Informatica

Solution Brief

Case study: Analytics comporta-mentali per SaaS di livello enterprise

Vantaggi principali

- Rendere possibili i processi di business con una gestione degli accessi rapida e agile
- Aumentare la garanzia di sicurezza su come e chi ha eseguito l'accesso ai dati sensibili
- Eliminare le incertezze relative a minacce interne e compromissione delle credenziali
- Focalizzare le iniziative di risposta e governance sulla risposta alle minacce reali

Garantisci agilità e velocità di business aumentando la sicurezza.

In un mercato competitivo come quello attuale, la velocità, l'agilità, l'accesso alle informazioni e i dati affidabili con cui prendere rapidamente decisioni possono fare la differenza tra un'azienda di successo e una che soccombe alla concorrenza. Il modello tradizionale di engagement in ambito sicurezza si focalizza sull'implementazione di sistemi sicuri in linea con i requisiti di business. Le rapide iterazioni della domanda del mercato dopo un go-live, tuttavia, sono imponenti anche per i team di sicurezza più agili e creano tensioni tra sicurezza e business.

Come può, quindi, un team di sicurezza tenere efficacemente il passo con il naturale cambiamento aziendale mantenendo al tempo stesso l'allineamento con la regola del privilegio minimo e l'obiettivo del controllo degli accessi basato sui ruoli (RBAC)?

Con la funzionalità Informatica Secure@Source User Behavioral Analytics (UBA), è possibile applicare modelli di conformità degli accessi da tempo utilizzati dagli amministratori IT, che offriranno ai data owner informazioni necessarie e affidabili su come e da chi vengono utilizzati i loro dati. Integrata con avvisi e risposte, UBA consente ai data manager e ai data owner di gestire e ridurre i rischi intrinseci di compromissione delle credenziali e abuso dei privilegi.

Grazie all'utilizzo di modelli ben noti ai team addetti ad audit e conformità, UBA consente anche agli ambienti altamente regolamentati di beneficiare di un accesso rapido alle informazioni necessarie per restare competitivi, senza impatti negativi sulla posizione relativa alla garanzia di sicurezza.

Quantifica in modo preciso i rischi legati agli utenti autorizzati

La situazione e l'opportunità

Se il cambiamento aziendale è rapido, i problemi relativi a sicurezza e accessi possono rallentare il ritmo del cambiamento e ostacolare l'operatività di business. Questo può portare l'azienda ad adottare scorciatoie e a condurre attività di gestione dei dati/analytics al di fuori del sistema di controllo primario.

Il conseguente ampliamento del controllo degli accessi è molto difficile da gestire, impedisce di vedere chi ha accesso a quali insiemi di dati e rende impossibile rilevare gli utilizzi impropri o non autorizzati. Comprendere come i processi di business utilizzano ed espongono i dati è fondamentale per migliorare i controlli senza interrompere le transazioni aziendali.

La confluenza dei requisiti di business in termini di velocità e agilità, requisiti normativi riguardanti la certezza sull'accesso ai dati e necessità di una posizione conservativa per i responsabili della conformità apre la strada a funzionalità in grado di garantire la sicurezza non solo su quali dati sono accessibili agli utenti, ma anche su che cosa gli utenti fanno con i dati.

Informazioni su Informatica

La Digital Transformation sta cambiando il mondo. Quale leader nell'enterprise cloud data management, possiamo aiutarti a guidare il tuo processo di trasformazione. Ti offriamo una prospettiva che ti consentirà di implementare una struttura più agile, realizzare nuove opportunità di crescita o persino inventare nuove cose. Ti invitiamo a scoprire tutto quello che Informatica ha da offrirti e a liberare "the power of data" per promuovere la tua prossima intelligent disruption. Non solo una volta, ma più e più volte.

