

**DOLANDIRICILIK TESPİTİ, ÖNLEMLERİ VE MÜŞTERİ
KORUMA OPERASYONLARI REHBERİ**

FRAUD TESPİTİ 101



formica

İçindekiler

01 / Giriş	3
02 / Dolandırıcılık ve Dolandırıcılık Tespiti Nedir?	5
03 / Neden Dolandırıcılık Tespitine İhtiyaç Duyarsınız?	9
04 / Dolandırıcılık Tespitinin Mekanikleri	12
05 / Şirketinizi Dolandırıcılıktan Korumanın 7 Yolu	16
◦ Dolandırıcılık Grafiği	17
◦ Makine Öğrenimi	18
◦ Alarm Yönetimi	22
◦ Gerçek Zamanlı	24
◦ Ölçeklenebilirlik	26
◦ Kod Gerektirmeyen İşlemler	27
◦ Esneklik- API Entegrasyonu	28
◦ Bonus: Mobil Raporlama	29
06 / Dolandırıcılık Tespit Operasyonunuzu Nasıl Başlatabilirsiniz?	30
07 / Sonuç & Sonraki Adımlar	35

01 /

Giriş

Günümüzde; alışverişten iş hayatına, bankacılık işlemlerinden birçok hobimize kadar her şeyi yönetebildiğimiz teknoloji, hayatımızı kolaylaştırmak için her geçen gün hızla gelişiyor. Kurumların yanı sıra bireyler de hayatın her alanına dair çözümlerin dijitalle aktarılması noktasında dijitalle uyumlu iş alanlarına odaklanıyor. Bu dijital dönüşüm, dolandırıcılar için de yeni fırsatlar yaratıyor.

Dijitalde barındırılan verilerin çok önemli hale geldiği bu çağda, geleneksel dolandırıcılıkların yerini yeni teknolojilerin kullanıldığı dijital dolandırıcılık yöntemleri alıyor.

01 /

Giriş

Şirketlerin veya kişilerin kullandığı teknolojik altyapılardaki zafiyetleri tespit etmeye çalışan ve dijital varlıklarını kötüye kullanan dolandırıcılara karşı geliştirilen teknolojiler de savunma oluşturmak ve kişi ve kurumları korumak için her geçen gün hızla gelişiyor.

Peki nedir bu dijital dolandırıcılık kavramı?

Almanız gereken önlemleri planlamadan önce bu riski yakından tanımakta fayda var.

Bu e-kitap **Formica** tarafından dolandırıcılık ve dolandırıcılık tespiti kavramlarını anlamanız, riskleri yakından tanımanız ve önlemlerinizi planlamanız için hazırlanmıştır.

02 /

Dolandırıcılık ve Dolandırıcılık Tespiti Nedir?

Dolandırıcılık Nedir?

Dolandırıcılık kavramı, temelinde bir suçlu ve bir kurbanı içerir. Ne yazık ki dolandırıcılık için net bir tanım ortaya koymak mümkün değil. Çeşitli yöntemlerle, birçok farklı alanda karşımıza çıkabilir. Öyle ki geleneksel dolandırıcılık ile dijital dolandırıcılık ayrımının yanı sıra dijital dolandırıcılık faaliyetleri bile kendi içinde oldukça çeşitlidir. Dolandırıcılar; kredi kartlarından kişisel verilere, promosyonlardan rezervasyonlara kadar birçok farklı segmentte karşımıza çıkıyor. Yasa dışı veya etik olmayan yollarla elde edilen her türlü kazanç dolandırıcılık olarak sınıflandırılabilir.

Dolandırıcılık sonucu kaybedilen şey ise her zaman para olmak zorunda değildir.

Dolandırıcılık Nedir?

Dolandırıcılığın bir sonucu olarak para ile telafisi mümkün olmayan, uzun vadede kişi ve kurumlar için itibar kaybı, yanlış bilgilendirme, iş fırsatlarının kaybedilmesi gibi daha ciddi sonuçlara yol açabilecek kayıplarla da karşılaşılabilir. Dolandırıcılık ile mücadelede en önemli nokta, suistimalin meydana gelmeden tespit edilebilmesi ve önlenebilmesidir.

