Yapay Zeka Destekli Siber Güvenlik Teknikleri: 2025 ve Sonrası İçin Kapsamlı Bir Değerlendirme

Yönetici Özeti

2025 yılına girerken, yapay zeka (YZ) siber güvenlik ortamını temelden yeniden şekillendirmektedir. Bu rapor, YZ'nin hem güçlü bir savunma aracı hem de daha sofistike saldırıların bir kolaylaştırıcısı olarak oynadığı ikili rolü incelemektedir. Kuruluşların, gerçek zamanlı tehdit tespiti, otomatik yanıt ve gelişmiş kimlik yönetimi gibi alanlarda YZ'yi savunma stratejilerine proaktif bir şekilde entegre etmelerinin kritik önemi vurgulanmaktadır. Aynı zamanda, yeni YZ'ye özgü güvenlik açıklarının ele alınması ve insan-YZ işbirliğinin teşvik edilmesi de hayati önem taşımaktadır.

Bu raporun temel çıkarımları arasında, YZ destekli tehdit tespiti ve öngörücü analitik, üretken YZ'nin güvenlik operasyonlarında kullanımı, YZ ile güçlendirilmiş uç nokta güvenliği, kimlik ve erişim yönetiminde (KİM) YZ'nin rolü, YZ destekli Güvenlik Orkestrasyonu, Otomasyon ve Yanıt (SOAR) platformları, derin sahtecilik (deepfake) ve gelişmiş sosyal mühendislik savunması ile kuantum güvenli güvenlik planlaması yer almaktadır. Bu teknikler, siber savunmanın geleceğini şekillendirecek temel unsurlardır.

Giriş: 2025'in YZ Odaklı Siber Güvenlik Ortamında Gezinmek

Yapay zeka, artık uzak bir gelecek kavramı olmaktan çıkmış, siber güvenlikte merkezi bir itici güç haline gelmiştir. 2025 RSA Konferansı gibi büyük etkinliklerde YZ tartışmalara hakim olmuş, ürün duyurularında, gösterilerde ve açılış konuşmalarında öne çıkmıştır.[1] Bu yaygın benimseme, YZ'nin gelişmiş tehditleri tespit etme ve azaltmadaki kritik rolünün bir göstergesidir.[2]

YZ'nin siber güvenlikteki etkisi, onun ikili doğasından kaynaklanmaktadır: hem savunmacılar için güçlü bir araç hem de tehdit aktörleri için etkili bir saldırı vektörü.[1] Derin sahtecilikler, polimorfik kötü amaçlı yazılımlar ve gelişmiş sosyal mühendislik gibi YZ destekli saldırıların artan karmaşıklığı ve ölçeği, savunma stratejilerinde YZ'nin hızla benimsenmesini zorunlu kılmaktadır. Bu durum, siber güvenlikte sürekli inovasyonun kaçınılmaz olduğu dinamik bir "YZ silahlanma yarışı" yaratmaktadır. 2024 yılında BT uzmanlarının %51'inin başarılı siber saldırıları YZ'ye atfetmesi, savunmacılar için YZ'den yararlanmanın aciliyetini açıkça ortaya koymaktadır.[3]

Proaktif ve Adaptif Güvenlik Stratejilerinin Zorunluluğu

YZ odaklı tehditlerin dinamik doğası, reaktif savunmadan proaktif bir yaklaşıma geçişi gerektirmektedir.[3] Kuruluşlar, yalnızca saldırılara yanıt vermek yerine, bunları öngörmeli

ve önlemelidir.[7] Bu, gelişen tehditlerin önünde kalmak için YZ'nin öngörücü analitik ve sürekli öğrenme yeteneklerinden yararlanmayı içermektedir.[6]

Geleneksel, imza tabanlı savunmaların giderek yetersiz kalması, kuruluşları güvenlik duruşlarını temelden yeniden değerlendirmeye zorlamaktadır.[8] Bu, YZ destekli davranışsal analiz, sürekli izleme ve öngörücü modellere doğru stratejik bir kaymayı ifade etmektedir. YZ siber güvenlik pazarının 2024'te 30 milyar dolardan 2030'a kadar 134 milyar dolara çıkması beklenen yatırım projeksiyonu [8], bu stratejik değişimin ve YZ entegrasyonunun algılanan gerekliliğinin altını çizmektedir.

2025 ve Sonrası İçin Temel YZ Destekli Siber Güvenlik Teknikleri ve Trendleri

Bu bölümde, siber güvenlik ortamını şekillendiren en etkili YZ destekli teknikler detaylandırılmaktadır.

