Informatica

Documentation de solution

Étude de cas : Analyse comportementale pour SaaS Enterprise

Principaux bénéfices

- Activer les processus métiers avec une gestion d'accès rapide et agile
- Augmenter l'assurance de l'accès des données sensibles (comment et qui accède aux données)
- Supprimer l'incertitude autour de la menace interne et le compromis des informations d'identification
- Concentrer les efforts de réponse et de gouvernance sur la réponse aux menaces réelles

Améliorez la rapidité et la flexibilité de l'entreprise tout en augmentant l'assurance.

Sur le marché concurrentiel d'aujourd'hui, la rapidité, la flexibilité, l'accès à l'information et les données fiables pour accélérer la prise de décision peuvent faire la différence en matière de réussite d'une entreprise face à la concurrence. Le modèle d'engagement de sécurité traditionnel est axé sur l'implémentation de systèmes sécurisés qui répondent aux exigences métiers. Toutefois, les itérations rapides de demande du marché après une mise en service s'étendent même aux équipes de sécurité les plus agiles et créent des tensions entre la sécurité et l'activité.

Comment une équipe de sécurité peut-elle alors réussir à suivre le rythme de l'évolution naturelle de l'activité tout en s'alignant sur le principe de privilège et d'objectif moindre du contrôle d'accès basé sur les rôles (RBAC) ?

Avec Informatica Secure@Source User Behavioral Analytics (UBA), les modèles de conformité d'accès utilisés depuis longtemps par les administrateurs informatiques peuvent être appliqués et fourniront aux propriétaires de données des informations et la garantie de la façon dont leurs données sont utilisées et par qui elles sont utilisées. Associé aux alertes et à la réponse, UBA permet aux gestionnaires et aux propriétaires de données de gérer et d'atténuer les risques inhérents aux abus de privilèges et aux compromis d'identifiants.

UBA utilise des modèles familiers des équipes de conformité et d'audit. Ainsi, il permet même aux environnements hautement réglementés de bénéficier d'un accès rapide aux informations nécessaires pour rester concurrentiel sans impact négatif sur la posture de l'assurance.

Quantifier précisément votre risque à partir des utilisateurs autorisés

Situation et opportunité

Quand le rythme de l'évolution est soutenu, les préoccupations liées à la sécurité et l'accès peuvent ralentir le taux de changement et entraver l'habilitation de l'activité. Cela peut inciter l'entreprise à adopter des solutions de contournement et mener des activités de gestion et d'analyse de données à l'extérieur du système de contrôle principal.

Le développement du contrôle d'accès qui en résulte est très difficile à gérer, empêche de comprendre qui a accès à quels ensembles de données, et rend la détection d'abus/d'utilisation abusive impossible. La compréhension de l'utilisation des processus métiers et de l'exposition des données est fondamentale pour améliorer les contrôles sans interrompre les transactions commerciales.

La confluence des exigences métiers en matière de vitesse et d'agilité, les exigences réglementaires en matière de certitude sur l'accès aux données et les besoins de position conservatrice des moteurs de conformité créent une opportunité en termes de capacités, qui peuvent fournir une garantie sur les données auxquelles les utilisateurs ont accès, ainsi que sur la façon dont ils les utilisent.

Approche et solution

Nous avons constaté qu'UBA fournissait suffisamment de garantie sur l'accès aux données sans nuire à la rapidité et la souplesse de l'entreprise. Dans notre exemple en interne, nous avons d'abord examiné quelques processus métiers clés et suivi l'ensemble de données lors de son déplacement de la source d'autorité en aval à travers l'analyse et la pile de rapports. Évaluer l'activité à travers le domaine de données plutôt que dans une seule application fournit un contexte plus important sur les activités de l'ensemble des données et une meilleure garantie sur les limites d'utilisation des données. Nous n'avions pas défini les scénarios d'accès utilisateur à l'avance. Au lieu de cela, nous avions conservé la garantie et la transparence grâce à la surveillance des actions de l'utilisateur facilitées par les capacités de création de rapports et de détection d'anomalies.

La détection et les alertes seules ne peuvent pas réduire les risques sans une action rapide des utilisateurs, des propriétaires de données et de la gestion. Il est fondamental que les propriétaires de données et les responsables d'équipe reviennent tôt dans la boucle. Ils doivent assumer la responsabilité des résultats des risques quant à l'accès à leurs données. La meilleure façon d'y parvenir est de démontrer le risque (ou risque potentiel) du point de vue des données. Dans la plupart des cas, les propriétaires et les responsables de données n'ont pas d'informations faciles à utiliser dans l'accès aux données et les habitudes d'utilisation. Une boucle de rétroaction impliquant les utilisateurs, le service de gestion et les propriétaires de données souligne les habitudes d'utilisation et les comportements acceptables, et encourage l'adoption de modèles responsables.

Il existe de nombreuses similitudes entre ce modèle et le modèle d'accès « bris de glace » généralement utilisé par les administrateurs de systèmes sensibles qui ont besoin d'enfreindre la répartition des contrôles de responsabilité pendant la maintenance et le dépannage. L'administrateur possède des autorisations suffisantes pour accomplir les fonctions du rôle. Un accès élevé déclenche un examen pour s'assurer que toutes les mesures ont été autorisées. L'apprentissage de la machine permet à ce modèle, reconnu par les auditeurs comme adéquat, de s'adapter et de couvrir l'entreprise.

Un programme réussi doit d'abord se concentrer sur l'optimisation du modèle de réponse axé sur l'action pour répondre aux comportements et anomalies de l'utilisateur. Il se développe ensuite pour couvrir les processus métiers critiques qui nécessitent la vitesse/flexibilité ou présentent un risque significatif pour les objectifs de l'entreprise.

Conclusion

Les capacités d'apprentissage de la machine de Secure@Source offrent un niveau d'assurance inaccessible par une révision manuelle, et le résultat est un alignement plus étroit entre autorisations d'accès et utilisation des données.

UBA s'intègre naturellement aux modèles de propriété des données pour établir un moteur formel et encourager les propriétaires à gérer et protéger leurs données. Par le biais de programmes de sensibilisation, formation ciblée et correction de processus, UBA peut conduire à des améliorations et des changements, afin de s'assurer que l'entreprise respecte les objectifs de conformité pendant une phase de croissance rapide.

UBA n'étant pas lié à une application ou plate-forme spécifique, il peut être utilisé dans les applications pour protéger un écosystème complet de données au lieu de se concentrer uniquement sur un système source et de laisser les systèmes de rapports à découvert.

L'UBA Secure@Source d'Informatica prend en charge la rapidité et la flexibilité de l'entreprise, ainsi que les objectifs de sécurité et de conformité, impliquant le propriétaire et la gestion des données dans le processus de réponse.

À propos d'Informatica

Informatica se concentre à 100 % sur les données, car ce sont les données qui font tourner le monde. Les entreprises ont besoin de solutions de données pour le Cloud, les Big Data, le temps réel et les flux de données en continu. Informatica est le premier fournisseur mondial de solutions de gestion de données, que ce soit dans le Cloud, sur site ou dans les environnements hybrides. Plus de 7 000 entreprises du monde entier font appel aux solutions de données d'Informatica.

Informatica

Siège mondial, 2100 Seaport Blvd, Redwood City, CA 94063, États-Unis Téléphone : +33 1 42 04 89 00 (France)
www.informatica.com/fr linkedin.com/company/informatica twitter.com/InformaticaFr

IN17_0617_3339