Çoğu dolandırıcılık vakası meydana geldikten sonra fark edildiğinde, bu kayıpların telafisi neredeyse imkansızdır. Bir e-ticaret firması olduğunuzu ve müşterilerinizin verilerinin sızdırıldığını düşünün, bu sahtekarlığı gerçekleştikten sonra fark edip yasal işlem başlatsanız bile şirketinizin itibarınızı, medyadaki haberleri ve müşterilerinizin yaşadığı kötü tecrübeyi geri alamazsınız.

Bu noktada kötü bir deneyim yaşamadan önce atmanız gereken adımları planlamalı ve müşterilerinize bu güveni verebilmelisiniz. Güncel teknolojilerin sunduğu dolandırıcılık tespit ve önleme araçları bu aşamada devreye girerek kahramanınız olabilir.

Fraud Tespiti Nedir?

Dolandırıcılık tespiti, kurumların dolandırıcılık faaliyetlerini tespit etme sürecinin tamamını içerir.

Bu faaliyetler finansal olabileceği gibi, sahte kredi kartı işlemleri, veri hırsızlığı veya siber saldırılar gibi diğer biçimlerde de olabilir.

Dolandırıcılık tespiti, genellikle önceden belirlenmiş kural akışlarını dikkate alarak anormal davranışları tahmin etmeye yönelik yöntemlerle yapılır. Dolandırıcılık gibi dolandırıcılık tespit yöntemleri de kendi içinde oldukça çeşitlidir.

Kullanılan teknolojiden tanımlanan iş akışlarına, kullanıldığı sektöre kadar özelleştirilebilen dolandırıcılık tespit ürünleri de artan dijitalleşme ile birlikte yükselen dolandırıcılık vakalarıyla baş edebilmek için hızla gelişiyor.

Fraud Tespiti Nedir?

Dolandırıcılık tespiti için geliştirilen yöntemlerin tıpkı bir hırsız-polis kovalamacası gibi güncel teknolojiye uyum sağlaması, güvenlik açıklarını dolandırıcılardan önce tespit etmesi ve dolandırıcılara açık kapı bırakmaması çok önemlidir.

Birçok dolandırıcı önceden belirlenmiş kalıpları test eder ve güvenlik açıklarından yararlanır.

Her geçen gün gelişen teknolojinin sağladığı imkanlar, dolandırıcılık tespitinin en iyi dostu olduğu gibi, aynı zamanda dolandırıcıların da en iyi dostudur.



03 /

Neden Dolandırıcılık Tespitine İhtiyaç Duyarsınız?

Büyük işletmelerin genellikle dolandırıcılık tespitinde önemli rol oynayan analiz ekipleri vardır, ancak mesai saatleri, insan beyninin hızı ve çoklu görev kapasitesi göz önüne alındığında, hiçbir analistin teknolojiden daha hızlı olamaması şaşırtıcı değildir. Bu noktada analistlerin en büyük destekçisi dolandırıcılık tespit ürünleridir.

İdeal dolandırıcılık tespit ürünleri, müşterilerinizin hareketlerini, normal ve anormal davranışlarını kolayca ayırt ederek size gerçek zamanlı veri sağlayabilmelidir.

Bu verilerin tek tek analiz edilmesinin zorluğu göz önüne alındığında, anormal davranışların önlenmesi, alarm yönetimi, kullanıcı davranışlarının sınırlandırılması gibi aksiyonlar alabilen bir dolandırıcılık tespit aracı, gerçek zamanlı veri sağlamanın yanı sıra dolandırıcılık tespit süreçlerinizde en büyük yardımcınız olacaktır.