1. YZ Destekli Tehdit Tespiti ve Öngörücü Analitik

YZ destekli tehdit tespiti, büyük veri kümelerini (günlükler, ağ trafiği, kullanıcı davranışı) benzeri görülmemiş hızlarda analiz etmek için makine öğrenimi ve derin öğrenme algoritmalarını kullanır. Bu sayede, insan analistlerin veya geleneksel kural tabanlı sistemlerin gözden kaçırabileceği kalıpları, anormallikleri ve potansiyel ihlalleri belirleyerek proaktif savunmayı mümkün kılar. Bunun bir alt kümesi olan öngörücü analitik, geçmiş ve gerçek zamanlı verileri kullanarak saldırı vektörlerini ve güvenlik açıklarını ortaya çıkmadan önce tahmin eder.

YZ modelleri, hem geçmiş verilerden hem de gerçek zamanlı girdilerden sürekli olarak öğrenerek yeni ve gelişen tehditleri tahmin edebilmektedir.[7] Bu yetenek, güvenlik açığı penceresini önemli ölçüde daraltır ve önleyici eylemlere olanak tanıyarak hasarı en aza indirir.[3] Siber güvenliği reaktif bir duruştan öngörücü bir konuma taşımaktadır.

2025 yılında bu tekniklerin potansiyel etkileri ve uygulama alanları şunlardır:

- **Gerçek Zamanlı Tehdit Tespiti:** Karmaşık kalıpların ve anormalliklerin daha hızlı belirlenmesi, manuel müdahaleye olan bağımlılığı azaltır.[5]
- **Sıfır Gün Güvenlik Açığı Tespiti:** YZ, sistem davranışını ve kod anormalliklerini analiz ederek daha önce bilinmeyen güvenlik açıklarını tanımlayabilir.[8]
- **Polimorfik Kötü Amaçlı Yazılım Tespiti:** YZ modelleri, geleneksel imza tabanlı tespitten kaçınmak için kodunu sürekli değiştiren kötü amaçlı yazılımları tespit etmede üstündür.[9]
- **Kaynakların Optimizasyonu:** YZ, güvenlik açıklarını istismar edilmeden önce belirleyerek önleyici tedbirlerin önceliklendirilmesine ve kaynakların daha verimli

tahsis edilmesine yardımcı olur.[6]
- **Finans Sektörü:** Dolandırıcılık amaçlı işlemlerin gerçek zamanlı tespiti ve finansal ağlara yönelik potansiyel risklerin tahmini.[7]
- **Sağlık ve Kritik Altyapı:** Hassas hasta verilerinin korunması ve siber güvenlik açıkları için endüstriyel kontrol sistemlerinin izlenmesi.[7]

Geleneksel siber güvenlik, bilinen tehditlere karşı etkili olan imza tabanlı tespit yöntemlerine büyük ölçüde güvenmektedir; ancak, yeni veya polimorfik saldırılara karşı yetersiz kalmaktadır.[8] YZ'nin tehdit tespitinde yaygın olarak benimsenmesi ve özellikle "davranışsal analiz"e [8] verdiği önem, savunma felsefesinde temel bir değişime işaret etmektedir. YZ'nin "kullanıcıların ve sistemlerin tipik olarak nasıl davrandığını" öğrenme ve "şüpheli etkinlikleri" işaretleme yeteneği [8], güvenliğin statik kuralların ötesine, dinamik ve bağlama duyarlı izlemeye doğru ilerlediğini göstermektedir. Bu, geleneksel yöntemleri atlayabilen YZ tarafından üretilen tehditlerle mücadele etmek için hayati önem taşımaktadır.[4]

2. Güvenlik Operasyonları İçin Üretken YZ (Büyük Dil Modelleri, Doğal Dil İşleme)

Büyük Dil Modelleri (LLM'ler) ve Doğal Dil İşleme (NLP) dahil olmak üzere üretken YZ, karmaşık görevleri otomatikleştirerek, veri analizini geliştirerek ve iletişimi kolaylaştırarak güvenlik operasyonlarını dönüştürmektedir. Geniş veri kümelerinden insan benzeri metinleri anlama, üretme ve işleme yeteneği, kritik içgörüler sağlar ve olay yanıtını hızlandırır.

