KPMG
Make the Difference.

Güvenilir Yapay Zeka için Siber Güvenlik Hizmetlerimiz

KPMG Türkiye

-

2026

İçindekiler

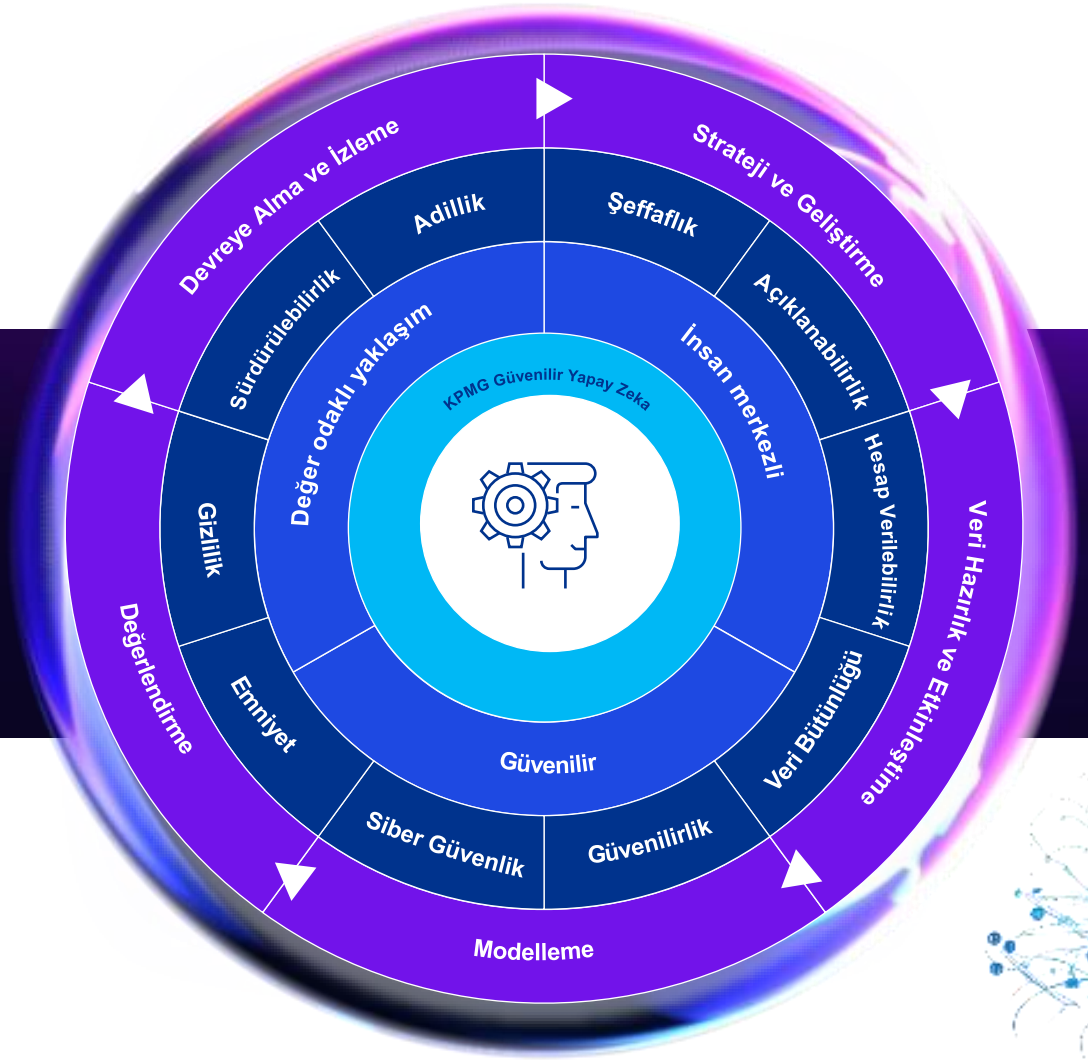
01

KPMG Güvenilir Yapay Zeka Çerçevesi

KPMG Güvenilir Yapay Zeka Çerçevesi

Güvenilir ve etik yapay zeka kullanımının; iş, teknoloji ve yasal düzenlemeler boyutlarıyla karmaşık bir alan olduğunun farkındayız ve müşterilerimizin bu yaklaşımı uygulamaya geçirmelerindeki zorluklarına çözüm üretiyoruz.

