



KISA REHBER · RİSK · KİMLİK DOLANDIRICILIĞI

Yeni müşteri, sahte kimlik mi? Taahhütten önce sinyaller kontrol edilir.

Kayıt olan ya da sözleşme başvurusunda bulunan herkes önce kim olduğunu söyleyerek başlar. Bu rehber, PaperOffice'in e-posta adresini, IP adresini, cihazı ve kimlik belgesini kontrol edebileceğiniz sinyaller olarak nasıl sunduğunu gösterir. Mağazalar, platformlar, ev sahipleri ve taksitle satış yapan perakendeciler için.

TEMEL ÇIKARIM

Her kontrol, kuralınızın işleyebileceği alanlar döndürür: e-posta için bir öneri, VPN ve Tor için işaretler, bir cihaz kimliği ve kaynak konumlarıyla kimlik belgesi alanları. Kararı ekibiniz verir.

01 · SORUN NEDİR

İsim doğru. Arkasındaki kişi değil.

Yeni bir müşteri çevrimiçi sözleşme imzalar, akıllı telefon taksitle gönderilir. Ad, adres ve e-posta adresi gerçek görünür. Yalnızca ödemeler durduğunda anlaşılır: veriler başkasına aittir ya da kişi hiç yoktur.

NEDEN OLUR

Çalınmış ve uydurulmuş veriler

Dolandırıcılar veri sızıntılarından gerçek adları ve adresleri kullanır ya da bunları uydurulmuş ayrıntılarla karıştırır. Formda ikisi de aynı görünür.

Ağda gizlenmek

Tek kullanımlık adresler, VPN'ler, Tor ve kiralık sunucular kimin sipariş verdiğini gizler. Aynı kişi az çabayla birçok hesap açabilir.

Acele eden kimlik kontrolleri

Tezgâhta kimlik kopyasına hızlıca bakılır ve yazılır. Bir yazım hatası ya da eksik bir alan kolayca gözden kaçır.

NASIL FARK EDİLİR

- E-posta adresi tek kullanımlık bir hizmetten geliyor ya da alan adının bir posta sunucusu yok.
- Kayıt, normal bağlantı yerine bir VPN, Tor veya veri merkezi üzerinden geliyor.
- IP adresinin ülkesi, belirtilen adresle eşleşmiyor.
- Aynı cihaz farklı adlarla birkaç kayıta görünüyor.
- Formdaki ayrıntılar ile kimlik belgesindeki ayrıntılar farklı.

02 · PAPEROFFICE İLE YAKLAŞIM

Sinyalden karara.

PaperOffice e-posta, ağ, cihaz ve belge üzerinde sinyaller sunar; REST API, SDK ve uygulama üzerinden. Bundan sonrası kuralınıza bağlıdır: kabul etmek, yeniden sormak, incelemeye göndermek veya reddetmek.

1

E-posta adresini değerlendirin

POST /fakeemail/check tek kullanımlık alan adlarını, MX kayıtlarını, SPF ve DMARC'ı kontrol eder ve risk_score ile ACCEPT, REVIEW veya REJECT önerisini döndürür.

MODÜL: SAHTE E-POSTA TESPİTİ

2

Ağı ve konumu kontrol edin

/ip2location/full ülke, bölge ve sağlayıcıyı döndürür; ayrıca is_vpn, is_proxy, is_tor ve is_datacenter değerlerini. Type alanı eşleşen listeyi adlandırır.

MODÜL: VPN TESPİTİ

3

Cihazı tanıyın

Tarayıcı SDK'sı cihaz başına bir visitor_id döndürür. Bir sonraki girişte /fingerprint/verify aynı cihaz olup olmadığını kontrol eder ve risk.factors olağandışı her şeyi adlandırır.

MODÜL: CİHAZ PARMAK İZİ

4

Kimlik belgesini okuyun

Bir IDP Agent, bir fotoğraftan ya da taramadan ad, doğum tarihi, adres, belge numarası ve son geçerlilik tarihini okur; her değer orijinaldeki konumuyla birlikte.

MODÜL: IDP AGENT

5

Karar verin

Uygulamanız alanları bir kurala bağlar, örneğin: tek kullanımlık bir adres ya da Tor, bir kişi tarafından incelenmesi anlamına gelir. Kararı ekibiniz verir.

03 · UYGULAMADA

Anahtarlar, SDK, ajan: kurulum nasıl yapılır.

Sinyal kontrolleri REST API ve SDK üzerinden çalışır, kimlik belgesi ise uygulamadaki bir IDP Agent üzerinden. Adlar uygulamayla eşleşir.