LLM'ler, güvenlik günlüklerini, olay raporlarını ve tehdit istihbaratı beslemelerini analiz ederek kalıpları ve anormallikleri belirleyebilir.[4] Ayrıntılı raporlar oluşturabilir, karmaşık verileri özetleyebilir [4] ve hatta sonraki adımları önererek vaka yönetiminde yardımcı olabilir.[10] NLP, dil kalıplarını analiz ederek kimlik avını tespit etmeye yardımcı olur.[4] Bu, manuel iş yükünü azaltır, verimliliği artırır ve yetersiz personel bulunan Güvenlik Operasyon Merkezi (SOC) ekiplerini güçlendirir.[10]

2025 yılında bu tekniklerin potansiyel etkileri ve uygulama alanları şunlardır:

- **Otomatik Rapor Yazma ve Özetleme:** SOC analistleri için vardiya değişiklikleri sırasında kapsamlı güncellemeler oluşturma veya karmaşık vakaları ve uyarıları özetleme.[5]
- **Kimlik Avı Tespiti ve Analizi:** Şüpheli e-postaları inceleme ve bir e-postanın neden kimlik avı girişimi olabileceğini açıklama.[10]
- **Gelişmiş Güvenlik Otomasyonu:** Otomasyon sistemlerine akıllı bir katman ekleyerek daha önce manuel olarak ele alınan görevleri kolaylaştırma.[10]
- **Analist Güçlendirmesi:** Rutin veri işleme ve içgörü oluşturmayı otomatikleştirerek

güvenlik analistlerinin daha üst düzey stratejik görevlere odaklanmasını sağlama.[10]
- **Tehdit Önceliklendirme:** LLM destekli SOAR platformları, tehditleri operasyonel ve kritik bağlama göre önceliklendirebilir.[11]

Siber güvenlik endüstrisi önemli bir yetenek açığıyla karşı karşıyadır, bu da analistlerin aşırı yüklenmesine ve yetersiz personel bulunan SOC'lara yol açmaktadır.[10] Üretken YZ, özellikle LLM'ler, rutin görevleri otomatikleştirerek, iş akışlarını kolaylaştırarak ve yanıt sürelerini hızlandırarak bu sorunu doğrudan ele almaktadır.[10] Bu, mevcut insan analistlerin "daha fazlasını, daha hızlı yapmasını" sağlayan ve hatta Tier 1 analistlerinin daha üst düzey analistler kadar verimli çalışmasına olanak tanıyan bir güç çarpanı görevi görmektedir.[10] Bu durum, YZ'nin işleri tamamen "değiştirmek" yerine, insan yeteneklerini "artırarak" mevcut iş gücünü daha etkili hale getireceğini ve potansiyel olarak tükenmişliği azaltacağını göstermektedir.

3. YZ Destekli Uç Nokta Güvenliği (EDR)

YZ destekli Uç Nokta Tespit ve Yanıt (EDR) çözümleri, uç nokta cihazlarını (dizüstü bilgisayarlar, cep telefonları, IoT cihazları) hedef alan tehditleri izlemek, tespit etmek ve bunlara yanıt vermek için makine öğrenimi ve akıllı algoritmaları entegre eder. Geleneksel imza tabanlı araçların aksine, YZ şüpheli etkinlikleri belirlemek için davranışsal analize odaklanır.

EDR'deki YZ, tipik kullanıcı ve sistem davranışlarını öğrenir. Bir cihaz bu normdan saparsa (örneğin, dosyaları şifreleme, olağandışı oturum açma, bilinmeyen IP'lerle iletişim kurma), YZ bunu anında işaretler.[8] Bu, enfekte cihazların anında izole edilmesini, şüpheli süreçlerin kapatılmasını veya kötü amaçlı faaliyetlerin insan müdahalesi olmadan engellenmesini sağlayarak yanıt sürelerini önemli ölçüde azaltır.[8]

2025 yılında bu tekniklerin potansiyel etkileri ve uygulama alanları şunlardır:

- **Gerçek Zamanlı Davranışsal Analiz:** Kullanıcı ve ağ davranışını izleyerek ihlalleri veya içeriden gelen tehditleri gösteren anormallikleri tespit etme.[5]
- **Otomatik Olay Yanıtı:** Etkilenen uç noktaları izole etme veya kötü amaçlı IP'leri engelleme gibi adımları otomatikleştirerek tehditlerin anında engellenmesi.[8]
- **Genişleyen Saldırı Yüzeyinin Korunması:** Uzaktan çalışma ortamları da dahil olmak üzere geleneksel ağ sınırları dışındaki artan sayıda cihazı güvence altına almak için kritik öneme sahiptir.[8]
- **Gelişmiş Tehditlerin Tespiti:** Gelişmiş kalıcı tehditlerin (APT'ler) ve dosyasız kötü amaçlı yazılımlar dahil olmak üzere sofistike fidye yazılımı saldırılarının gelişmiş tespiti.[9]
- **Sürekli Öğrenme:** YZ modelleri, gelişen tehditleri tanımak için gerçek zamanlı

olarak adapte olur ve savunmaları sürekli manuel güncellemelere gerek kalmadan keskin tutar.[8]

YZ destekli EDR'deki "sürekli öğrenme" kavramı [8], güvenlik çözümlerinin artık statik ürünler değil, dinamik, gelişen sistemler olduğu anlamına gelmektedir. Siber tehditler "daha karmaşık hale geldikçe" [8], önde kalmanın tek yolu, YZ'nin modellerini gerçek zamanlı olarak uyarlama yeteneği sayesinde "daha akıllı, daha hızlı ve daha proaktif savunma"dır.[8] Bu durum, makine öğrenimi tarafından yönlendirilen adaptasyonun, 2025'te etkili siber güvenlik için temel bir gereklilik haline geldiğini vurgulamaktadır.