KPMG Güvenilir Yapay Zeka yaklaşımımız; yapay zeka uygulamalarının sorumlu ve etik bir şekilde tasarlanması, geliştirilmesi, devreye alınması ve kullanılması için oluşturduğumuz stratejik yaklaşım ve çerçeveyi ifade etmektedir.



200+
Kontrol Sayısı

90+
Risk Tanımı

KPMG Güvenilir Yapay Zeka Çerçevesi; siber güvenlik, gizlilik, veri bütünlüğü başta olmak üzere dijital güven oluşturulması için gerekli yönetişim, risk ve kontrol unsurlarını bir araya getirmektedir.

02

KPMG olarak Nasıl Yardımcı Olabiliriz?

KPMG olarak Nasıl Yardımcı Olabiliriz?

Yapay zeka teknolojilerinin hızla yaygınlaşması, kurumların siber güvenlik yaklaşımlarını ve operasyonel yetkinliklerini yeniden şekillendirmelerini gerektirmektedir. Bu kapsamda sunduğumuz hizmetler; yapay zeka sistemlerinin güvenliğinin sağlanması, siber güvenlik süreçlerinin yapay zeka ile güçlendirilmesi, insan kaynağı ihtiyaçlarının değerlendirilmesi ve yapay zeka güvenliği farkındalığının artırılması olmak üzere dört temel başlık altında yapılandırılmıştır.

01 Yapay Zeka için Siber Güvenlik Hizmetleri

- Yapay Zeka Güvenliği Risk Kontrol Ortamı Analizi
- Yapay Zeka Sızma Testi
- Siber Güvenlik Yaklaşımlarının Yapay Zeka Çerçeveleri ile Desteklenmesi

02 Siber Güvenlik için Yapay Zeka Etkinleştirilmesi Hizmetleri

- Siber Güvenlik Teknolojilerinin Yapay Zeka Uyum ve Hazırlık Analizi

03 Yapay Zeka Dönüşümünde Siber Güvenlik Yetkinlik Analizi Hizmetleri

- Yapay Zeka ve Yeni Nesil Teknoloji Dönüşümleri Işığında Siber Güvenlik Yetkinlikleri İhtiyaç ve Beklentilerinin Değerlendirilmesi

04 Yapay Zeka Güvenliği Eğitim Hizmetleri

- Güvenilir Yapay Zeka Çerçevesi Eğitimi
- Yapay Zeka Güvenliği ve Mimari Eğitimi

01 Yapay Zeka için Siber Güvenlik Hizmetleri

Yapay zeka sistemlerinin güvenli kullanımı, yeni risklerin ve güvenlik ihtiyaçlarının değerlendirilmesini gerektirmektedir.

Bu kapsamda yaklaşımımız; risk analizi, teknik güvenlik testleri ve mevcut güvenlik yaklaşımlarının yapay zeka çerçeveleri ile desteklenmesini içermektedir.

01. Yapay Zeka Güvenliği Risk Kontrol Ortamı Analizi

Yapay zeka ile ilişkili tüm yönetişim, risk ortamı ve siber güvenlik unsurlarını kapsamlı bir bakış açısıyla değerlendiriyor, organizasyon içindeki mevcut riskleri, tehditleri ve güvenlik açıklarını detaylı şekilde analiz ediyoruz. Yaklaşımımızın ana başlıkları;

Değerlendir (Assess):
Kurumların yapay zeka risklerini yönetme yetkinliğine odaklanır.

Güvence Altına Al (Secure):
Yaşam döngüsü güvenliği, anomali tespiti ve saldırılara karşı dayanıklılık gibi yöntemleri içerir.

Mahremiyete Uyum (Respect):
Yapay zeka sistemleri ve çözümleri; veri koruma mevzuatlarına uygun şekilde tasarlanmalı ve yapılandırılmalıdır.

Olay Müdahale (Respond):
Müdahale planları, yapay zeka güvenlik ihlallerinin etkisini azaltır ve savunmadaki eksikleri ortaya çıkarır.