1

Arka ucunuz için bir API anahtarı

API ve Geliştirici > API Anahtarları altında Yeni anahtar oluştur seçeneğini kullanarak bir API Anahtarı oluşturun. Arka ucunuz bunu e-posta ve IP kontrolü için kullanır. Anahtarı istediğiniz zaman oradan kopyalayabilirsiniz.

2

Tarayıcı SDK'sı için bir anahtar

API ve Geliştirici > API Anahtarları altında Yeni anahtar oluştur seçeneğini kullanın, Yayınlanabilir Anahtar türünü seçin ve web sitenizin alan adlarını girin. Sitenizde parmak izi SDK'sı bununla yüklenir.

3

Kimlikler için bir IDP Agent oluşturun

Bir örnek fotoğraf seçin, ardından Eylemler > Ajanlar ve iş akışları > IDP ve Yeni ajan oluştur seçeneklerini kullanın. Kimlik belgeleri için bir şablon seçin ya da alanları kendi cümlelerinizle tarif edin.

4

Değerleri kaynakla karşılaştırın

Veri Alanları sekmesinde her değer, kimlik belgesindeki kod parçasının yanında durur. IDP Review görünümü, açık alanları olan tüm belgeleri gösterir.

5

İnceleme görevlerini tamamlayın

Zorunlu bir alan eksiğe seçilen inceleme kuyruğunda bir görev oluşturulur. Workflow AI > Human In The Loop görevleri altında bir kişi kimliği ve alanları görür ve incelemeyi tamamlar.

UYGULAMADAN BİR İPUCU

Birkaç sinyali birlikte tartın Tek başına bir VPN çoğunlukla zararsız nedenlere dayanır. Tek kullanımlık bir adresle ya da sisteminizde zaten başka hesaplara bağlı bir cihazla birlikte anlam kazanır. Bir kişinin ne zaman inceleme yapacağını tanımlayın.

04 · BİR ÖRNEK

Bir telefon perakendecisi. Taksitli sözleşmeler.



Altı mağazası ve bir çevrimiçi mağazası olan bir cep telefonu perakendecisi, akıllı telefonları sözleşmeler ve taksit planlarıyla satıyor. Mağazada ekip kimlik kopyalayıp verileri yazıyor; çevrimiçi ise bir form yeterli. Ödemeler tekrar tekrar duruyor ve müşterilere ulaşılamıyor.

ÖNCE

- Mağazada kimlik kopyalanır ve sözleşme formuna alan alan yazılır.
- Çevrimiçi olarak, tek kullanımlıklar dahil her e-posta adresi kabul edilir.
- VPN'ler veya veri merkezleri üzerinden gelen başvurular diğerleri gibi görünür.
- Bir cihazın zaten birkaç başvuru yaptığı kimsenin dikkatine gelmez.

PAPEROFFICE İLE

- Çevrimiçi form e-posta adresini kontrol eder; REVIEW durumunda başvuru incelemeye gider.
- IP kontrolü VPN, Tor ve veri merkezini bildirir; başvuru ülkeyi adresle karşılaştırır.
- Her başvuru visitor_id'yi saklar, böylece birden çok kullanılan cihazlar öne çıkar.
- Mağazada bir IDP Agent kimliği bir fotoğraftan okur ve ekip değerleri kaynakla karşılaştırır.

Örnektir, şirket ve süreç uydurulmuştur. Hangi kimlik ve cihaz verilerini topladığınızı ve bunları ne kadar süre sakladığınızı veri koruma görevinizle kontrol edin.

05 · KONTROL LİSTESİ

On madde müşteri onboarding'iniz için.

Bu maddeleri satış, BT ve veri koruma ile birlikte gözden geçirin. Her biri kendi işletmenizde kontrol edilebilir.

- | | |
|--|--|
| ☐ Her kayıt, hesap etkinleştirilmeden önce e-posta adresini kontrol eder. | ☐ REVIEW ve REJECT için ne olacağı tanımlanmıştır: yeniden sormak, incelemeye göndermek veya reddetmek. |
| ☐ Arka ucunuz müşterinin IP adresini ip parametresiyle API'ye gönderir. | ☐ VPN, Tor ve veri merkezi ayrı ayrı değerlendirilir; her durum için bir kural vardır. |
| ☐ IP adresinin ülkesi belirtilen adresle karşılaştırılır. | ☐ visitor_id her hesapla ve her başvuruyla birlikte saklanır. |
| ☐ Bilinen bir hesap tanınmayan bir cihazdan giriş yaparsa, uygulamanız ikinci bir faktör ister. | ☐ Bir IDP Agent kimlik belgelerini okur ve gerekli alanlar tanımlanmıştır. |
| ☐ Silme talepleri için POST /privacy/forget yolu belgelenmiştir. | ☐ Cihaz verilerinin amacı, yasal dayanağı ve saklama süresi veri koruma ile karşılaştırılmıştır. |

06 · SIK SORULAN SORULAR

Ekiplerin başlamadan önce bilmek istedikleri.