4. Kimlik ve Erişim Yönetiminde (KİM) YZ

YZ, tehdit tespitini geliştirerek, insan ve insan olmayan varlıklar (YZ ajanları gibi) için kimlik yaşam döngüsü yönetimini kolaylaştırarak ve daha güvenli kimlik doğrulama yöntemlerinin benimsenmesini hızlandırarak KİM'i dönüştürmektedir. KİM'i geleneksel kural tabanlı sistemlerden daha akıllı, adaptif bir çerçeveye taşımaktadır.

YZ destekli Kimlik Tehdit Tespiti ve Yanıtı (ITDR), oturum açma davranışını izler, kullanıcı normlarını belirler ve geleneksel sistemlerin gözden kaçırabileceği anormallikleri (örneğin, ayrıcalık yükseltme, olağandışı coğrafi konum oturum açmaları) işaretler.[12] Ayrıca, 2025 yılına kadar kurumsal iş gücünün ayrılmaz bir parçası haline gelen cihazlar ve YZ ajanları ile ilişkili "insan olmayan" kimliklerin yönetimini de destekler.[2]

2025 yılında bu tekniklerin potansiyel etkileri ve uygulama alanları şunlardır:

- **YZ Destekli ITDR:** Kimlik tabanlı saldırıların (kimlik bilgisi doldurma, oturum ele geçirme) daha hızlı ve daha hassas tespiti, adım adım doğrulama veya erişim askıya alma gibi otomatik yanıtlarla birlikte.[12]
- **Parolasız Kimlik Doğrulama:** Parolaları biyometrik olarak güvenli genel-özel anahtar çiftleriyle değiştiren parolasız oturum açmaların (örneğin, geçiş anahtarları) hızlanması, saldırı yüzeyini önemli ölçüde azaltır ve kullanıcı deneyimini iyileştirir.[2]
- **YZ Ajanlarının Yönetimi:** Otonom YZ ajanları için gelişmiş izleme, otomatik kimlik yaşam döngüsü yönetimi (işe alım, yetki kaldırma) ve zaman sınırlı erişim kontrolleri (Tam Zamanında erişim) uygulama.[13]
- **Merkezi Olmayan Kimlik (DID):** Kullanıcılara kendi verileri üzerinde daha fazla kontrol sağlamak, merkezi sağlayıcılara olan bağımlılığı azaltmak ve gizliliği artırmak için kurumsal pilotlarda DID'in test edilmesi.[12]
- **Kimlik Kumaşı:** Parçalanmış KİM araçlarını hibrit ve çoklu bulut ortamlarında birleştirme, tutarlı politikalar uygulama ve kimlik etkinliğine gerçek zamanlı görünürlük sağlama.[12]

Geleneksel olarak, KİM insan kullanıcılara odaklanmıştır. Ancak, "insan olmayan" kimliklerin (cihazlar, sunucular, uygulamalar ve kritik olarak "ajan YZ" sistemleri) ortaya çıkışı [2], KİM'in kapsamını temelden genişletmektedir. Bu, yalnızca YZ'yi mevcut KİM'e uygulamakla ilgili değil, aynı zamanda KİM'in sofistike, adaptif kontroller gerektiren yeni bir dijital varlık kategorisine "uyum sağlaması" ile ilgilidir. YZ ajanlarının 2025 yılına kadar "kurumsal iş gücünün ayrılmaz üyeleri" olacağı tahmini [13], "erişim yayılımını" önlemek ve uygun yönetimi sağlamak için "geleneksel KİM yaklaşımlarının temelden yeniden düşünülmesini" [13] zorunlu kılmaktadır.

5. YZ Destekli Güvenlik Orkestrasyonu, Otomasyon ve Yanıt (SOAR)

YZ destekli SOAR platformları, çeşitli güvenlik araçlarını entegre eder, rutin iş akışlarını otomatikleştirir ve siber tehditlere koordineli yanıtları orkestre eder. Büyük Dil Modellerini (LLM'ler) dahil ederek, yeni nesil SOAR sistemleri akıllı, bağlama duyarlı ve sürekli öğrenme yeteneğine sahip hale gelir ve olay yanıtını dönüştürür.