Uygun dolandırıcılık tespit teknolojisinin faydaları;

- Dolandırıcılık girişimlerini gerçek zamanlı olarak tespit ederek kayıpları önleyebilirsiniz.
- Müşterilerinizin işlem verilerini ve davranış geçmişlerini analiz ederek bir profil oluşturabilir ve risk durumlarını önceden tespit edebilirsiniz.
- Standart kural akışlarınıza yeni kurallar ekleyerek yeni dolandırıcılık tekniklerine hızla uyum sağlayabilirsiniz.
- Risk durumlarına öncelik verebilir ve kritik durumlara erken müdahale edebilirsiniz
- Manuel incelemeleri azaltarak, dolandırıcılık ekibinizin iş yükünü azaltabilir, daha kritik vakalara odaklanmalarını sağlayabilir ve iş verimliliğini artırabilirsiniz.

Uygun dolandırıcılık tespit teknolojisinin faydaları;

- Verilerinizi daha iyi sınıflandırarak işlevselliği artırabilirsiniz.
- Yanlış pozitif oranlarını azaltarak müşterilerinizle aranızdaki güven ilişkisini koruyabilirsiniz.
- Esnek ve kolay dağıtılan kurallar veya iş akışları ile ekibinizi ve şirketinizi sürekli değişen dolandırıcılık tekniklerine adapte edebilirsiniz.
- Çalışanlarınız ve risk ekipleriniz üzerindeki stresli ve verimsiz dolandırıcılık takibi yükünü azaltarak şirketinizin performansını ve dönüşüm oranını optimize edebilirsiniz.

04 /

Dolandırıcılık Tespitinin Mekanikleri

Artan dijitalleşmenin bir sonucu olarak dolandırıcılık artık birçok farklı varyasyonu ile hayatımıza girdi.

Geleneksel dolandırıcılıklara karşı geliştirilen geleneksel yöntemler, farklı dolandırıcılık türlerinin tespiti ve önlenmesinde oldukça yetersiz kalıyor.

Dolandırıcılığın mekaniklerini yakından tanımak, doğru dolandırıcılık çözümlerine uyum sağlamanın en önemli adımlarından biridir.





Yaygın Dolandırıcılık Türleri

Başvuru Dolandırıcılığı

Başvuru dolandırıcılığı sizin için paradan daha büyük kayıplara mal olabilir. Verilerinizin güvenliği, şirketinizin itibarı için çok önemlidir. Dolandırıcılar, sentetik kimlikleri taklit etmek veya başka birinin kimliğine bürünmek için başvuru sahtekarlığı yöntemlerini kullanarak gerçekleştirdikleri hileler ile sizi oldukça yanıltabilir ve hizmetlerinizi suistimal edebilirler.

Rezervasyon & Bilet Dolandırıcılığı

Hizmetlerinizin kalitesi arttıkça etki alanınız genişler, bunun paralelinde müşteri aktivitelerinizi takip etmek daha zor hale gelir. Gün geçtikçe büyüyen işletmenizi rezervasyon dolandırıcılarına karşı korumak ve hizmetlerinizin kötüye kullanılmasını önlemek oldukça önemlidir.

Promosyon Dolandırıcılığı

Promosyonlar, müşterilerinizi mutlu etmek ve yeni müşteriler kazanmak için oldukça iyi araçlardır. Promosyonların şirketinizi suistimale açık hale getirmemesine dikkat etmelisiniz. Promosyonun kötüye kullanılması, marka kimliğinize ve müşteri sadakatinize zarar verir. Promosyonlarınızın kötüye kullanılmasına izin vermemek için kullanıcı kimliği ve IP'ye özel promosyonlar sağlayabilirsiniz.

Debit Kart ve Kredi Kartı Dolandırıcılığı

Kredi kartınız çalınmasa dahi kart dolandırıcılığına maruz kalabileceğinizi biliyor muydunuz? Güvenlik açığı bulunan kartlar, dolandırıcılar için kolayca erişilebilir hedeflerdir. Kartınızdaki güvenlik açıklarını tespit etmek için dolandırıcılardan daha hızlı olmalısınız. Bunu önlemek için kart işlemlerinizi gerçek zamanlı olarak izlemeli, hesap ekstrelerinizi daima kontrol etmelisiniz.

