TD SYNNEX

Dolandırıcılık Tespiti

Hedef Yapay Zeka: Kullanım Örneği

Giriş

Fraud Detection, finansal hizmetler, sigorta, perakende ve e-ticaret gibi sektörlerdeki dolandırıcılık faaliyetlerini proaktif olarak belirlemek, araştırmak ve azaltmak için gelişmiş yapay zeka ve makine öğrenimi tekniklerinden yararlanır. Yapay zeka sistemleri işlem verilerini, kullanıcı davranışlarını ve geçmiş dolandırıcılık modellerini analiz ederek anormallikleri gerçek zamanlı olarak tespit edebilir ve daha fazla inceleme için şüpheli faaliyetleri işaretleyebilir. Bu yaklaşım sadece tespit sürecini hızlandırmakla kalmaz, aynı zamanda gelişen dolandırıcılık taktiklerine uyum sağlamakta zorlanan geleneksel kural tabanlı sistemlere olan bağımlılığı da azaltır. Kuruluşlar, sürekli olarak yeni verilerden öğrenen dinamik, veri odaklı bir sistemden faydalanarak dolandırıcılık tespit yeteneklerinin ortaya çıkan tehditlere karşı sağlam kalmasını sağlar. Önde gelen tedarikçiler bu girişimleri desteklemek için özel çözümler sunmaktadır. Örneğin, IBM bilişsel bilişimi dolandırıcılık analitiği ile entegre eder; AWS ölçeklenebilir, gerçek zamanlı dolandırıcılık tespit hizmetleri sunar; Microsoft Azure gelişmiş güvenlik analitiği sunar; Google Vertex AI anomali tespiti için büyük ölçekli makine öğreniminden yararlanır; ve HPE Private Cloud AI güvenli, uyumlu şirket içi veya hibrit çözümler sunar. Bu teklifler birlikte, kurumların varlıklarını korumalarını, müşteri güvenini sürdürmelerini ve giderek karmaşıklaşan dijital ortamda mevzuata uygunluğu sağlamalarını destekliyor.

Sıkıntı Noktaları

Geleneksel dolandırıcılık tespit yöntemleri genellikle yavaş ve verimsiz olabilen statik kurallara ve manuel incelemelere dayanır. Kuruluşlar, dolandırıcılık davranışına işaret eden ince anormallikleri belirlemek için büyük hacimli işlem verilerini eleme konusunda önemli zorluklarla karşılaşmaktadır. Bu eski sistemler hızla gelişen dolandırıcılık taktiklerine uyum sağlamakta zorlanmakta, bu da yanıtların gecikmesine ve daha yüksek mali kayıplara neden olmaktadır. Ayrıca, yüksek orandaki yanlış pozitifler güvenlik ekiplerini bunaltarak kaynakları gerçek tehditlerden uzaklaştırabilir ve meşru müşterilere rahatsızlık verebilir. Veri siloları ve farklı sistemler, potansiyel dolandırıcılığın kapsamlı bir görünümünü oluşturma yeteneğini daha da engelleyerek zamanında tespit ve müdahaleyi zorlaştırır. Bu sorunlar toplu olarak riski yükseltir, operasyonel maliyetleri artırır ve müşteri güvenini tehlikeye atar.

Çözümün Faydaları

Yapay zeka odaklı dolandırıcılık tespit çözümlerinin entegre edilmesi, şüpheli faaliyetlerin tanımlanmasını otomatikleştirerek ve gerçek zamanlı müdahaleye olanak sağlayarak dönüştürücü faydalar sunar. Gelişmiş makine öğrenimi algoritmaları, dolandırıcılığa işaret edebilecek kalıpları belirlemek için büyük miktarda işlemsel ve davranışsal veriyi analiz ederek tespit süresini önemli ölçüde azaltır ve mali kayıpları en aza indirir. Yeni verilerden sürekli

öğrenme, zaman içinde doğruluğu artırır, böylece yanlış pozitif oranını düşürür ve güvenlik ekiplerinin yüksek öncelikli tehditlere odaklanmasına olanak tanır. Gelişmiş veri entegrasyonu, işlemlerin bütünsel bir görünümünü sağlayarak daha doğru risk değerlendirmelerini kolaylaştırır. Dahası, otomatik sistemler geniş ölçekte çalışabilir ve en yüksek hacimli ortamların bile güvenli kalmasını sağlar. Bu faydalar, gelişmiş operasyonel verimlilik, daha az riske maruz kalma, gelişmiş yasal uyumluluk ve kuruluşun hassas bilgileri koruma becerisine daha fazla müşteri güveni anlamına gelir.