YZ destekli SOAR platformları, etkilenen uç noktaların izole edilmesi veya kötü amaçlı IP'lerin engellenmesi gibi adımları otomatikleştirerek olay yanıtını kolaylaştırır ve kalış süresini önemli ölçüde azaltır.[9] LLM'ler, analistlerin sistemlerle doğal dil kullanarak etkileşim kurmasını, oyun kitapları oluşturmasını, uyarıları yorumlamasını, rapor taslakları hazırlamasını ve adaptif yanıtlar önermesini sağlar.[11] Bu, manuel kodlamayı azaltır, karar verme sürecini iyileştirir ve güvenlik ekiplerinin daha az kaynakla daha büyük ortamları yönetmesine olanak tanır.[9]

2025 yılında bu tekniklerin potansiyel etkileri ve uygulama alanları şunlardır:

- **Otomatik Oyun Kitabı Oluşturma:** Doğal dil açıklamalarına dayalı oyun kitapları oluşturma.[11]
- **Olay Özetleme ve Raporlama:** Olayları otomatik olarak özetleme ve teknik raporlar oluşturma, kaliteyi ve hızı iyileştirme.[10]
- **Tehdit Önceliklendirme:** Operasyonel ve kritik bağlama göre tehditleri önceliklendirme, uyarı yorgunluğunu azaltma.[9]
- **Adaptif Yanıt Önerileri:** MITRE ATT&CK gibi çerçevelere dayalı yanıtlar önerme.[11]
- **Ölçeklenebilirlik ve Verimlilik:** Orantılı personel artışı olmadan büyük ölçekli ortamları yönetme, Ortalama Araştırma Süresi'nde (MTTI) önemli azalmalar sağlama.[9]

LLM'lerin SOAR platformlarına entegrasyonu, doğal dil etkileşimi ve otomatik oyun kitabı oluşturma yeteneğiyle [11], gelişmiş güvenlik operasyonlarının "demokratikleşmesini" temsil etmektedir. Manuel kodlamaya ve karmaşık betik yazımına olan bağımlılığı azaltarak [11], bu sistemler, analistlerin sofistike görevleri yerine

getirmesi için teknik engeli düşürmektedir. Bu sadece güvenlik operasyonlarını daha verimli hale getirmekle kalmaz, aynı zamanda daha geniş bir güvenlik profesyoneli yelpazesinin etkili bir şekilde katkıda bulunmasına olanak tanıyarak yetenek açığını giderir ve daha az deneyimli analistleri güçlendirir.[10]

6. Derin Sahtecilik ve Gelişmiş Sosyal Mühendislik Savunması

Siber suçlular, son derece gerçekçi derin sahtecilikler (ses, video, metin) ve sofistike sosyal mühendislik kampanyaları oluşturmak için YZ'den giderek daha fazla yararlandıkça, geleneksel yöntemlerin ötesinde tutarsızlıkları tespit etmek ve davranışları doğrulamak için YZ destekli savunma mekanizmaları ortaya çıkmaktadır.

YZ, saldırganlar tarafından ikna edici kimlik avı e-postaları oluşturmak, gelişmiş keşif yapmak ve insan benzeri etkileşimleri simüle etmek için kullanılır.[1] Derin sahtecilikler, dolandırıcılık veya yanlış bilgi yaymak amacıyla yöneticileri taklit etmek için kullanılabilir.[3] Savunma amaçlı YZ çözümleri, bu sahtecilikleri tespit etmek için piksel kalıplarını, ses modülasyonunu, dudak senkronizasyonunu ve davranışsal tutarsızlıkları analiz eder.[9] Çok katmanlı kimlik doğrulama giderek daha kritik hale gelmektedir.[14]

2025 yılında bu tekniklerin potansiyel etkileri ve uygulama alanları şunlardır:

- **Derin Sahtecilik Tespiti:** YZ modelleri, YZ üretimi olduğunu gösteren ince tutarsızlıklar için ses, video ve metinleri analiz eder.[9]
- **Gelişmiş Kimlik Avı Tespiti:** Özellikle hiper kişiselleştirilmiş, YZ tarafından oluşturulan mesajlara karşı, e-postalardaki dil kalıplarını aldatma açısından analiz etme.[4]
- **Davranışsal Doğrulama:** Biyometrik doğrulamayı aşan çok faktörlü kimlik doğrulama tekniklerini dolandırıcılık davranışlarını tespit etmek için dahil etme.[9]
- **Güncellenmiş Kimlik Doğrulama Protokolleri:** Kimlik doğrulama süreçlerinde sesli, görüntülü ve metinsel aldatmaları hesaba katma.[14]

