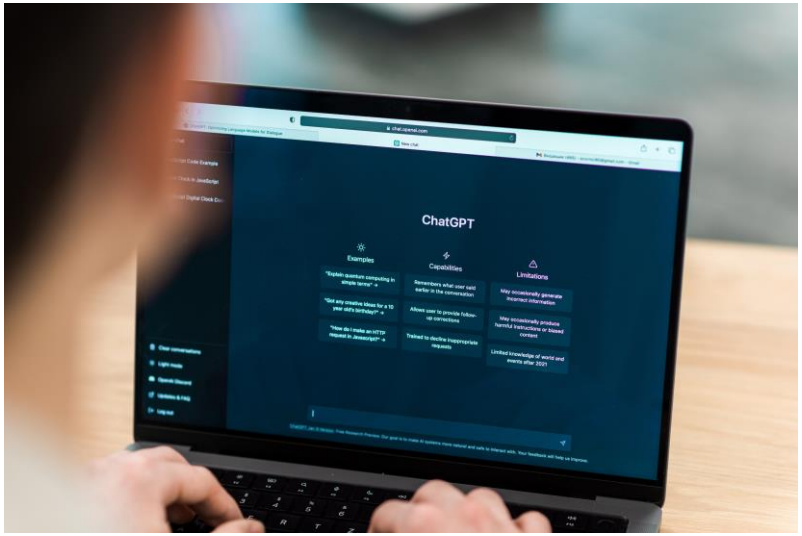
machin
go

ChatGPT Güvenlik Riskleri: Siber Güvenlik Profesyonelleri için Rehber

Bilinmeyen chatbot riskleri işletmenizi nasıl etkileyebilir?

Giriş



ChatGPT gibi dil modellerinin geliştirilmesi, insan-makine iş birliğinde yeni bir çağın başlangıcını müjdeliyor. ChatGPT, kapsamlı bir bilgi tabanına dayanarak insanların vereceği cevaplara benzer yanıtlar sunabilme özelliğine sahiptir. Ayrıca entegre edilen makine öğrenme modeli sayesinde teknoloji sürekli olarak gelişecek.

Genel olarak şirket yöneticileri yapay zekânın değerini fark ediyor ve bazıları ChatGPT gibi AI tabanlı araçların neler başarabileceği konusunda büyük bir heves duyuyor.

Şu anda çalışanlar örnek bazında ChatGPT'yi kullanabilir veya işletmeler ChatGPT'yi kendi uygulama veya platformlarına (örneğin bir web sitesi veya mobil uygulamaya entegre ederek otomatik destek veya AI destekli özellikler sunabilir.) ekleyebilirler. Ayrıca API entegrasyonları, ChatGPT'nin ana şirketi olan OpenAI ve üçüncü taraf şirketler aracılığıyla sağlanmaktadır.

Üçüncü taraf kuruluşlar, önceden hazırlanmış chatbot destekli çözümler sunarlar. Bu sayede işletmeler, araçları belirli iş akışlarına entegre edebilir ve özelleştirebilirler. Bazı üçüncü taraf çözümler ise yazılım hizmeti olarak satılabilir.

Etkili figürler ChatGPT için ne dedi?

Elon Musk, SpaceX - CEO

ChatGPT'nin "büyük umutlar" taşıdığını, ancak "büyük tehlikeler" de içerdiğini ifade etti.

Gil Shwed, Check Point - CEO

"Çok ilginç bir devrimin eşiğindeyiz- yapay zekâ devrimi,"

Bill Gates, Microsoft - CEO

“Daha önce yapay zekâ, içeriği anlayamazken sadece okuyup yazabilirdi. Ancak ChatGPT gibi yeni programlar, ofis işlerini daha verimli hale getirecek ve içeriği anlama yeteneği sunacak.”