Etkilenen KPI'lar

Yapay zeka odaklı dolandırıcılık tespitinden olumlu etkilenebilecek temel performans göstergeleri şunlardır:

- Dolandırıcılık Olay Oranı: Başarılı dolandırıcılık işlemlerinde ölçülebilir bir azalma.
- Yanıt Süresi: Potansiyel dolandırıcılık vakalarının daha hızlı tespiti ve çözümü.
- Yanlış Pozitif Oranı: Gereksiz uyarıları ve manuel incelemeleri azaltarak geliştirilmiş doğruluk.
- Mali Kayıplar: Zamanında müdahale ve önleme sayesinde daha az parasal kayıp.
- Müşteri Güveni: Sağlam güvenlik önlemleri sayesinde artan memnuniyet ve güven.

Kullanım Durumunun Uygulanması

Yapay zeka odaklı dolandırıcılık tespitinin uygulanması, teknik inovasyonu operasyonel stratejiyle bütünleştiren kapsamlı ve çok aşamalı bir yaklaşım gerektirir.

Planlama ve Paydaş Uyumu

Hedefleri Tanımlayın: Dolandırıcılık olay oranlarını düşürmek, yanıt sürelerini en aza indirmek ve yanlış pozitifleri azaltmak gibi net hedefler belirleyin. Bu hedefleri ölçülebilir KPI'larla eşleştirin.

Çapraz Fonksiyonlu Bir Ekip Kurun: Tüm gereksinimlerin ele alındığından emin olmak için BT, güvenlik, risk yönetimi, uyumluluk ve operasyonlardan temsilcileri dahil edin.

Satıcı ve Araç Değerlendirmesi: IBM, AWS, Microsoft Azure, Google Vertex AI ve HPE Private Cloud AI gibi satıcıların mevcut çözümlerini değerlendirerek mevcut sistemler ve düzenleyici standartlarla uyumluluğu sağlayın.

Kaynak Tahsisi ve Altyapı

Veri Entegrasyonu: İşlemsel sistemlerden, CRM platformlarından ve harici kaynaklardan gelen verileri kapsamlı analiz için birleşik, güvenli bir havuzda birleştirin.

Bütçe Planlaması: Yapay zeka yazılım lisanslaması, potansiyel donanım veya bulut altyapısı yükseltmeleri ve personel eğitimi için kaynak ayırın. Beklenen dolandırıcılık kaybı azalmalarını uygulama maliyetleriyle karşılaştırarak yatırım getirisini değerlendirin.

Güvenlik ve Uyumluluk: Sıkı veri yönetimi politikaları uygulayın ve çözümün PCI-DSS, GDPR ve diğer sektöre özgü standartlar gibi düzenlemelere uygun olmasını sağlayın.

Pilot Proje & Kavram Kanıtı

Bir Hedef Segment Seçin: İlk pilot uygulama için dolandırıcılık riski yüksek olan belirli bir iş birimi veya işlem türü seçin.

Yapay Zeka Araçlarını Yapılandırma: Seçilen dolandırıcılık tespit çözümünü mevcut sistemlerinizle entegre edin, gerçek zamanlı veri akışları ve uyarı mekanizmaları kurun.

Temel Ölçütler: Pilot başarının ölçülmesinde ölçüt olarak kullanılmak üzere mevcut dolandırıcılık oranlarını, yanıt sürelerini ve yanlış pozitif oranları belgeleyin.

Yürütme ve Benimseme

İşe Alıştırma ve Eğitim: Yapay zeka tarafından oluşturulan uyarıların ve sistem işlevlerinin etkili bir şekilde kullanılmasını sağlamak için güvenlik ve operasyon ekipleri için kapsamlı eğitim oturumları düzenleyin.