L'approccio e la soluzione

Abbiamo scoperto che UBA offre la necessaria garanzia di sicurezza sull'accesso ai dati mantenendo al tempo stesso la velocità e la flessibilità del business. Nel nostro esempio di situazione in-house, abbiamo innanzitutto analizzato alcuni processi di business e seguito l'insieme di dati nel suo spostamento da una fonte autorevole downstream attraverso lo stack di analytics e reporting. Valutando l'attività in tutto il dominio di dati anziché esclusivamente in un'applicazione, si ottiene un contesto più ampio delle attività dell'insieme di dati e una maggiore garanzia di sicurezza sui limiti di utilizzo dei dati. Non abbiamo definito in anticipo scenari di accesso degli utenti. Al contrario, abbiamo mantenuto la garanzia di sicurezza e la responsabilità attraverso la supervisione delle azioni degli utenti, facilitata dalle funzionalità di rilevamento e reporting delle anomalie.

Il rilevamento e gli avvisi di per sé non possono ridurre il rischio senza una rapida azione da parte di utenti, data owner e management. Occorre coinvolgere da subito i data owner e i team manager. Queste figure devono assumersi la responsabilità dei risultati del rischio di accesso ai loro dati, un obiettivo che si raggiunge al meglio dimostrando il rischio (o il rischio potenziale) da un punto di vista legato ai dati. Nella maggior parte dei casi, data owner e manager non dispongono di approfondimenti di facile impiego sui pattern di accesso e utilizzo dei dati. Un ciclo di feedback che coinvolge utenti, management e data owner mette in evidenza i modelli di utilizzo e i comportamenti accettabili e incoraggia l'adozione di pattern responsabili.

Esistono molte analogie tra questo modello e il modello di accesso "break glass" utilizzato dagli amministratori dei sistemi sensibili, che devono violare i controlli sulla separazione delle funzioni per la manutenzione e la risoluzione di problemi. L'amministratore dispone delle opportune autorizzazioni per svolgere le funzioni del ruolo. Un accesso elevato attiva una revisione, per garantire che tutte le azioni eseguite fossero autorizzate. L'utilizzo del machine learning consente a questo modello, riconosciuto come adeguato dagli auditor, di scalare e coprire tutta l'organizzazione.

Un programma di successo dovrebbe innanzitutto focalizzarsi sull'ottimizzazione del modello di risposta orientata all'azione per rispondere a comportamenti degli utenti e anomalie. Quindi, dovrebbe venire esteso per coprire i processi di business fondamentali che richiedono velocità/agilità o rappresentano un rischio significativo per gli obiettivi dell'organizzazione.

Conclusione

Le funzionalità di machine learning di Secure@Source offrono un livello di garanzia di sicurezza impossibile da ottenere con la revisione manuale e il risultato è un allineamento più rigoroso tra autorizzazioni di accesso e utilizzo dei dati.

UBA si integra in modo naturale con i modelli di data ownership, definendo un fattore formale e incoraggiando gli owner a gestire e proteggere i propri dati. Attraverso programmi di awareness, formazione mirata e correzione dei processi, UBA può portare a miglioramenti e modifiche dei processi per mantenere l'organizzazione in linea con gli obiettivi di compliance durante una rapida crescita.

Poiché UBA non è legato a un'applicazione o piattaforma specifica, può essere utilizzato in tutte le applicazioni per proteggere un intero ecosistema di dati, anziché focalizzarsi unicamente su un sistema sorgente e lasciare scoperti i sistemi di reporting.

Secure@Source UBA di Informatica supporta la velocità e l'agilità del business, nonché gli obiettivi di sicurezza e conformità coinvolgendo i data owner e il management nel processo di risposta.

Informatica

Piazza della Repubblica 14/16 - 20124 Milano, Italia Tel: +39 02 37 05 80 00 | Via Luca Gaurico 9/11 - 00143 Roma, Italia Tel: +39 06 54 83 21 34
informatica.com/it linkedin.com/company/informatica twitter.com/InformaticaITA

IN17_0617_3339