사례 연구: 엔터프라이즈 SaaS를 위한 행동 분석

핵심 이점

- 신속하고 민첩한 액세스 관리를 통한 비즈니스 프로세스 지원
- 민감한 데이터에 누가 어떻게 액세스하는지에 대한 확신을 높임
- 내부 위협 및 자격 증명 손상과 관련한 불확실성 제거
- 실제 위협에 대응할 때 대응 및 거버넌스 노력에 집중

확신을 높이는 동시에 비즈니스 민첩성 및 속도 실현

오늘날과 같이 경쟁이 치열한 시장에서 신속한 의사 결정을 지원하는 속도, 민첩성, 정보에 대한 액세스, 신뢰할 수 있는 데이터는 기업의 성공 혹은 경쟁에서의 실패를 결정짓는 차이가 될 수 있습니다. 기존 보안 참여 모델은 비즈니스 요구 사항을 충족하는 안전한 시스템을 구현하는 데 중점을 두고 있습니다. 그러나 개시 후 시장의 요구가 빠르게 반복되면 가장 민첩한 보안 팀조차도 부담이 될 수 있으며, 보안 부서와 현업 부서 사이에 긴장감이 형성되게 됩니다.

그렇다면 보안 팀은 어떻게 해야 필연적인 비즈니스 변화를 성공적으로 따라잡으면서, 최소 권한의 원칙과 RBAC(역할 기반 액세스 제어)의 목표에 계속해서 부합할 수 있을까요?

Informatica Secure@Source UBA(사용자 행동 분석) 기능을 사용하면 IT 관리자가 오랜 기간 사용한 액세스 규정 준수 모델을 적용할 수 있습니다. 이 기능은 데이터 소유자에게 데이터가 어떻게 사용되고 있고 누가 데이터를 사용하고 있는지에 대한 통찰력과 확신을 제공합니다. UBA는 경고 및 대응과 함께 데이터 관리자와 소유자가 자격 증명 손상 및 권한 남용의 내재된 위험을 관리하고 완화할 수 있게 해줍니다.

감사 및 규정 준수 팀에 친숙한 모델을 사용하므로 UBA는 규제가 심한 환경에서도 경쟁 우위를 유지하는 데 필요한 정보에 신속하게 액세스하는 이점을 활용할 수 있으며, 이때 데이터에 대한 확신에 부정적인 영향을 주지 않습니다.

권한 있는 사용자의 위험을 정확하게 수치화

상황 및 기회

비즈니스 변화가 빠르게 진행될 때 보안 및 액세스에 대한 우려 때문에 변화 속도가 늦어지고 비즈니스 지원이 방해될 수 있습니다. 이로 인해 기업은 주요 제어 시스템 외부에서 해결책을 도입하고 데이터 관리/분석 활동을 수행하는 방법을 찾게 될 수 있습니다.

그러면 액세스 제어가 무분별하게 확산되어 관리하기 매우 어려워지고, 데이터 세트에 누가 액세스하는지 파악하는 데 방해가 되며, 오용/남용 감지가 불가능해집니다. 비즈니스 프로세스에서 데이터를 사용하고 노출하는 방식을 이해하는 것은 비즈니스 거래를 방해하지 않고 제어 기능을 향상하는 데 필수적인 과정입니다.

속도와 민첩성에 대한 비즈니스 요구사항, 데이터 액세스 확실성에 대한 규제 요구사항, 보수적인 입장을 위한 규정 준수 추진 요인의 필요성이 하나로 모이면서, 사용자가 액세스할 수 있는 데이터가 무엇이며 사용자가 데이터로 어떤 작업을 수행하는지를 확실히 알 수 있는 기능에 대한 기회가 드러났습니다.

Informatica 정보

디지털 변혁은 세상을 변화시키고 있습니다. Informatica는 엔터프라이즈 클라우드 데이터 관리의 선두 주자로서 고객이 지능적으로 업계를 선도할 수 있도록 도와드릴 준비가 되어 있습니다. 보다 민첩해지고, 새로운 성장 기회를 깨닫고, 새로운 것을 고안해낼 수 있도록 고객에게 선견지명을 제공해 드립니다. Informatica가 제공하는 모든 서비스에 관해 알아보고 데이터의 힘을 활용하여 미래의 지능형 혁신을 실현하시기 바랍니다. 한 번만이 아니라 반복해서 해보시길 바랍니다.