İnternet Dolandırıcılığı

En yaygın dolandırıcılık türlerinden biri olan internet dolandırıcılığı, dolandırıcıların internet yoluyla kurbanlara verdiği zararların tümünü içerir. En yaygın yolu; veri hırsızlığı, e-posta saldırısı, kötü amaçlı yazılımlar ve kimlik avı olarak bilinir. İnternet dolandırıcılığından korunmanın en etkili yollarından biri, cihazınızdaki yazılımları güncel tutmaktır. Ayrıca, güvenilmeyen kaynaklardan gelen e-postalara karşı da dikkatli olmalı, bilinmeyen kaynaklardan gelen bağlantılara tıklamamalı, ekleri indirmemelisiniz.

E-Posta Dolandırıcılığı

E-posta yoluyla para veya kişisel bilgi almak veya birinin e-postasını çalarak para veya mal toplamak için yapılan dolandırıcılıklardır. Sürecin herhangi bir noktasında e-posta kullanılıyorsa, bu bir e-posta sahtekarlığı olarak kabul edilir. Buna karşı korunmanın en iyi yolu, yanıtlamadan önce bir e-postanın yasal ve gerçek olduğundan emin olmaktır. E-postalarınızı kontrol ederken kurumsal adreslerden geldiğinden emin olmalı, güvenilir kaynaklardan gelmeyen bağlantılara tıklamamalı, zararlı yazılım barındırma riski taşıyan ekleri indirmemelisiniz.

Farklı **dolandırıcılık** türleri
hakkında bilgi sahibi
olmak, risklerin **farkında**
olmanıza ve **çözüm**
bulmanıza yardımcı olur.



05 /

Şirketinizi Dolandırıcılıktan Korumanın 7 Yolu

Dolandırıcılık Grafiği

Dolandırıcılığın birçok yöntemi olduğu gibi gelişen dolandırıcılık teknolojileri dolandırıcılık faaliyetlerinin tespit edilmesini oldukça zorlaştırır.

Birden fazla dolandırıcı, dolandırıcılık amaçlı işlemler gerçekleştirmek için çok sayıda kullanıcıyla dolandırıcılık halkaları oluşturabilir.

Bu organize hareket, tespit noktasında geleneksel dolandırıcılık tespiti araçları ve analistler için oldukça zordur. Dolandırıcılık grafikleri, kullanıcıların verilerindeki ortak kalıpları bulabilir; işlemler, aktörler ve diğer tüm veriler arasındaki ilişkileri gösterebilir.

Dolandırıcılık Grafiği

Şirketler dolandırıcılık grafiği kullanarak, bir ağdaki bağlı kullanıcılar, e-posta hesapları, adresler ve ortak telefon numaraları gibi öğeleri tanımlayabilirler.

Bu sayede dolandırıcılığı tespit etmek için görselleştirilebilen, analiz edilebilen ve bağ oluşturulabilen bir bilgi ağına sahip olabilirsiniz. Örneğin kara para aklamayı ele alalım. Kara para aklamanın birçok yolu vardır, çoğu zaman bu fonlar birçok farklı kuruluştan geçer ve bu da paranın kaynağını izlemeyi zorlaştırır.

Takip edilemeyen para ise aklanır.

Grafik veri tabanları, işlemleri izlemenize olanak tanır ve size paranın kaynağından varış noktasına kadar izlediği tüm yolun net bir resmini sunar.

Makine Öğrenimi

Hileli faaliyetleri kontrol etmek ve tespit etmek, dolandırıcılık analistleri için oldukça zaman alan bir işlemdir. Suistimallerin tespit edilme hızı, analistlerin harcadıkları zamanla doğru orantılıdır. Ancak dolandırıcılar gelişen teknolojik cihazlarla saniyeler içinde milyonlarca dolandırıcılık işlemi gerçekleştirebilir.

Bu zaman kaybı ise para kaybına neden olur, bunun sonucunda aklanan para geri alınamaz. Geleneksel olarak işletmeler, hileli ödemeleri önlemek için yalnızca kurallara dayalı dolandırıcılık tespit sistemleri kullanırdı.

Kurallar, günümüzde hala dolandırıcılık tespit ve önleme araçlarının önemli bir parçası olmakla birlikte, geçmişte tek başlarına kullanımları da bazı sorunlara neden olmuştur.