02. Yapay Zeka Sızma Testi

Yapay zeka sistemlerine yönelik sızma testleri gerçekleştirerek model manipülasyonu, kötü niyetli saldırılar, veri manipülasyonu ve yetkisiz erişim gibi senaryolar kapsamında potansiyel güvenlik açıklarını tespit ediyoruz.

- Saldırı Yüzeyinin Kapsamlı Değerlendirilmesi
- Model Dayanıklılık Testleri
- Veri Hattı Denetimi
- Uygulama ve Dağıtım Analizi

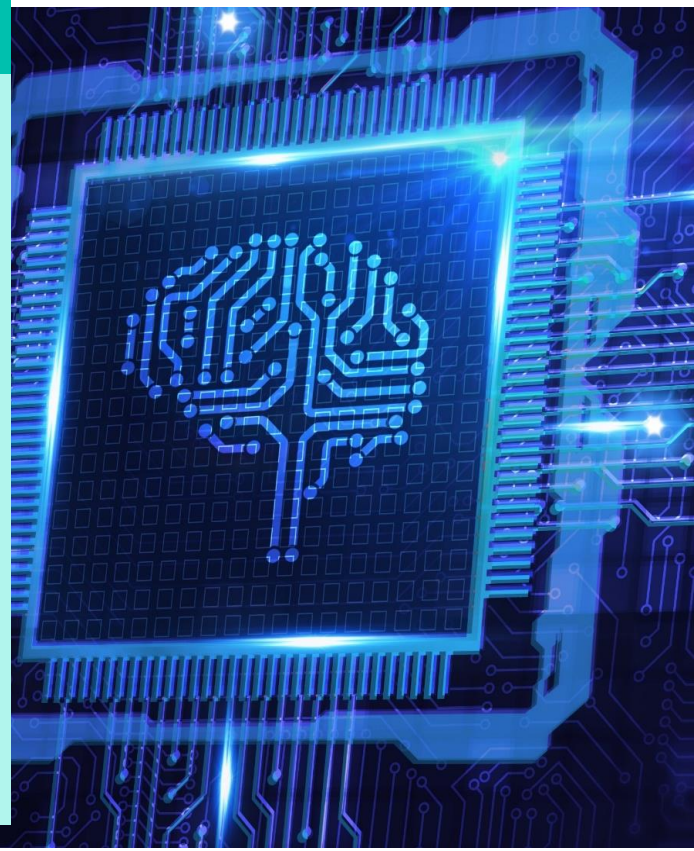
Test sonuçlarına dayanarak yapay zeka sistemlerinin güvenliğini artırmaya yönelik iyileştirme önerileri sunuyoruz.

Geleneksel sızma testlerini, yapay zeka sistemleri için geliştirilen ileri yöntemlerle birleştiriyor ve genelde 4 grupta ele alınan saldırı vektörleri trendleri uyarınca güvenlik analizlerini gerçekleştiriyoruz. İlgili saldırı vektörlerinin detaylarına sayfa 8'de yer verilmiştir.

03. Mevcut Siber Güvenlik Yaklaşımlarının Yapay Zeka Çerçeveleri ile Desteklenmesi

- **NIST AI Risk Management Framework** doğrultusunda NIST'i baz alan kurumlar için çerçevenin mevcut güvenlik yapılarına entegrasyonunu destekliyoruz.
- **KVKK** tarafından yayımlanan yapay zeka rehberleri doğrultusunda veri koruma ve yapay zeka kullanımına yönelik iyileştirme aksiyonlarının belirlenmesine destek oluyoruz.
- **ISO** tabanlı güvenlik yönetim sistemleri kullanan kurumlar (örn. ISO/IEC 27001, ISO/IEC 27701) için yapay zeka yönetişimi kapsamında ISO/IEC 42001 uyum ve implementasyon hizmetleri sunuyoruz.
- **EU AI Act** kapsamında uyum ön hazırlıkları, mevcut durum değerlendirmeleri ve gap analizi çalışmaları gerçekleştiriyoruz.

Farklı güvenlik çerçeveleri kullanan kurumlar için ise benzer yapay zeka güvenliği çerçevelerinin mevcut yapılara adaptasyonuna destek sağlayabiliriz.