PaperOffice kimlikleri biyometrik olarak kontrol ediyor mu?

PaperOffice yüz eşleştirmesi olmadan çalışır. Bir IDP Agent kimlik belgesinin alanlarını kaynak konumuyla okur; diğer kontroller e-posta, ağ ve cihaz hakkında sinyaller verir. Bir kimliğin doğrulanıp doğrulanmayacağına ekibiniz karar verir.

İyi nedenlerle VPN kullanan kişiler ne olacak?

VPN, kuralınızın tartıştığı bir sinyaldir. Yanıt VPN, proxy, Tor ve veri merkezini ayırır ve eşleşen listeyi type alanında adlandırır. Engelleme listelerindeki adresler de is_vpn altında görünür.

Kontroller portalımıza nasıl girer?

Arka ucunuzdan REST API ile, alan adlarınıza bağlı bir **Yayınlanabilir Anahtar** ile parmak izi SDK'sı üzerinden ve MCP ile. Kimlik belgelerini, bir IDP Agent'in çalıştığı bir workspace'e yüklersiniz.

Risk puanı nereden geliyor?

E-posta kontrolünden: 0 ile 100 arasında risk_score, MINIMAL ile CRITICAL arasında risk_level ve ACCEPT, REVIEW veya REJECT önerisi. Cihaz kontrolü, bir VPN ya da olanaksız seyahat hızı gibi kendi risk faktörlerini verir.

Aynı cihazı birden çok hesabın arkasında tespit edebilir miyim?

Evet, visitor_id'yi her hesapla birlikte saklarsanız. O zaman aynı kimlik birden çok hesapta görünür. /fingerprint/similar benzer özelliklere sahip cihazları, /fingerprint/linked ise aynı ağdaki cihazları bulur.

Silme taleplerini nasıl yönetim?

POST /privacy/forget, kuruluşunuzdaki bir tanımlayıcı için cihaz profilini, bağlantıları, geçmişi ve uyarıları siler. Bir engelleme işareti, aynı tanımlayıcının yeniden kaydedilmesini önler.

07 · NASIL BAŞLANIR

Sıradaki kaydınızı gerçek sinyallerle kontrol edin.

app.paperoffice.ai üzerinde bir hesap oluşturun, **API ve Geliştirici > API Anahtarları** altında bir API anahtarı üretin ve ilk adresinizi POST /fakeemail/check ile kontrol edin. Faturalandırma kullandıkça ödeme esasına göre yapılır; ayrıntılar fiyatlandırma sayfasındadır.

E-posta kontrolünü ekleyin

Kayıt formunuz adresi arka ucunuz üzerinden /fakeemail/check adresine gönderir ve öneri alanına göre hareket eder.

IP ve cihazı ekleyin

Ağ ve konum için /ip2location/full, visitor_id için parmak izi SDK'sı. İkisini de başvuruyla birlikte saklayın.

Kimlikleri okutun

Bir kimlik şablonu ile bir IDP Agent oluşturun ve başvurular için workspace'te işlemiden sonra otomatik çalışmasını sağlayın.

BU KONUYLA İLGİLİ TEKNİK VERİ SAYFALARI**Sahte e-posta tespiti**

paperoffice.ai/downloads/paperoffice-ai-datasheet-fake-email-detector.pdf

VPN tespiti

paperoffice.ai/downloads/paperoffice-ai-datasheet-anonymity-detector.pdf

IP konum API'si

paperoffice.ai/downloads/paperoffice-ai-datasheet-ip-location.pdf

Cihaz parmak izi

paperoffice.ai/downloads/paperoffice-ai-datasheet-device-fingerprint.pdf

IDP Agent

paperoffice.ai/downloads/paperoffice-ai-datasheet-idp-intelligent-document-processing-tr.pdf

BU KONUDA DAHA FAZLASI**Kimlik dolandırıcılığı**

paperoffice.ai/tr/solutions/risk/yapay-zeka-kimlik-dolandiriciligi-tespiti-onleme

**BU KONUDA DAHA FAZLASI**

paperoffice.ai/tr/solutions/risk/yapay-zeka-kimlik-dolandiriciligi-tespiti-onleme

FİYATLANDIRMA

paperoffice.ai/en/pricing

İLETİŞİM

paperoffice.ai/tr/iletisim