Sofistike derin sahteciliklerin ve YZ destekli sosyal mühendisliğin yükselişi [3] önemli bir etkiye sahiptir: dijital kimliğe olan güvenin aşınması. YZ, bir CEO'dan bir aile üyesine kadar herkesi ikna edici bir şekilde taklit edebilirse [3], dijital güvenin temeli sarsılır. Bu durum, görülen veya duyulan şeyin ötesine, yapılan ve nasıl yapıldığına odaklanan "çok katmanlı kimlik doğrulama" [14] ve davranışsal doğrulamaya [9] hızlı bir geçişi zorunlu kılmaktadır. Bir finans direktörü derin sahtecilik videosu nedeniyle kaybedilen 25 milyon dolar [3] bu etkinin çarpıcı bir örneğidir.

7. Kuantum Güvenli Güvenlik Planlaması

Henüz tam olarak gerçekleşmemiş olsa da, kuantum hesaplama mevcut kriptografik

standartlar için gelecekte bir tehdit oluşturmaktadır. Kuantum güvenli güvenlik planlaması, gelecekteki kuantum şifre çözme yeteneklerine karşı verileri korumak için proaktif önlemleri, özellikle kritik KİM sistemleri içinde, içermektedir.

Kuantum bilgisayarlar mevcut şifreleme algoritmalarını potansiyel olarak kırabilir.[1] "Şimdi topla, sonra şifre çöz" riski, bugün çalınan şifreli verilerin gelecekte şifresinin çözülebileceği anlamına gelmektedir.[12] Proaktif planlama, kuantum açısından savunmasız protokoller için KİM sistemlerinin denetlenmesini ve kriptografik geçişe, dahil olmak üzere kuantum sonrası kriptografi (PQC) standartlarının benimsenmesine hazırlanmayı içermektedir.[12]

2025 yılında bu tekniklerin potansiyel etkileri ve uygulama alanları şunlardır:

- **KİM Sistemi Denetimleri:** Kuantum saldırılarına karşı savunmasız olabilecek kriptografik bağımlılıkların (akıllı kartlar, SAML belirteçleri, OAuth, PKI sertifikaları) belirlenmesi.[12]
- **Kripto-Çevik Mimariler:** Minimum kesintiyle klasik ve kuantum sonrası algoritmalar arasında sorunsuz geçiş yapabilen sistemlerin uygulanması.[12]
- **PQC Standartlarına Uyum:** ABD hükümetinin Kuantum Hesaplama Siber Güvenlik Hazırlık Yasası gibi zorunluluklara hazırlanma.[12]
- **Uzun Vadeli Veri Koruma:** Onlarca yıl boyunca güvenli kalması gereken verilerin (örneğin, tıbbi kayıtlar, ulusal güvenlik verileri) gizliliğinin sağlanması.[1]

Kuantum hesaplamanın 2025 tartışmalarına dahil edilmesi [1], teknolojinin henüz "tam olarak gerçekleşmemiş" olmasına rağmen [1], siber güvenlik endüstrisinin "proaktif önlemlere" ve "geleceğe hazırlık"a olan bağlılığını vurgulamaktadır. "Şimdi topla, sonra şifre çöz" tehdidi [12], kuantum bilgisayarların gerçeğe dönüşmesini beklemenin çok geç olduğunu göstermektedir. Bu durum, kuruluşları kriptografik çeviklik ve PQC standartlarına *şimdi* yatırım yapmaya zorlamakta, acil tehditlerin ötesine geçerek veri gizliliğine yönelik uzun vadeli varoluşsal risklere karşı stratejik bir öngörü sergilemektedir.

Aşağıdaki tablo, 2025 yılı için temel YZ destekli siber güvenlik tekniklerini özetlemektedir:

Tablo 1: Temel YZ Destekli Siber Güvenlik Teknikleri (2025 Odaklı)

Teknik/Trend	Temel İşlev	2025'teki Temel	Birincil Uygulama	İlgili Kaynak Kimlikleri