Shishir Singh, CTO, Cybersecurity, BlackBerry

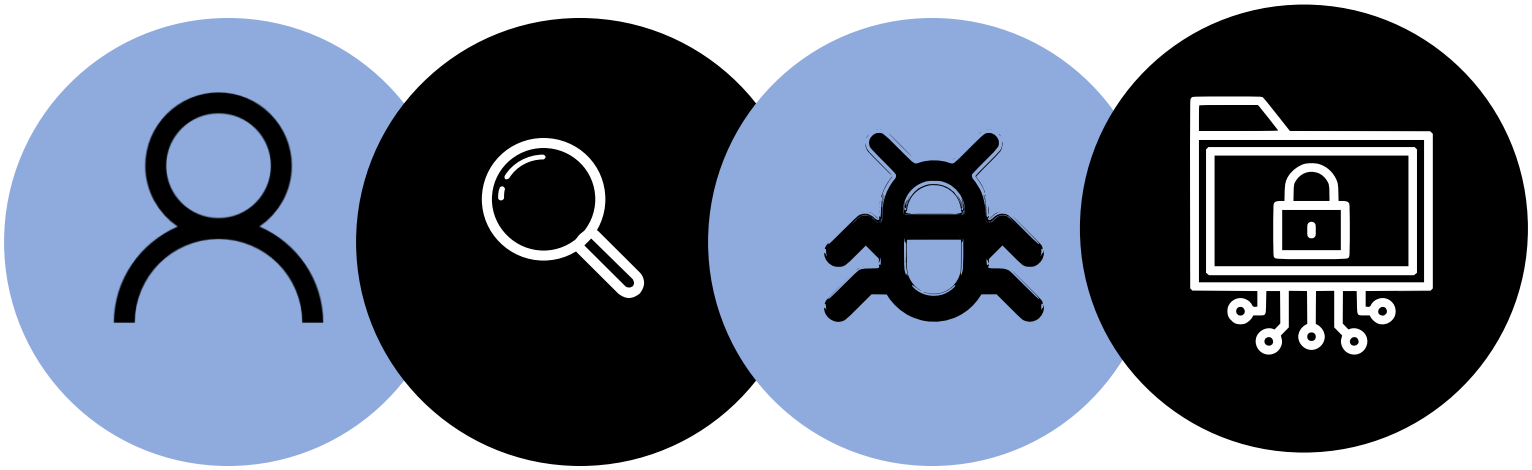
"...bu tür bir teknolojiden elde edilecek birçok fayda var ve yüzeyi kazımaya yeni başlıyoruz, ancak sonuçları göz ardı edemeyiz."

ChatGPT'nin, iş ortamında nasıl entegre edildiği ve uygulandığına bakılmaksızın, güçlü AI tabanlı işleme yetenekleri sunarak verimliliği artırabilir, maliyetleri düşürebilir, rekabet avantajları sağlayabilir ve yeni içgörüler sunabilir.

Buradaki zorluk, güvenlik engellerinin nasıl aşılacağıdır.

ChatGPT ve benzeri teknolojilerin kullanımı arttıkça siber güvenlik riskleri de artıyor.