Kurumların incelemesi gereken veriler arttıkça, bu verilerin uygun yöntemlerle analiz edilmesi, verilerin doğru sınıflandırılması ve dolandırıcılık tedbirlerine paralel olarak kullanıcı hareketlerinin takip edilmesi makine öğrenimi sistemlerinin gerekliliğini ortaya çıkarmıştır.

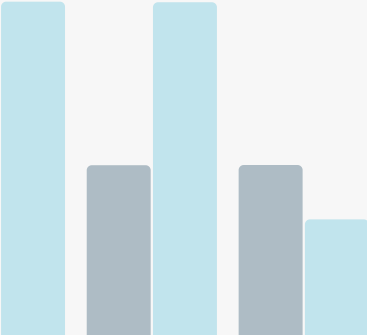
Machine Learning

Makine öğrenimini kullanarak yapılan dolandırıcılık tespiti, bu noktada işletmelere pek çok fayda sağlıyor.

Bu faydalardan bazıları;

- **Daha Az Yanlış-Pozitif Vak**

Dolandırıcılığı tespit etme noktasında bir işlemin gerçek mi yoksa şüpheli mi olduğuna karar vermek analistler için büyük bir zaman kaybı yaratır. Gerçek gibi görünen ancak dolandırıcılık olmayan yanlış pozitifler, iş yükünden dolayı yarattığı zaman kaybı ile gerçek dolandırıcılık hareketlerinin tespit edilme hızını yavaşlatır. Makine öğrenimi modellerini kullanarak yapılan dolandırıcılık tespiti, tespit noktasında hızlı aksiyon alır ve kayıpları en aza indirir.



Machine Learning

- **Daha Az Çalışan İhtiyacı**

Yapay zekaya ne kadar fazla veri ve deneyim sağlanırsa, sonuçlar o kadar iyi olur. Bu noktada elde ettiğiniz verilerin dolandırıcılık analizinde makine öğrenimiyle işlenmesi ve makine öğrenimi ile doğru karar verme algoritmalarının oluşturulması önem arz eder. Makine öğrenimini kullanan dolandırıcılık tespit araçları, dolandırıcılık faaliyetlerini hızla tespit edip telafi etmeye ve işletmelere verilen zararı en aza indirmeye yardımcı olur.

- **Daha Hızlı Dolandırıcılık Tespiti**

Yanlış pozitif işlemler dolandırıcılık gibi görünen fakat analist incelemesi sonucunda gerçek dolandırıcılık olmadığı sonucuna varılan işlemlerdir. Bu durum, olası gerçek dolandırıcılıkların geç tespit edilmesine neden olur ve geç tespit nedeniyle kaybedilen fonlar geri alınamaz. Basit filtreleme mekanizmaları ve algoritmalarla bir araya gelen makine öğrenimi, doğru uyarı sistemlerini oluşturabilir, böylece gerçek dolandırıcılık işlemlerini hızlıca tespit edebilirsiniz

Machine Learning

- Normal ve Anormal Aktiviteleri Analiz Etme

Makine öğrenimi tabanlı anormallik algılama algoritmaları, farklı veri modellerindeki anormal davranışları doğru bir şekilde tespit eder ve bu anormalliklere filtreler uygulayarak yalnızca sizin için önemli olan konularda uyarılar almanızı sağlar. Makine öğreniminin en önemli faydalarından biri, bir analistin yapabileceğinden daha fazla veri işleme ve daha sonra bir insanın tanımlaması zor olan kalıpları tanımlamak için derlenmiş verileri kullanma kapasitesidir. Makine öğrenimini kullanan dolandırıcılık tespit araçları, analistlerin daha önce keşfedilmemiş şüpheli etkinlikleri araştırmasına olanak tanır. Modelleri yeniden eğitime ve ayarlama ve parametreleri otomatik olarak ayarlama yeteneği, risk modeli yönetimi için güçlü bir araçtır



Alarm Yönetimi

Kara para aklamayı önlemek için dolandırıcılık vakalarını gerçekleşmeden anında tespit edebilmeniz elzemdir.