		Faydaları	**Alanları**	
YZ Destekli Tehdit Tespiti ve Öngörücü Analitik	Gerçek zamanlı anomali tespiti, öngörücü tahmin	Daha hızlı tespit, azaltılmış yanlış pozitifler, proaktif savunma	Ağ güvenliği, uç nokta koruma, dolandırıcılık tespiti	3
Güvenlik Operasyonları İçin Üretken YZ (LLM'ler, NLP)	Otomatik görevler, gelişmiş veri analizi, raporlama	Azaltılmış manuel iş yükü, artan verimlilik, analist güçlendirmesi	SOC operasyonları, olay yanıtı, kimlik avı tespiti, raporlama	4
YZ Destekli Uç Nokta Güvenliği (EDR)	Davranışsal analiz, otomatik yanıt, sürekli öğrenme	Gerçek zamanlı tehdit engelleme, genişleyen saldırı yüzeyi koruması, gelişmiş APT tespiti	Dizüstü bilgisayarlar, mobil cihazlar, IoT cihazları, sunucular	5
Kimlik ve Erişim Yönetiminde (KİM) YZ	Kimlik tabanlı tehdit tespiti, kimlik yaşam döngüsü yönetimi	Daha hızlı ve hassas kimlik tehdidi yanıtı, gelişmiş kimlik doğrulama güvenliği, YZ ajanı yönetimi	Kimlik doğrulama, yetkilendirme, YZ ajanları, çoklu bulut ortamları	2
YZ Destekli Güvenlik Orkestrasyonu, Otomasyon ve Yanıt (SOAR)	İş akışı otomasyonu, olay yanıtı orkestrasyonu	Azaltılmış yanıt süreleri, artan ölçeklenebilirlik, uyarı yorgunluğunun azaltılması	Olay yönetimi, güvenlik operasyonları, tehdit önceliklendirme	9
Derin Sahtecilik ve Gelişmiş Sosyal Mühendislik Savunması	Sahtecilik tespiti, davranışsal doğrulama	Kimlik dolandırıcılığına karşı koruma, gelişmiş kimlik avı tespiti, güvenilir kimlik	Kimlik doğrulama, dolandırıcılık tespiti, iletişim güvenliği	3

		doğrulama		
Kuantum Güvenli Güvenlik Planlaması	Kriptografik denetim, kuantum sonrası kriptografi (PQC) geçişi	Gelecekteki şifre çözme risklerine karşı uzun vadeli veri koruma, düzenleyici uyum	Kriptografik sistemler, KİM altyapısı, uzun süreli veri depolama	[1]

Gelişen YZ Odaklı Tehditler ve Güvenlik Açıkları

YZ'nin siber güvenlik ortamına entegrasyonu, savunmacılar için yeni yetenekler sunarken, aynı zamanda saldırganlar için de yeni fırsatlar yaratmaktadır.

Saldırganların YZ'den Nasıl Yararlandığına Dair Analiz

Siber suçlular, saldırı stratejilerini otomatikleştirmek ve geliştirmek için YZ'yi giderek daha fazla kullanmakta, gerçek zamanlı olarak gelişen ve adapte olan tehditler oluşturmaktadır.[3] Bu, daha önce gelişmiş teknik beceriler gerektiren karmaşık görevlerin otomatikleştirilmesini içerir ve tehdit aktörleri için giriş engellerini düşürür.[4]

YZ, ikna edici kimlik avı kampanyaları oluşturmak için kullanılır, genellikle sosyal medyadan kişisel ayrıntıları dahil ederek gerçekçiliği artırır.[3] Derin sahtecilikler, kimlik dolandırıcılığı ve yanlış bilgi kampanyaları için kullanılır.[3] YZ, kötü amaçlı kod oluşturmak ve saldırı kampanyalarını optimize etmek için de kullanılır; örneğin, YZ tarafından oluşturulan DDoS modülleri ve fidye yazılımı grupları tarafından kullanılan özel ChatGPT tarzı sohbet robotları mevcuttur.[14] YZ ayrıca, çalınan verilerin (bilgi hırsızları, veri madencileri) hızla işlenmesinde ve temizlenmesinde kritik bir rol oynayarak para kazanmayı ve hedeflemeyi hızlandırır.[14] Saldırganlar, hedef ağlardaki güvenlik açıklarını hızla belirlemek için YZ destekli keşif araçlarını kullanır.[5]

Araştırmalar, YZ'nin saldırganlara "asimetrik bir avantaj" [15] sağladığını vurgulamaktadır; bu da onların sistemleri incelemesine, güvenlik açıklarını belirlemesine ve maksimum fayda sağlamak için saldırı zamanını ve yerini seçmesine olanak tanır. YZ'nin bu avantajı nasıl artırdığına dair detaylar, karmaşık görevleri otomatikleştirerek, "makine hızı ve ölçeğinde" saldırılara olanak tanıyarak ve daha az deneyimli tehdit aktörleri için "giriş engelini" düşürerek ortaya konmaktadır. Bu, YZ'nin saldırıları yalnızca tespit edilmesi "daha zor" hale getirmekle kalmayıp, aynı zamanda daha geniş bir kötü niyetli aktör yelpazesi için onları "daha sık" ve "daha erişilebilir" hale getirdiği anlamına gelir; bu da savunmacılar da YZ'yi benimsemedikçe güç dinamiğini temelden saldırgan lehine değiştirmektedir.