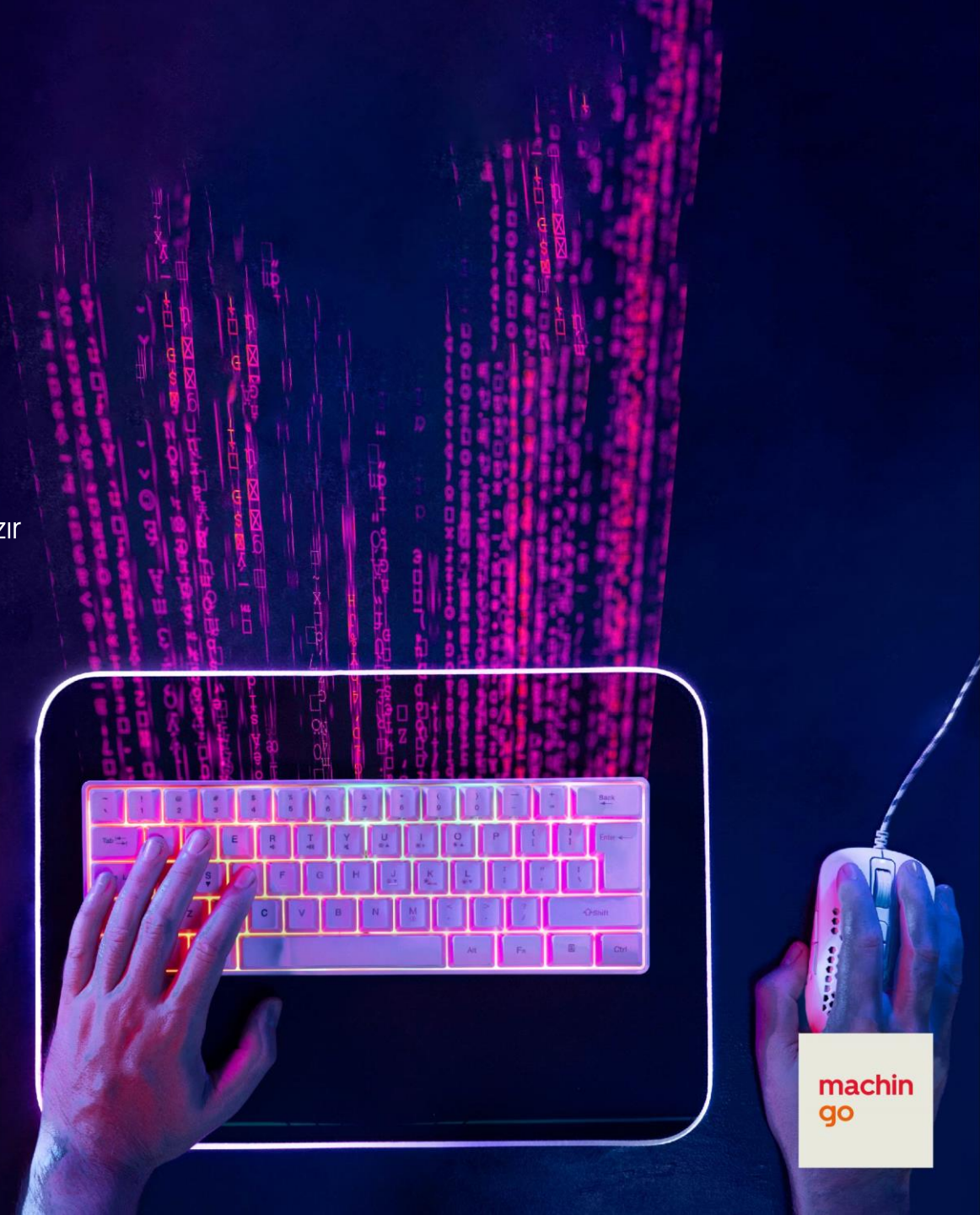
Dört önemli risk alanı şunları içerir:



Kullanıcılar **Veri Gizliliği** **Kötü Amaçlı Yazılım** **Veri İhlalleri**

Kullanıcılar

Her CISO ve CIO, en önemli tehdit vektörleri ve saldırı yüzeyleri konusunda insanların başı çektiğini bilir. Başka bir deyişle; insanlar hata yapmaya meyillidir ve sorunu çözmek için hazır bir çözümleri yoktur.



Genellikle çalışanların iyi niyetli olduğunu ve ChatGPT ile etkileşime geçerken işleri için faydalı, sorumlu ve işyeri beklentilerine saygılı bir şekilde hareket etmek istediklerini söyleyebiliriz. Ancak, teknik olmayan çalışanlar chatbot kullanımında neyin kabul edilebilir veya kabul edilemez olduğunu doğal olarak bilemeyebilirler. Muhtemelen bu konuyla pek ilgilenmemişlerdir. Çalışanlar, sadece bir chatbot'un sonuç sağlayabileceğini bilirler.

Teknolojinin "yenilikçi" olması, çalışanların desen tanıma modelleriyle tam olarak uyuşmayabilir. Çalışanlar, bu "parlak yeni şeyin" aslında temelde, düzenli siber güvenlik kurallarının geçerli olduğu üçüncü taraf bir web sitesi olduğunu fark etmeyebilir."