Yinelemeli Geri Bildirim Döngüleri: Algılama algoritmalarını iyileştirmek ve eşikleri gerçek dünya performans verilerine göre ayarlamak için düzenli geri bildirim oturumları oluşturun.

Tam Ölçekli Yaygınlaştırma: Dağıtımı kademeli olarak tüm ilgili iş birimlerine genişleterek sorunsuz entegrasyon ve devam eden operasyonlarda minimum kesinti sağlayın.

İzleme ve Değişim Yönetimi

Sürekli İzleme: Temel KPI'ları ve sistem performansını izlemek için gerçek zamanlı gösterge tablolarını kullanın ve ortaya çıkan sorunları derhal ele alın.

Risk Yönetimi: Veri ihlalleri veya otomatik uyarılara aşırı bağımlılık gibi riskleri azaltmak için protokoller geliştirin ve gerektiğinde sürekli insan gözetimi sağlayın.

Ölçeklendirme ve Entegrasyon: Suistimal tespit sistemini daha geniş güvenlik ve risk yönetimi çerçeveleriyle entegre ederek diğer BT ve uyumluluk sistemleriyle birlikte çalışabilirliği sağlayın.

Bakım ve Sürekli İyileştirme

Model Güncellemeleri: Gelişen dolandırıcılık modellerine ayak uydurmak ve yüksek tespit doğruluğunu korumak için yapay zeka modellerini yeni verilerle düzenli olarak yeniden eğitin.

Dokümantasyon: Sürekli iyileştirmeyi desteklemek için tespit metodolojilerinin, sistem konfigürasyonlarının ve süreç ayarlamalarının ayrıntılı dokümantasyonunu sürdürün.

Topluluk ve Ekosistem Katılımı: Dolandırıcılık tespitinde ortaya çıkan trendler ve en iyi uygulamalar hakkında bilgi sahibi olmak için satıcı toplulukları, endüstri forumları ve düzenleyici kurumlarla etkileşim kurun.

Satıcı Tekliflerinin Anlık Görüntüsü

- IBM: Güçlü tehdit tanımlaması için bilişsel bilgi işlem ile gelişmiş analitiği entegre eden kapsamlı dolandırıcılık tespit çözümleri sunar.
- AWS: Bulut altyapısının gücünden yararlanarak ölçeklenebilir, gerçek zamanlı dolandırıcılık tespit hizmetleri sağlar.
- Microsoft Azure: Güvenlik araçları paketi aracılığıyla gelişmiş güvenlik analizi ve anormallik tespiti sunar.
- Google Vertex AI: Dolandırıcılık modellerini tespit etmek amacıyla kapsamlı veri kümelerini analiz etmek için büyük ölçekli makine öğreniminden yararlanır.
- HPE Private Cloud AI: Sıkı uyumluluk ve veri egemenliği gereksinimleri olan kuruluşlar için özel olarak tasarlanmış güvenli, şirket içi veya hibrit çözümleri destekler.

Sonuç

Yapay zeka odaklı dolandırıcılık tespiti, kurumları mali kayıplara, yasal cezalara ve itibar kaybına karşı korumada kritik bir ilerlemeyi temsil etmektedir. Gelişmiş makine öğrenimi algoritmalarından ve gerçek zamanlı veri analizinden yararlanan kuruluşlar, dolandırıcılık faaliyetlerini hızlı bir şekilde tespit edip azaltarak genel güvenliği önemli ölçüde artırabilir. Net hedef belirleme, sağlam veri entegrasyonu, pilot test ve sürekli izlemeyi kapsayan yapılandırılmış bir uygulama süreci, çözümün dolandırıcılığı önlemede ölçülebilir iyileştirmeler sunmasını sağlar. Sektör liderlerinin tedarikçi tekliflerinden yararlanmak, günümüzün dinamik tehdit ortamında gerekli olan ölçeklenebilir, güvenli ve uyumlu bir çerçeve sağlar. Bu teknolojileri benimsemek yalnızca varlıkları korumakla kalmaz, aynı zamanda müşteri güvenini pekiştirir ve kurumu sürdürülebilir başarı için konumlandırır.