Yapay Zeka Güvenliğinde Saldırı Vektörü Trendleri

AI/ML sistemlerine özgü dört temel risk bulunmaktadır. Günümüzde güvenlik ekiplerinin bu tehditleri değerlendirme, koruma ve müdahale etme konularına odaklanması gerekmektedir.

Veri Zehirleme Saldırısı (Poisoning Attack)

- **Tanım:** Bir saldırganın, modelin eğitim sürecine müdahale ederek modeli manipüle etmeye çalıştığı saldırı türüdür. Genellikle modele zararlı veya manipüle edilmiş veri verilerek model içerisinde bir güvenlik açığı oluşturulması amaçlanır.
- **Konfigürasyon:** Geliştirme aşamasındaki AI/ML modelleri bu saldırı türünün temel hedefleri arasındadır.

Model Atlatma Saldırısı (Model Evasion)

- **Tanım:** Tespit sistemlerinden kaçınmayı amaçlayan kötü niyetli saldırı türüdür.
- **Konfigürasyon:** Saldırı tespit sistemleri (IDS – Intrusion Detection Systems) ağ üzerindeki kötü amaçlı trafiği tespit etmek için sıklıkla makine öğrenmesi kullanır. Model evasion saldırılarında ise saldırgan, kötü amaçlı aktiviteleri gizlemek için modelin algılama mekanizmasını yanıltacak teknikler kullanır.

Çıkarım Saldırısı (Inference Attack)

- **Tanım:** Model extraction saldırılarına benzer bir tekniktir. Saldırgan, makine öğrenmesi modeline tekrar tekrar sorgular göndererek modelin davranışlarını gözlemlemeye çalışır.
- **Ortam:** Dışa açık veya herkese erişilebilir modeller, saldırganların kolay erişimi nedeniyle bu tür saldırılara karşı daha yüksek risk altındadır.

Veri Çıkarma Saldırısı (Data Extraction)

- **Tanım:** Saldırganın, modele tekrar tekrar sorgular göndererek modelin verdiği çıkarımları toplaması ve bu sayede özel bir modeli kopyalamaya çalışmasıdır.
- **Ortam:** Dışa açık veya herkese erişilebilir modeller, saldırganların kolay erişimi nedeniyle bu tür veri çıkarma saldırılarına karşı yüksek risk taşımaktadır.

Siber Güvenlik için Yapay Zeka Etkinleştirilmesi Hizmetleri

02

Siber güvenlik operasyonlarında yapay zekadan etkin şekilde faydalanabilmek için mevcut teknoloji ve yetkinliklerin değerlendirilmesi gerekmektedir. Bu kapsamda yaklaşımımız, entegrasyon fırsatlarının analiz edilmesini ve gerekli yapay zeka yetkinliklerinin kuruma kazandırılmasını içermektedir.

01 Mevcut siber güvenlik teknolojileri için yapay zekaya hazırlık (AI readiness) değerlendirmesinin gerçekleştirilmesi

02 Mevcut siber güvenlik ürünlerinin yapay zeka çözümleri ile entegre edilip edilemeyeceğinin ve mevcut teknolojilerin yapay zeka ürünleri ile desteklenme potansiyelinin analiz edilmesi

03 Yapay zeka yetkinliklerinin kuruma nasıl kazandırılabileceğine yönelik teknik, operasyonel ve organizasyonel ihtiyaçların analiz edilmesi

04 Mevcut güvenlik ürünlerinde yer alan ancak aktif kullanılmayan yapay zeka özelliklerinin değerlendirilmesi (örn. IAM/IDM ürünlerindeki erişim analizi, rol önerileri ve anomali tespit fonksiyonları)

05 Yapay zeka yetkinliklerinin organizasyona kazandırılması için gerekli teknoloji güncellemeleri, ürün yenileme ihtiyaçları ve ek teknoloji gereksinimlerinin belirlenmesi

06 Üçüncü taraflardan alınan hizmetlerin sürece dahil edilmesi, hizmet kapsamlarının genişletilmesi ve gerekli sözleşme güncellemelerinin değerlendirilmesi

03 Yapay Zeka Dönüşümünde Siber Güvenlik Yetkinlik Analizi Hizmetleri

Yapay zeka ve yeni nesil teknolojiler, siber güvenlik iş gücünün yapısını ve gerekli yetkinlikleri yeniden şekillendirmektedir.