Riskli işlemleri ve olası dolandırıcılık olaylarını analiz etmek ve araştırmak için kapsamlı bir uyarı yönetimi ekranı kullanmak, dolandırıcılık analizi ekipleriniz için çok yararlı olacaktır. Özellikle alarmlarınızı aciliyete göre organize etmek, ilgili çalışma gruplarına veya kişilere e-posta, SMS, mobil bildirim gibi birçok farklı kanaldan bildirim göndermek sizi her zaman tetikte tutacaktır.

Alarm yönetimi sayesinde tüm günü bilgisayar başında geçirmek yerine acil durumlar için uyarı alabilirsiniz.

Ayrıca alarm yönetimi, gerektiğinde izinleri engelleme veya değiştirme gibi işlemleri kolayca gerçekleştirmenizi sağlar.

Alarm Yönetimi

İhtiyaçlarınıza, kurallarınıza ve iş akışlarınıza bağlı olarak işlemleri onaylayabilir veya reddedebilir ve tüm bu akışları alarm yönetim sisteminden kontrol ve koordine edebilirsiniz.

İyi bir dolandırıcılık aracı, dolandırıcılık analistinin alarmı görmesini ve müdahale etmesini beklemeden, belirlediğiniz kural akışları doğrultusunda yüksek riskli işlemler için aksiyon alabilir.

Bu size daha fazla kolaylık ve daha az dolandırıcılık vakası sağlar.



Gerçek Zamanlı

Gerçek zamanlı dolandırıcılık tespiti, dolandırıcılık faaliyetlerini tespit etmek için dolandırıcılık tespit algoritmalarının gerçek zamanlı, anlık olarak yürütülmesidir.

Devam eden bir işlemin meşru olup olmadığını belirlemek için gerçek zamanlı veri analizini kullanır. Gerçek zamanlı sistemler dolandırıcılığı anında tespit etmeden önce, dolandırıcılık sonuçları genellikle dolandırıcılık işlendikten haftalar veya aylar sonra elde edilebilirdi.

Bu durum, dolandırıcılık faaliyetinin izini sürmeyi zorlaştırdı ve dolandırıcıların çok sayıda sahte satın alma yapmasına izin verdi.



Real-Time

Dolandırıcılardan birkaç adım önde olmanın en iyi yolu, şüpheli işlemleri gerçekleşmeden önce gerçek zamanlı olarak tespit etmektir.

Erken saptama, herhangi bir zarar görmeden önlem almanın ilk adımıdır. Böylece firmanızı geri dönüşü olmayan zararlara karşı her zaman koruyabilirsiniz.

Gerçek zamanlı dolandırıcılık tespitinin anahtarı, makine öğrenimi araçlarından yararlanmaktır. Potansiyel dolandırıcılık risklerini analiz etme ve tespit etmede proaktif olmak esastır.

Tespit edilmeyen dolandırıcılıklar müşterilerinizi azaltabilir, itibarınıza zarar verebilir. Yeni stratejilere uyum sağlayarak müşterilerinizin güvenlik endişelerini azaltmalısınız.

Bunu başarmanın en iyi yolu, sahtekarlığı gerçek zamanlı olarak tespit etmek ve kaybı en aza indirmektir.

Ölçeklenebilirlik

Dolandırıcılık tespitine yönelik ölçeklenebilir bir yaklaşım, karmaşık çevrim içi dolandırıcılıklarla başa çıkma becerisini geliştirmek için büyük veri analitiğinin verimli bir şekilde kullanılmasını sağlar.

Bu yaklaşım, dolandırıcılık tespiti verimliliğini artırmak için makine öğrenimi algoritmalarını büyük veri ile destekleyerek uygulanır. Dijital ödeme yöntemlerinin hızla gelişmesiyle birlikte dolandırıcılık tespiti için büyük veri analitiğinin önemi günden güne artıyor. Ölçeklenebilirlik, sahtekarlık tespiti için aynı güvenlik önlemlerini saniyede milyonlarca kez uygulamanıza olanak tanır. Böylece düşük kapasiteli işlemlerde sağladığınız yüksek güvenliği daha yüksek kapasitelerde de rahatlıkla sağlayabilirsiniz.