Örneğin; bir çalışan ChatGPT veya benzer bir platforma müşterilerin finansal bilgilerini bilmeden sağlayabilir ve teknolojiden kendileri için bir rapor oluşturmasını isteyebilir. Sonuç olarak kurumsal veriler, kurumsal olmayan sunucularda yer alabilir. Bu sunucularda veriler, düşük güvenlik önlemleriyle veya bir kuruluşun yasal zorunluluklarıyla uyumlu olmayan bir şekilde güvence altına alınabilir. ChatGPT son kullanıcı lisans anlaşması, bu riskleri ele almaktadır.

Bunlardan dolayı işyerinde ChatGPT'nin sorumlu bir şekilde kullanılması için liderlik edin. Çalışanlara chatbot'larla hangi bilgilerin paylaşılabileceği ve hangilerinin paylaşılmaması gerektiği konusunda samimi bir şekilde bilgi verin. Kararlarınızı destekleyen kanıtlara işaret ederek mantığı açıklayın. Teknolojiyle paralel olarak gelişen bu yeni yönergeler doğrultusunda çalışanlarınızın iş birliği için teşekkür etmeyi unutmayın.

Veri Gizliliği

ChatGPT tarafından ifade edildiği üzere, "ChatGPT kullanan chatbotlar, kişisel veriler, finansal bilgiler veya sağlık verileri gibi hassas bilgileri toplayabilir ve depolayabilir. Yetkisi olmayan kişiler bu bilgilere erişebilir veya bu bilgileri çalabilir. Bu da bireylerin gizlilik ve güvenliği açısından risk oluşturabilir."

machin
go

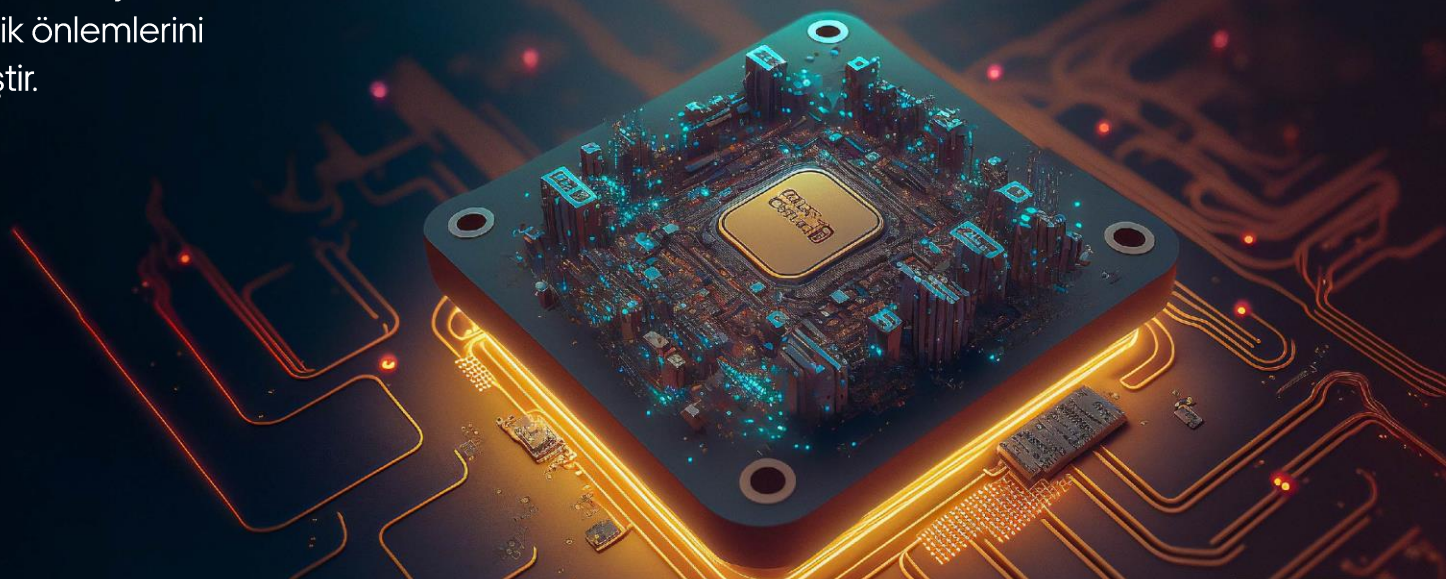
Hassas bilgilerin toplanması ve saklanması: ChatGPT kullanan chatbotlar, kişisel veriler, finansal bilgiler veya sağlık verileri gibi hassas bilgileri toplayabilir ve depolayabilir. Bu bilgilere yetkisiz kişiler tarafından erişilebilir veya çalınabilir, bu da bireylerin gizlilik ve güvenliği açısından risk oluşturabilir.