Bu kapsamda gelecekteki iş gücü yapısı, sektörel öngörüler ve kurum özelindeki yetkinlik ihtiyaçları birlikte değerlendirilmektedir.

Hizmet Kapsamı

Gelecek Siber Güvenlik İş Gücü Tasvirinin Oluşturulması

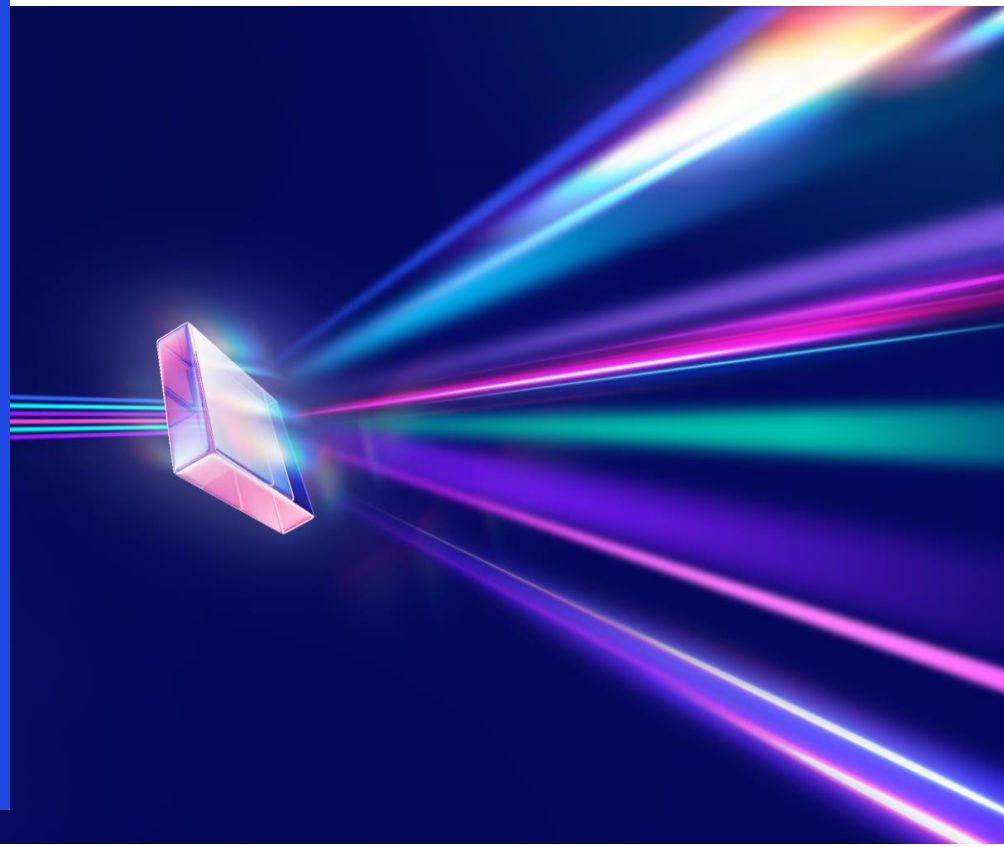
Yapay zeka ve yeni nesil teknoloji dönüşümleri doğrultusunda mevcut siber güvenlik iş gücünün gelecekteki yapısının değerlendirilmesi

Sektörel Öngörüler Doğrultusunda Siber Güvenlik İş Gücü Analizi

Bağımsız kuruluşların tahminleri ve sektörel öngörüler dikkate alınarak siber güvenlik iş gücüne yönelik analiz çalışmalarının gerçekleştirilmesi

Mevcut Durum ve Siber Güvenlik Yetkinlik İhtiyaç Analizi

Önümüzdeki dönemde ihtiyaç duyulacak siber güvenlik yetkinliklerinin değerlendirilmesi ve ihtiyaç-beklenti analiz raporunun oluşturulması



Yapay Zeka Güvenliği Eğitim Hizmetleri

04

Yapay zeka teknolojilerinin güvenli ve etkin şekilde kullanılabilmesi için kurumların hem iş hem de teknik ekiplerinin gerekli bilgi ve yetkinliklerle desteklenmesi gerektiğini düşünüyoruz. Bu kapsamda farklı hedef kitlelere yönelik yapay zeka güvenliği eğitimleri sunmaktayız.