Verimli bir şekilde ölçeklenmeyen sistemler, trafik yoğun olduğunda daha yüksek bir dolandırıcılık riskiyle karşı karşıya kalmanıza neden olur.



Kod Gerektirmeyen İşlemler

Modern teknoloji altyapıları ve kullanıcı dostu arayüzler, ekibinizin dolandırıcılık tespit ve önleme süreçlerine kolayca uyum sağlamasına olanak tanır.

Kodsuz dolandırıcılık tespiti sunan dolandırıcılık ürünleri, verimliliğinizi artıracak ve teknik bilgi eksikliği güvenlik önlemlerinize engel teşkil etmeyecektir.

Kodsuz kullanıcı müdahalesi sayesinde, teknik bilgi olmadan karmaşık görevleri yürütmek ve otomasyonlar oluşturmak sizi çok zahmetli bir teknik iş yükünden kurtarır.



Esneklik– API Entegrasyonu

Dolandırıcılık tespit teknolojilerinden en kritik beklenti, gelişen dolandırıcılık teknolojilerine karşı her zaman esnek olmasıdır.

Esnek kullanım sunan dolandırıcılık tespit ürünleri, API ağ geçidi aracılığıyla şirketinizin kullandığı herhangi bir hizmet veya uygulama ile entegre olarak birçok iş akışınızı kolayca yönetmenizi sağlar.

API entegrasyonları sayesinde herhangi bir kanalda gerçekleşen etkileşimlerin verilerini gerçek zamanlı olarak dolandırıcılık tespiti platformunuza aktarabilirsiniz.





Bonus: Mobil Raporlama

İşte sizin için bir bonus!

Bunu bulduğunuzda, asla kaçırmamalısınız. Mobil raporlama sunan dolandırıcılık ürünleri, nerede olursanız olun tehlikelerden, iyileştirmelerden, iş süreçlerinden anında haberdar olabilmenizi sağlayarak hayatınızı çok kolaylaştırır.

Mobil raporlama uygulamaları, iş verilerinize ve bilgilerinize doğrudan cep telefonunuzdan güvenli erişim sağlar.

Seyahat ederken, bir toplantıda veya trafikteyken iş raporlarınızı, KPI'larınızı ve gösterge tablolarınızı cep telefonunuzdan kontrol edebilirsiniz. Ayrıca, kullanıcı grupları ve görevlere göre bildirimler ve zamanlanmış raporlar alabilirsiniz.

06 /

Dolandırıcılık Tespit Operasyonunuzu Nasıl Başlatabilirsiniz?

Hedefleri, Metrikleri ve Kaynakları Tanımlayın

Hangi projeye başlarsanız başlayın, ilk adımınız hedeflerinizi belirlemek olmalıdır.

- Dolandırıcılık tespiti ile neyi hedefliyorsunuz?
- Size en çok zarar veren dolandırıcılık türleri nelerdir?
- Dolandırıcılık tespitinde hangi verileri ölçmek istiyorsunuz? Varsa bu verilerin ne kadarını sistemlerinizde tutuyorsunuz?
- Ne tür dolandırıcılık vakalarını tespit etmek istiyorsunuz?
- Daha önce hangi yöntemleri kullandınız?
- Sisteminizin etkinliğini ölçmek için kriterleriniz nelerdir?
- Hayalinizdeki dolandırıcılık tespit operasyonu için ihtiyaçlarınız nelerdir?

Uygun Veri Kaynaklarını Belirleyin

Dolandırıcılık tespit operasyonu ile ilgili hedeflerinizi tamamladıktan sonra bu hedeflerden biri olan veri kaynaklarına odaklanmalısınız.

Dolandırıcılık tespit sistemlerinde yaygın olarak kullanılan veriler;

fatura verisi

ürün kullanımı

risk profili

müşteri profili

Müşteriler hakkında ihtiyaç duyulan diğer veriler satıcı firmalardan alınabilir.

