièrement automatisées et continues
- Visibilité sur le cycle de vie complet des attaques en tirant profit de la collecte de données, de la détection, de l'investigation et de la réponse
- Indicateurs de langage naturel alignés sur le cadre MITRE ATT&CK™
- Apprentissage automatique non supervisé avec un modèle de science des données clé en main qui ne nécessite aucun réglage
- Un agent de point de terminaison qui est au cœur de la plate-forme et qui associe la collecte de journaux à la détection des points de terminaison et à la réponse

FONCTIONNALITÉS DE BASE DE L'ANALYTIQUE UEBA DE NIVEAU ENTREPRISE

COLLECTE DE DONNÉES NATIVE

De nombreuses équipes SOC sont confrontées à la gestion de la collecte, du stockage et de l'analyse de tous les journaux produits dans différents formats par les nombreux systèmes de leur entreprise, sur site et dans le Cloud. La solution RSA NetWitness UEBA répond à ce défi en recueillant des données de journaux brutes à partir de ces systèmes, en analysant dynamiquement les activités générées par les personnes et les processus à partir d'un large éventail de sources, et en interprétant les informations de sécurité pertinentes à partir de ces sources de données.

TAXONOMIE UNIFIÉE DES MÉTADONNÉES

Pour qu'une solution UEBA fonctionne de manière optimale, les données de journal, de trafic réseau et de points de terminaison qui l'alimentent doivent être analysées, normalisées et transformées au moment de la capture dans une taxonomie unifiée et cohérente des métadonnées. Étant donné que la solution RSA NetWitness UEBA est un composant central de l'approche SIEM avancée de RSA NetWitness Platform, cela se produit automatiquement.

DÉTECTION À LA VITESSE DE L'APPRENTISSAGE AUTOMATIQUE

Trop souvent, les indicateurs de menaces provenant de solutions de sécurité ad-hoc ne peuvent pas être utilisés de manière fiable ou cohérente pour identifier une attaque, car la plupart du temps, ces activités prises séparément ne font pas partie d'une attaque et leur signalement sous forme d'alerte pourrait rapidement noyer les analystes dans un océan de fausses alertes. La solution RSA NetWitness UEBA génère des alertes beaucoup plus ciblées et exploitables que les solutions de sécurité ad-hoc, car elle examine les schémas d'activité et de comportement au fil du temps, utilise l'apprentissage automatique pour identifier les écarts par rapport aux comportements de référence et apprend à partir d'alertes passées qui ont été signalées comme faux positifs.

POURQUOI L'ANALYTIQUE UEBA EST-ELLE DEVENUE UNE EXIGENCE CLÉ DE SÉCURITÉ ?

- 28 % des violations signalées proviennent d'acteurs internes : UEBA permet de détecter plus facilement ce type de menaces
- Les principaux acteurs internes provoquant des violations signalées sont les administrateurs système et les utilisateurs finaux
- Dans 68 % des cas, il a fallu deux mois ou plus pour découvrir les failles de sécurité : UEBA aide les équipes de sécurité à détecter les menaces plus rapidement
- Les principales actions des violations signalées sont le vol d'informations d'identification et l'utilisation abusive/privilégiée : ce sont des activités que l'analytique UEBA est conçue pour signaler

Rapport d'enquête Verizon 2018 sur la violation de données.

EN SAVOIR PLUS

Visitez RSA.com/DoMore ou planifiez une démonstration

RSA

6 CAS D'UTILISATION QUE RSA NETWITNESS UEBA EST CONÇU POUR DÉTECTER

ACTIONS/MODIFICATIONS ANORMALES

Si un pirate bénéficie d'un accès privilégié à un domaine Active Directory (AD) ou à un contrôleur de domaine, il peut tirer parti de cet accès pour contrôler ou même détruire l'intégralité de la forêt AD. S'il compromet ne serait-ce qu'un seul contrôleur de domaine, toutes les modifications apportées à ce contrôleur peuvent être répliquées sur tous les autres systèmes. RSA NetWitness UEBA aide les analystes à détecter ces types de scénarios en identifiant les pics du volume d'actions des utilisateurs par rapport à un domaine AD qui peut indiquer qu'un compte est compromis et/ou utilisé pour corrompre ou détruire les données stratégiques de répertoire.

