FICHE TECHNIQUE

One Identity Safeguard for Privileged Analytics

Détectez et évitez les violations de sécurité liées aux accès à privilèges

Avantages

- Suivi et visualisation des activités des utilisateurs afin d'offrir des informations sur ce qui se passe au sein de votre système informatique.
- Authentification continue par le biais d'analyses constantes des frappes et des mouvements de la souris.
- Identification des déviations inhabituelles de l'activité de référence avec l'apprentissage automatique.
- Réduction du délai de détection d'un incident de sécurité avec des informations contextuelles et la hiérarchisation en fonction des risques des sessions enregistrées.
- Réduction des alertes de sécurité parasites pour que vous puissiez vous concentrer sur l'essentiel.
- Amélioration de la sécurité avec la fermeture des connexions lorsqu'une alerte est lancée sur une activité potentiellement nuisible.

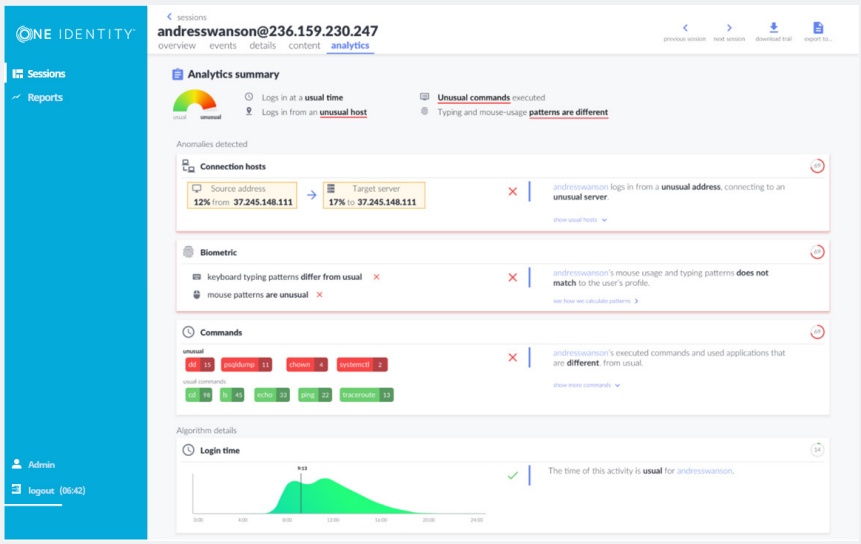
Présentation

En tant que responsable de la sécurité informatique, vous savez que votre entreprise n'est pas à l'abri d'une violation de compte à privilèges. Aujourd'hui, il faut 206 jours aux entreprises[1] pour détecter une violation. Et le temps, c'est de l'argent… Et des risques. Ainsi, que la violation émane d'un compte à privilèges piraté ou d'un administrateur malveillant, plus le délai de détection est long, plus les infiltrés auront de temps pour trouver et voler les données. Ceci augmente également le montant des amendes et des dépenses en analyses forensiques.

Vous avez sûrement dû fournir des accès privilégiés à des utilisateurs autres que vos administrateurs de confiance. Vous avez peut-être ajouté des administrateurs provenant de prestataires externes qui peuvent être basés partout dans le monde. Comment vous assurer que les administrateurs dotés d'un accès à privilèges n'utilisent pas ce dernier pour vous nuire ?

Avec One Identity Safeguard for Privileged Analytics, vous connaissez les utilisateurs à risque, vous gardez un œil sur les menaces internes et externes et vous pouvez détecter les comportements inhabituels des utilisateurs à privilèges. Cette solution puissante vous offre une visibilité complète sur vos utilisateurs à privilèges et leurs activités, et en cas de problème vous pouvez agir immédiatement et être en bonne position pour éviter le vol de données.

[1]Institut Ponemon, Cost of Data Breach Study (Enquête sur le coût des violations de données en 2017)



Identifiez facilement les utilisateurs et les comportements à risque

Détectez rapidement si l'activité d'un utilisateur est inhabituelle et potentiellement risquée avec l'écran de résumé des analyses. Il contient un résumé des commandes inhabituelles, l'activité biométrique et les hôtes de connexion.