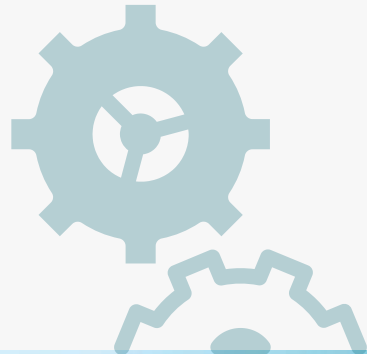
Dolandırıcılık Tespiti Sistemi Yapısını Planlayın

Dolandırıcılık tespit sistemi mimarinizi planlarken birçok faktörü göz önünde bulundurmalısınız.

Dolandırıcılık algılama sıklığı, verilerinizi dolandırıcılık algılama modeliniz aracılığıyla ne sıklıkla çalıştırdığınızı belirler. Dolandırıcılık tespitinde gerçek zamanlı olarak hareket etmelisiniz.

Dolandırıcılık tespit akışları, farklı dolandırıcılık vakalarını şüpheli olarak işaretlemenizi ve bu şüpheli vakaları nasıl değerlendirip onayladığınızı etkileyen parametreleri etkiler.

Puanlama doğruluğu temel çizgisi, dolandırıcılık puanlama modelinizin yeterliliğini değerlendirmek için önemlidir.



Veri Mühendisliği Geliştirin ve İşlem Hatlarını Modelleyin

Veri mühendisliği boru hattı için farklı kaynaklardan gelen verileri birleştirmeniz, bu verileri iş ölçümlerine dayalı olarak toplamamız ve işlemleri ayarlamamız gerekir.

Veri dönüştürme boru hattı için ana amaç, veri kalitesini iyileştirmektir. Eksik ve yanlış veri sorunlarıyla uğraşmak ve verileri makine öğrenimi modelleri için kullanılabilecek şekilde dönüştürmek çok önemlidir.

Makine öğrenimi modeli ardışık düzeni için, temel iş metriklerine dayalı olarak çeşitlendirilmiş makine öğrenimi modelleri oluşturmaya ve karşılaştırmaya odaklanmalısınız.



Dolandırıcılık Tespit Modelinizi Vaka Yönetim Sisteminize Entegre Edin

Artık son aşamaya geldiniz. Şimdi ideal makine öğrenimi modelinizi vaka yönetimi sisteminize entegre etmenin zamanı geldi. Oluşturduğunuz risk puanına göre vakaların risk düzeylerini sıralayabilirsiniz.

Ardından, kritik olarak şüphelenilen vakaların bir listesini gönderebilir ve vaka yönetimi sistemi aracılığıyla daha fazla araştırma için yetkili yöneticilere iletebilirsiniz.



07 /

Conclusion & Next Steps

Finans kurumları ve işletmeler dijital ödemeleri daha güvenli hale getirmek için en güncel stratejileri benimsese dahi dijital dolandırıcılık teknolojileri gelişmeye devam ediyor. Yeni nesil dolandırıcılar, değerli verilerinizi çalmak için yenilikçi teknolojilere hızla uyum sağlıyor.

Dolandırıcılığı önlemek için güvenlik açıklarınızı bilmeli ve riskleri azaltmak için uygun teknolojilere aşina olmalısınız. Çalışanlarınızı dolandırıcılık teknolojilerinden haberdar etmek ve onları kriz senaryolarına hazırlamak faydalı olacaktır. Müşteri ve şirket verilerinizin kötüye kullanılması, maddi kayıpların yanı sıra önemli itibar kayıplarına da neden olacaktır.

Güncel teknolojilere hızla adapte olarak yanlış alarm oluşturmayacak, müşteri deneyiminize zarar vermeyecek veya sizi dolandırıcılığa maruz bırakmayacak teknolojileri doğru bir şekilde tanıyarak ekibiniz ve müşterileriniz için çalışma süreçlerinizi iyileştirebilirsiniz.

Dolandırıcılığın
farkında olun ve
çabalarınızın kötüye
kullanılmasını önleyin.