Trusted AI Framework Eğitimi

1. Gün – Framework ve Risk Perspektifi

- Güvenilir yapay zeka ve yapay zeka yönetişimi yaklaşımı
- Yapay zeka kaynaklı risk kategorileri
- İç denetim ve iç kontrol ekipleri için dikkat edilmesi gereken risk alanları
- Yapay zeka sistemlerinde kontrol ve güvence mekanizmaları

2. Gün – Use Case Tabanlı Çalışmalar

- Kurumsal yapay zeka kullanım senaryolarının incelenmesi
- Yapay zeka risklerinin pratik use-case örnekleri üzerinden değerlendirilmesi
- Kontrol mekanizmalarının use-case bazlı uygulanması

Katılımcılar: Bilgi Güvenliği & Siber Güvenlik Uzmanları, İç Denetim, İç Kontrol ve Risk Ekipleri

Yapay Zeka Güvenliği Eğitimi

Tek Gün – Eğitim Ajandası

- Yapay zeka mimarisi ve AI sistem bileşenleri
- Yapay zeka güvenliği ve AI Secure Development Lifecycle
- Yapay zeka sistemlerinde saldırı vektörleri (prompt injection, model extraction, data poisoning vb.)
- LLM mimarisi ve LLM API güvenliği
- AI uygulamalarında deployment ve MLOps süreçleri
- Retrieval-Augmented Generation (RAG) ve AI sistem geliştirme yaklaşımları
- Model Context Protocol (MCP) ve LLM entegrasyon mimarileri

Katılımcılar: Bilgi Güvenliği & Siber Güvenlik Uzmanları, Yapay Zeka Mimarları / Yapay Zeka Mühendisleri

İletişim

Ümit Yalçın Şen
Şirket Ortağı, KPMG Türkiye
Siber Güvenlik Hizmetleri Lideri
M +90 532 387 40 38
E umitsen@kpmg.com

Abdurrahim Gök
Direktör, KPMG Türkiye
Siber Güvenlik Hizmetleri
M +90 506 710 16 25
E abdurrahimgok@kpmg.com

Ceyda Bursalı
Direktör, KPMG Türkiye
Siber Güvenlik Hizmetleri
M +90 536 567 60 36
E cbursali@kpmg.com

Berkay Şahin
Kıdemli Müdür, KPMG Türkiye
Siber Güvenlik Hizmetleri
M +90 506 962 50 29
E berkaysahin@kpmg.com

Detaylı bilgi için:
KPMG Türkiye
Clients & Markets
tr-dlmarkets@kpmg.com

İstanbul
İş Kuleleri Kule 3 Kat:1-9
Levent / İstanbul / Türkiye
T: +90 212 316 60 00

Ankara
The Paragon İş Merkezi Kızılırmak Mah.
Ufuk Üniversitesi Cad. 1445 Sk. No:2 Kat:13
Çukurambar / Ankara / Türkiye
T: +90 312 491 7231

İzmir
Folkart Towers Adalet Mah. Manas Bulvarı
No:39 B Blok Kat:35
Bayraklı / İzmir / Türkiye
T: +90 232 464 2045

Bursa
Odunluk Mah. Liman Cad. Efe Towers
No:11/B 9-10
Nilüfer / Bursa / Türkiye
T: +90 224 503 8000

Adana
Sunar Nuri Çomu İş Merkezi Çınarlı Mah.
61027 Sk. A Blok No:18/A İç Kapı No:9
Seyhan / Adana / Türkiye
T: +90 322 450 2120

Antalya
Altınova Sinan Mah. Ulu Sk. No:3 Altınova
Corner İş Merkezi B Blok 6.Kat No:21-24
Kepez / Antalya / Türkiye
T: +90 242 333 0909

kpmg.com/socialmedia

KPMG
Make the Difference.


KPMG