Fonctionnalités

Détection en temps réel de nouvelles menaces

La sécurité basée sur les règles ne peut pas détecter de nouvelles méthodes d'attaque ni les utilisateurs internes malveillants. Safeguard for Privileged Analytics suit et visualise en temps réel l'activité des utilisateurs afin de fournir une meilleure compréhension de ce qui se passe réellement dans votre environnement informatique. Il ne nécessite aucune règle de corrélation prédéfinie, il fonctionne simplement avec les données de sessions.

Fonctionnement sans schéma

Au lieu d'utiliser un modèle de correspondance des schémas (qui sont souvent erronés) pour détecter les comportements malveillants connus ; Safeguard for Privileged Analytics utilise les données recueillies dans votre environnement informatique. Il crée une référence de comportement dit « normal » et détecte les déviations en utilisant divers algorithmes d'apprentissage automatique.

Analyse du contenu de l'écran

En analysant le contenu de l'écran des sessions à privilèges, les commandes émises et les titres des fenêtres, Safeguard for Privileged Analytics peut enrichir le profil de comportement de référence de vos utilisateurs à privilèges des commandes et applications utilisées régulièrement. Cette analyse détaillée facilite l'identification des comportements types et peut aider à détecter le vol des identités à privilèges.

Biométrie du comportement

Chaque utilisateur présente un schéma comportemental caractéristique, même lorsqu'il s'agit d'actions communes à tous les utilisateurs, comme la saisie au clavier ou le déplacement de la souris. Les algorithmes intégrés à Safeguard for Privileged Analytics examinent les caractéristiques comportementales capturées par Safeguard for Privileged Sessions. L'analyse des schémas de frappe et des déplacements de la souris vous aident non seulement à identifier les violations, mais permettent également d'assurer une authentification biométrique continue.

Réduction des alertes parasites

La solution réduit les alertes parasites générées par les SIEM en catégorisant les événements utilisateurs en fonction du niveau de risque et de déviation et en mettant en avant les événements suspects. Les alertes peuvent être envoyées aux SIEM ou vos analystes de la sécurité peuvent consulter une liste des événements classés en ordre de priorité ce qui leur permet de se concentrer sur les événements les plus importants.

Réponse automatisée

Dans la plupart des scénarios d'attaques, les événements à grand impact sont souvent précédés d'une phase de reconnaissance. Ainsi, la détection et la réaction pendant cette phase sont cruciales pour éviter toute activité préjudiciable. L'intégration fluide avec Safeguard for Privileged Sessions autorise la fermeture automatisée de session dès qu'un événement suspect a lieu ou qu'un comportement malveillant est détecté.

L'approche One Identity de la gestion des accès à privilèges

La gamme One Identity comprend l'ensemble le plus complet de solutions de gestion des accès à privilèges. Vous pouvez tirer parti des fonctionnalités de One Identity Safeguard for Privileged Analytics avec des solutions conçues pour la gestion des sessions et mots de passe, la délégation granulaire des comptes root UNIX et administrateur Active Directory ; des extensions pour que les commandes sudo open source répondent aux besoins des entreprises ; et l'enregistrement des frappes pour les activités root UNIX. Toutes ces fonctions sont étroitement intégrées avec la solution de pont Active Directory leader du marché.

À propos de One Identity

One Identity aide les entreprises à assurer une gestion réussie des accès et des identités. Grâce à notre combinaison unique d'offres, incluant la gestion des identités, gestion des accès, gestion des accès à privilèges, et des solutions d'identité « as a service », les entreprises peuvent atteindre leur plein potentiel sans être entravées par la sécurité tout en étant protégées contre les menaces. En savoir plus sur le site OneIdentity.com

© 2019 One Identity LLC. TOUS DROITS RÉSERVÉS. One Identity et le logo One Identity sont des marques et des marques déposées de One Identity LLC aux États-Unis et dans d'autres pays. Pour obtenir la liste complète des marques déposées One Identity visitez notre site Web https://www.oneidentity.com/fr-fr/legal/. Toutes les autres marques, marques de service, marques déposées et marques de service déposées appartiennent à leurs propriétaires respectifs.
Datasheet_2019_PAM-Privileged-Analytics_US_RS_41021