YAPAY ZEKÂ VE AJAN GÜVENLİĞİ

AI Guard

Yapay zekâ kullanımı. Sınırlarını siz belirleyin.

ScoutByt ekosisteminde yapay zekâ kullanımını, istemleri ve yönetilen ajan eylemlerini tanımlı bir görünürlük ve politika kapsamında değerlendirin.

BİR BAKIŞTA

01 Tarayıcı ve istem denetimi

02 Model trafiği politikaları

03 Yönetilen ajan sınırları

04 Denetim ve güvenlik olayları

AI Guard, ScoutByt AI Security adıyla sunulan yapay zekâ güvenliği yaklaşımının değerlendirme kapsamını temsil eder. Kullanılabilir kontroller; desteklenen alan, yapılandırılan politika ve doğrulanmış kurulum kapsamına bağlıdır.

YETENEKLER VE İŞ AKIŞI

Yapay zekâ kontrollerini belirli sınırlar içinde değerlendirin.

01 ## Yapay zekâ kullanımını anlayın

Doğrulanmış değerlendirme kapsamında Browser Guard ve Application Discovery, desteklenen ortamlardaki yapay zekâ kullanımının görünürlüğünü destekleyebilir.

02 ## Veri ve istem sınırlarını belirleyin

Desteklenen trafik yollarında Prompt Guard ve AI Gateway, yapılandırılan kontrolleri istemlere ve model trafiğine uygulayabilir.

03 ## Ajan erişimini tanımlayın

Tanımlı değerlendirme kapsamında Agent Guard ve MCP & Tool Control; yönetilen oturumları, kaynak erişimini ve araç eylemlerini değerlendirebilir.

04 ## Kararları inceleyin

Değerlendirilen kapsamda etkinleştirildiğinde Policy Center ve Audit & Security Events, politika kararlarını ve güvenlik bağlamını inceleme sürecine taşıyabilir.

Yapay zekâ kullanım alanları

Bağlam ve politika

Tanımlı kapsamda kontroller

Denetim ve inceleme

KULLANIM ALANLARI VE KURULUM

Politika uygulamasından önce ortamı doğrulayın.

Kurumsal yapay zekâ kullanımı	Tarayıcıdaki yapay zekâ kullanımını değerlendirin; uygun veri sınırlarını belirleyin.
Geliştirici iş akışları	Desteklenen geliştirici ortamlarında model trafiğini ve araç çağrılarını değerlendirin.
Yönetilen ajan oturumları	Kontrollü değerlendirme için kaynak erişimi ve eylem sınırları belirleyin.

Entegrasyon alanları: Desteklenen tarayıcılar · Model geçitleri · Geliştirici ortamları · MCP ve yönetilen araçlar

Desteklenen ortam ve kontrol matrisi teknik keşifte belirlenir. Bir entegrasyon kategorisinin listelenmesi, tüm sağlayıcı ve sürümlerin desteklendiği anlamına gelmez.

info@softbytlabs.com