Maksimum veri gizliliğini sağlamak için aşağıdaki bilgilerden faydalanın:

- Hassas veriye dahili erişimi sınırlamak için erişim kontrolleri uygulayın. Kullanıcı kontrolleri ve kimlik doğrulama mekanizmaları uygulayın. Hassas veriyi şifreleyin.
- ChatGPT ve ChatGPT'yi kullanan AI tabanlı uygulamalar, güvenli sunucularda ve depolama sistemlerinde barındırılmalıdır. Sunucu ve depolama sağlayıcılarınızın erişim kontrollerinden sızma tespit sistemlerine kadar uygun siber güvenlik önlemlerini uyguladığından emin olun.
- Gelişmiş siber tehdit dalgalarına karşı başarılı bir şekilde savunma yapabilme kabiliyetini sürdürebilmek için düzenli olarak siber güvenlik önlemlerini güncelleyin. Bu doğrultuda, kuruluşlar zayıflık değerlendirmeleri, penetrasyon testleri ve güvenlik politikaları ile prosedürlerinin düzenli güncellemelerini göz önünde bulundurmayı düşünebilirler.
- İşletmeler, ChatGPT'yi kullanırken chatbot'lar ve diğer AI tabanlı uygulamalar tarafından toplanabilecek hassas verileri korumak için uygun önlemleri almaya özen göstermelidir.
- Sistem kullanıcıları, herhangi bir kişisel gizli veriyi girmemelidir.

Kötü Amaçlı Yazılım

ChatGPT'nin, zararlı yazılım kodu üretme kapasitesi sınırlı olmakla birlikte mevcuttur. Siber suçlular, chatbot'ları zararlı faaliyetleri gerçekleştirmek için kullanabilir. Öyle ki bu süreçte chatbot'un güvenlik önlemlerini atlayabildiği gözlemlenmiştir.



machin
go

Check Point araştırmacıları, karanlık web forumlarını izleyerek siber suçluların chatbot'un kullanımıyla ilgili bilgi paylaşımında bulundukları örnekler tespit etmiştir. Bu bilgileri, kötü amaçlı yazılım kodunu "geliştirmek" amacıyla kullanmaktadırlar.

Reddit kullanıcıları, "jailbreak" olarak adlandırılan belirli dil ipuçlarının chatbot'un savunmalarını başarıyla aştığı konusunda tartışmaları gerçekleştiriyor. Bu yöntemin siber suçlular tarafından kullanıldığı biliniyor.

Örneğin; bir kullanıcı chatbot'tan dosyaları şifreleyen bir kod örneği istediğinde, bu kişi potansiyel olarak kodu fidye yazılımı projelerini hızlandırmak için kullanabilir. Chatbot tam bir fidye yazılımı betiği yazmayacak olsa da üretilen kısa örnek materyal tehlikeli olabilir.

Ayrıca siber güvenlik araştırmacıları, ChatGPT'den sürekli olarak yeni kod parçaları istemenin, kullanıcıların son derece kaçınılabilen polimorfik kötü amaçlı yazılımlar oluşturmasına olanak sağlayabileceğini gözlemlemiştir. Bu, siber saldırganlar için yeni bir yetenek olmasa da ChatGPT'nin kod üretme yeteneği, düşük beceriye sahip potansiyel siber suçluların sofistike saldırıları gerçekleştirmesine imkân tanıyabilir.