ACCÈS ANORMAL D'UTILISATEURS PRIVILÉGIÉS

La solution RSA NetWitness UEBA vous aide à identifier les cas dans lesquels un utilisateur privilégié peut présenter une menace interne. Par exemple, si un technicien du centre d'assistance s'éloigne des processus normaux et des politiques de sécurité établies pour configurer des mots de passe sans date d'expiration pour les nouveaux utilisateurs, RSA NetWitness UEBA le détecte.

SURVEILLANCE DE TYPE « SNOOPING »

La surveillance de type « snooping » fait référence à l'accès non autorisé aux données d'une autre personne ou entreprise. Il peut s'agir d'un utilisateur interne ou d'un pirate externe qui tente de parcourir les serveurs et les emplacements de dossiers auxquels il n'est pas autorisé à accéder, généralement dans le but de localiser et d'obtenir des informations importantes sur l'entreprise. Le snooping sophistiqué exploite des programmes personnalisés qui surveillent à distance l'activité sur un ordinateur ou effectuent une détection automatisée des fichiers.

La solution RSA NetWitness UEBA peut détecter le snooping de plusieurs manières : Elle capture les tentatives d'accès (échecs et réussites) d'utilisateurs à des données auxquelles ils n'ont pas le droit d'accéder. Lorsque la solution identifie un nombre anormalement élevé de tentatives d'accès (réussies ou non) à des fichiers d'un nouvel emplacement, et ce dans un court laps de temps, elle déclenche une alerte.

AUTHENTIFICATION PAR FORCE BRUTE

Les solutions UEBA sophistiquées peuvent distinguer une véritable attaque par force brute d'un échec d'authentification bénin en examinant les authentifications défaillantes dans le contexte d'activités utilisateur anormales. RSA NetWitness UEBA ne déclenche des alertes que lorsqu'il détecte d'autres schémas de comportement suspects en plus d'échecs d'authentification répétés. Cela permet d'éliminer les faux positifs associés aux configurations réseau défectueuses ou aux utilisateurs tâtonnant pour retrouver leurs mots de passe.

ACTIVITÉS RÉALISÉES PAR DES MACHINES

RSA NetWitness UEBA peut détecter lorsqu'un programme malveillant tente d'accéder à des ressources d'entreprise restreintes à l'aide d'informations d'identification corrompues. Le profilage des utilisateurs peut révéler des signes d'une attaque par force brute, tandis que le profilage des entités peut montrer un pic significatif dans le comportement d'entités suspectes. Par exemple, il peut s'agir d'un nombre excessif d'activités sur des centaines de comptes à partir d'un seul appareil ou d'une seule adresse IP, ou d'une quantité considérable de fichiers renommés sur plusieurs ordinateurs à partir d'une seule machine sur laquelle le programme malveillant est installé.

PRIVILÈGES ÉLEVÉS

Les pirates tentent de tirer parti d'utilisateurs moyens de l'organisation qui sont souvent une cible plus facile, plutôt que de s'octroyer des privilèges élevés pour exploiter davantage le réseau. Il est essentiel de surveiller étroitement les activités des utilisateurs privilégiés, les accès accordés, les groupes sensibles, etc. pour lutter contre les informations d'identification corrompues. Cependant, du fait que les utilisateurs privilégiés ne suivent pas toujours un schéma défini de comportement « normal », les faux positifs sont inévitables. Par conséquent, l'identification, la collecte et l'analyse d'une accumulation d'indicateurs sont essentielles pour localiser les personnes malveillantes.

Ainsi, lorsqu'un utilisateur avec des privilèges élevés se connecte à partir d'un emplacement atypique après plusieurs tentatives d'authentification défaillantes, puis crée de nouveaux comptes utilisateur avec des privilèges élevés, le risque apparaît comme élevé dans la liste des alertes principales.

Avant d'ajouter une nouvelle solution ad-hoc (dans ce cas, UEBA) à votre pile d'outils de sécurité, demandez-vous si elle va vraiment ajouter de la valeur ou simplement créer plus d'interférences. L'avantage de la solution RSA NetWitness UEBA est qu'elle détecte les anomalies critiques basées sur les utilisateurs en plus des menaces traditionnelles, le tout au sein d'une seule et même plate-forme.

09/20 Cas d'utilisation, H17457-1 W386667