접근 방식 및 솔루션

Informatica는 UBA가 데이터 액세스에 있어 필요한 확신을 제공하면서 비즈니스 속도 및 민첩성을 유지할 수 있다는 점을 발견했습니다. Informatica 내부에서 예를 찾아 먼저 몇 가지 핵심 비즈니스 프로세스를 검토했으며, 데이터 세트가 분석 및 보고 스택을 통해 권한 있는 소스의 다운스트림에서 이동할 때 이를 추적해 보았습니다. 하나의 애플리케이션에서 독점적으로 평가하는 대신 데이터 도메인 전반에서 활동을 평가하여 데이터 세트 활동의 컨텍스트를 폭넓게 이해하고 데이터의 사용 경계에 있어 더 큰 확신을 얻을 수 있었습니다. 이때 사용자 액세스 시나리오를 미리 정의하지는 않았습니다. 대신, 이상 감지 및 보고 기능을 통해 사용자 행동을 관찰함으로써 확신과 책임 수준을 유지했습니다.

사용자, 데이터 소유자 및 관리자의 신속한 조치 없이 감지 및 경고만으로는 위험을 줄일 수 없습니다. 데이터 소유자 및 팀 관리자를 조기에 개입시켜야 합니다. 이들은 데이터에 액세스하여 발생하는 위험에 대한 소유권을 지녀야 하며, 데이터 관점에서 이러한 위험(또는 잠재적인 위험)을 보여줄 때 가장 좋은 결과를 달성할 수 있습니다. 대부분의 경우 데이터 소유자와 관리자는 데이터 액세스 및 사용 패턴에 있어 준비된 통찰력을 보유하고 있지 않습니다. 사용자, 관리자, 데이터 소유자가 관여하는 피드백 루프는 사용 패턴과 허용 가능한 동작에 대해 점수를 낮게 책정하여 책임에 따른 패턴을 도입하도록 유도합니다.

유지관리 및 문제 해결 동안 업무 분리를 위반해야 하는 민감한 시스템의 관리자가 주로 사용하는 '유리 깨기' 액세스 모델과 이 모델 간에는 많은 유사점이 있습니다. 관리자는 역할의 직무를 완료할 수 있는 적절한 권한을 갖고 있습니다. 향상된 액세스에서는 모든 조치가 승인되었는 확인하는 검토를 시작합니다. 기계 학습을 활용하면 감사자가 적절하다고 판단한 이 모델을 확장하여 조직에 적용할 수 있습니다.

프로그램이 성공하기 위해서는 처음에는 사용자 동작 및 이상에 대응하는 행동 중심적인 반응 모델을 활용하는 데 중점을 두어야 합니다. 그런 다음 속도/민첩성이 요구하거나 조직의 목표에 상당한 위험을 제기하는 중요한 비즈니스 프로세스를 포함하도록 확장해야 합니다.

결론

Secure@Source의 기계 학습 기능은 수동 검토로는 불가능한 수준의 확신을 제공하며 그 결과 액세스 권한과 데이터 사용 간에 더 긴밀한 조정이 가능해집니다.

UBA는 데이터 소유권 모델에 자연스럽게 통합되어 공식적인 동인을 만들고 소유자의 데이터 관리 및 보호를 촉진합니다. 인식 프로그램, 타겟팅된 교육, 프로세스 수정을 통해 UBA는 조직이 빠르게 성장할 때 조직이 규정 준수 목표에 부합하도록 프로세스를 변경하고 수정할 수 있게 해줍니다.

UBA는 특정 애플리케이션이나 플랫폼과 묶여 있지 않으므로, 하나의 소스 시스템에만 집중 사용하고 시스템에는 적용하지 않는 대신, 애플리케이션 전반에서 사용해 전체 데이터 에코시스템을 보호할 수 있습니다.

Informatica의 Secure@Source UBA는 데이터 소유자와 관리 부서를 대응 프로세스에 개입시켜 비즈니스 속도 및 민첩성뿐 아니라 보안 및 규정 준수 목표도 지원합니다.

Informatica

한국인포매티카 06611 서울시 서초구 서초동 강남대로 465 교보타워 B동 13층, 대표 전화: +82 2 6293 5001
미국 내 수신자 부담 번호: 1.800.653.3871 informatica.com/kr linkedin.com/company/informatica twitter.com/InformaticaKR

IN17_0617_3339