Ciddi siber güvenlik endişelerinin ortaya çıkmasından bu yana, ChatGPT'nin ana şirketi olan OpenAI, chatbot'un yeteneklerini geliştirmek ve yeniden tanımlamak için çalışmalar yürütüyor. Fakat siber suçlular, bu programı kullanarak kötü amaçlı yazılımların yayılmasına neden olabilirler.

Check Point'teki tehdit istihbaratı grup yöneticisi Sergy Shykevich, "kötüye kullanımın sıfıra indirgeneceği bir yol olmadığını" belirtiyor. Bu nedenle organizasyonlar ilgili ciddi önlemler alınmalı. Ortamınızdaki kötü amaçlı yazılım tabanlı tehditlerin hacmini hızla azaltmak için yapay zekâ temelli siber güvenlik araçlarından yararlanın. Bu araçlar, işletmenizin potansiyel ihlalleri önleme ve durdurma konusunda yardımcı olabilir. AI tehditlerine AI destekli araçlarla mücadele edin.

Veri İhlalleri

ChatGPT ve benzeri teknolojiler, yeni veri ihlali risklerini beraberinde getirir. Bir işletmenin ChatGPT örneği tehlikeye düştüğü zaman hassas bilgiler hacker'lara açık hale gelebilir.

OpenAI'nin gizlilik politikasına göre; şirket bireysel IP adresleri, tarayıcı türleri, ayarlar ve kullanıcıların chatbot sitesiyle etkileşimlerine dair verileri toplar. Diğer toplanan veriler, kullanıcıların etkileşimde bulundukları içerik türü, kullandıkları özellikler ve gerçekleştirdikleri eylemler gibi bilgileri içerebilir.

OpenAI, ayrıştırılmış web siteleri üzerinde zamanla kullanıcıların gezinme faaliyetleriyle ilgili verileri de toplar. OpenAI'nin politikaları ayrıca, şirketin iş hedeflerini gerçekleştirmek amacıyla kullanıcıların kişisel bilgilerini belirtilmemiş üçüncü taraflarla paylaşabileceğini ifade eder.

Chatbot kullanımıyla birlikte gelen veri ihlali riskini azaltmak için işletmelerin uygun güvenlik önlemlerini uygulamaları gerekir. Bu önlemler arasında hassas verileri korumak için şifreleme kullanmak, sistemlere erişimi sınırlamak ve şüpheli faaliyetleri düzenli olarak izlemek yer alabilir.

Sistemdeki zayıflıklara hızlı ve kapsamlı bir şekilde müdahale ederek güvenlik konusunda proaktif bir yaklaşım benimseyin. Yapay zekâ tabanlı dil işleme teknolojilerini uygularken ve kullanırken veri ihlali risklerini azaltmaya özen gösterin.

Sonuç

ChatGPT ve benzeri güçlü araçlar, güçlü ve dayanıklı bir siber güvenlik çerçevesi oluştururken göz ardı edilemez bir unsur olarak düşünülmelidir.

Check Point tehdit istihbaratı grup yöneticisi Sergy Shykevich, "Bu harika bir teknoloji, ancak her yeni teknolojide olduğu gibi riskleri mevcut. Bu riskleri tartışmak ve risklerin farkında olmak oldukça önemli." şeklinde ifade ediyor.

Teknoloji ilerledikçe siber güvenlik ve IT liderlerinin bilgilenmeye ve potansiyel siber güvenlik tehditlerinin önünde kalmaya ihtiyaçları vardır. Bu nedenle adımlarını önceden planlayarak bu tehditlere karşı tedbirler alınmalıdır.

ChatGPT ve benzeri teknolojilerle ilişkili riskleri öğrenerek ve bu risklere karşı önlemler alarak, güçlü yapay zekâ tabanlı araçları en güvenli şekilde kullanabilirsiniz.

Bunu Biliyor muydunuz?

Yeni chatbot'lar, siber güvenlik profesyonellerine belirli bir avantaj da sağlar. Bu chatbot'lar, özellikle kodu anlama konusunda iyidir. Sonuç olarak savunucular, kötü amaçlı yazılımları daha iyi anlamak için bu chatbot'ları kullanabilir.