

İSTEM VE AJAN GÜVENLİĞİ MİMARİSİ

İstemden araç çağrısına kadar katmanlı kontrol.

İstem ve ajan güvenliği mimarisi

Kullanıcı girdilerini, model trafiğini, yapay zekâ (YZ) ajanlarını ve araç çağrılarını ortak kimlik, politika ve denetim yaklaşımıyla ele alan yüksek seviyeli mimari görünüm.

KİMLİK

POLİTİKA

KAYNAK

AĞ

DENETİM

SOFTBYT LABS ÜRÜN AİLESİ • GENEL MİMARİ



İSTEM VE AJAN GÜVENLİĞİ MİMARİSİ

Korunması gereken yüzeyler

YZ güvenliği yalnızca istem filtresi değildir; konuşma geçmişi, dosya, kaynak, araç, ağ ve kimlik birlikte değerlendirilir.

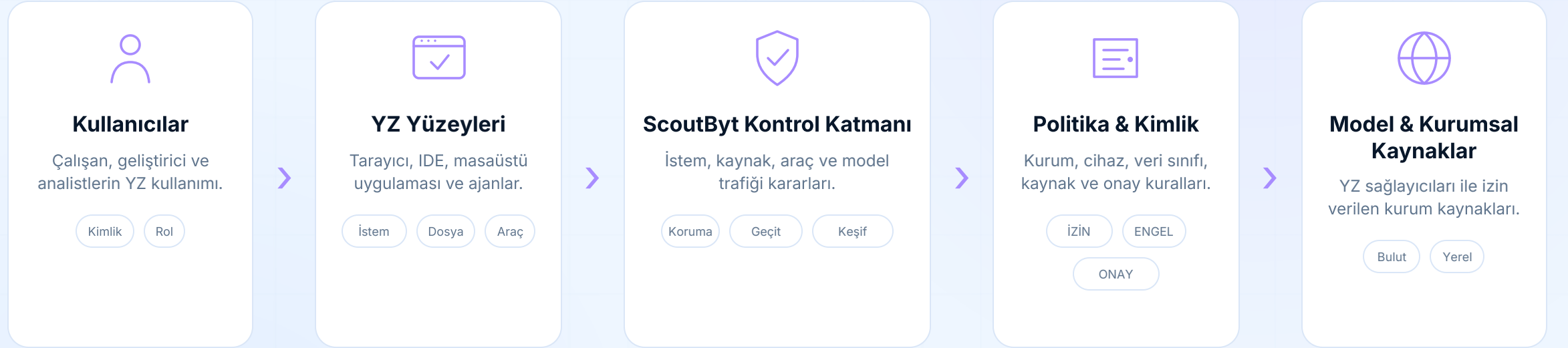
Doğrudan veri sızıntısı • dolaylı istem enjeksiyonu • aşırı yetki • Gölge YZ



İSTEM VE AJAN GÜVENLİĞİ MİMARİSİ

Yüksek seviyeli çalışma modeli

Bu görünüm ürünün güvenlik mantığını anlatır; özel entegrasyon ve doğrulama yöntemlerini açıklamaz.



Yüksek seviye

Her entegrasyon aynı teknik yöntemle çalışmaz; kapsam ilgili ürünün sunduğu güvenlik yüzeylerine göre uygulanır.

İSTEM VE AJAN GÜVENLİĞİ MİMARİSİ

Yönetilen bir akışta her işlem, bağlamına göre açık bir güvenlik kararı üretir.

Karar modeli ve tasarım ilkeleri

İzin Ver

Politika ve bağlam uygun.

Uyar

Kullanıcıya görünür risk bildirimi.

Engelle

Korunan veri veya yetkisiz eylem.

Onay Gerekli

İnsan kararına yönlendirilen işlem.

Kullanıcı yetkisi, YZ yetkisi değildir

İnsan erişimi, ajana otomatik olarak devredilmez.

Asgari yetki

Ajan yalnız görev için gereken kaynak ve araçlara erişir.

Eylem öncesi kontrol

Desteklenen yüzeylerde istem veya araç eylemi gerçekleşmeden değerlendirilir.

Mahremiyet odaklı denetim

Karar ve politika izi tutulur; ham hassas veri gereksiz yere saklanmaz.

Güvenli hata davranışı

Yönetilen politika uygulaması akışlarında doğrulanamayan işlem sessizce serbest bırakılmaz.

Kademeli uygulama

Önce keşif ve simülasyon, ardından kanıtlanan yüzeylerde politika uygulaması.