YZ'ye Özgü Güvenlik Açıklarının Tartışılması

YZ sistemleri, geleneksel yazılımlardan farklı bir şekilde veri işler ve birçok kuruluşun henüz yönetmeye hazır olmadığı benzersiz güvenlik açıkları sunar:

- **Düşmanca Girdiler:** YZ modellerini yanlış kararlar vermeye zorlamak, içerik filtrelerini atlamak veya dolandırıcılık tespit araçlarını devre dışı bırakmak için tasarlanmış kötü amaçlı girdiler.[6]
- **Veri Zehirlenmesi:** Bir modelin davranışını etkilemek için eğitim veri kümelerine kötü amaçlı veriler enjekte etme, arka kapılar, yanlış sınıflandırmalar veya azaltılmış doğrulukla sonuçlanma.[10] Bu, modern LLM'lerin gerçek zamanlı çevrimiçi bilgilere eriştiği "geri alma zehirlenmesini" de içerir.[14]
- **Model Tersine Çevirme ve Çıkarma:** Bir YZ modelini, eğitim verilerinden veya modelin kendisinden hassas bilgileri ortaya çıkarmak için sorgulama, potansiyel olarak özel verileri yeniden yapılandırma veya fikri mülkiyeti çalma.[16]
- **İstem Enjeksiyonu:** Üretken YZ sistemlerini, çıktıyı manipüle etmek veya veri sızdırmak için yasal kullanıcı istemleri olarak gizlenmiş zararlı talimatlar girerek hedefleme.[16]
- **Güvenli Olmayan API'ler ve Uç Noktalar:** YZ modellerine genellikle güçlü kimlik doğrulama, hız sınırlama veya izleme eksikliği olan açık API'ler aracılığıyla erişilir, bu da onları ele geçirme veya yük enjeksiyonuna karşı savunmasız hale getirir.[16]
- **Şeffaflık Eksikliği ("Kara Kutular"):** Birçok YZ modeli "kara kutu" olarak çalışır, bu da karar verme süreçlerini anlamayı veya açıklamayı zorlaştırır ve risk yönetimini karmaşıklaştırır.[16]
- **Karmaşıklık ve Dinamik Saldırı Yüzeyi:** YZ modelleri karmaşıktır, gelişen veri ve mantık katmanları üzerine kuruludur ve büyük ve dinamik bir saldırı yüzeyi oluşturur.[16]
- **Standartlaştırılmış Güvenlik Uygulamalarının Eksikliği:** YZ geliştirme genellikle yönetim ve politika çerçevelerini geride bırakır ve geleneksel sistemlere kıyasla güvenlik açıklarına yol açar.[16]

Raporun büyük bir kısmı "YZ ile Güvenlik" (savunma için YZ kullanma) üzerine odaklanırken, YZ'ye özgü güvenlik açıklarının ayrıntılı listesi [10], "YZ'nin Güvenliği"ne olan eşit derecede kritik ihtiyacı vurgulamaktadır. Bu, kuruluşların yalnızca savunma için YZ dağıtmakla kalmayıp, aynı zamanda YZ sistemlerinin kendilerini de güvence altına alması gerektiği anlamına gelmektedir. Bu ikili zorluk, özel savunmalar [6], sağlam yönetim çerçeveleri [6] ve kendi YZ modellerine karşı YZ destekli saldırıları belirleme ve simüle etmeye yönelik proaktif bir yaklaşım gerektirmektedir.[6] Siber güvenlik profesyonellerinin %74'ünün YZ destekli tehditleri önemli bir zorluk olarak görmesi [16] bu karmaşıklığın altını çizmektedir.

Aşağıdaki tablo, YZ odaklı tehditleri ve bunlara karşılık gelen savunma stratejilerini detaylandırmaktadır:

Tablo 2: YZ Odaklı Tehditler ve Karşılık Gelen Savunma Stratejileri

YZ Odaklı Tehdit/Güvenlik Açığı	Saldırganlar YZ'yi Nasıl Kullanır?	Karşılık Gelen YZ Destekli Savunma Stratejisi	İlgili Kaynak Kimlikleri
Derin Sahtecilik Saldırıları	Dolandırıcılık için gerçekçi taklit, yanlış bilgi yayma	Davranışsal doğrulama, çok katmanlı kimlik doğrulama, ses/video analizi	3
Gelişmiş Sosyal Mühendislik	Kişiselleştirilmiş kimlik avı, insan benzeri etkileşim simülasyonu	Gelişmiş kimlik avı tespiti (dil analizi), davranışsal doğrulama	4
YZ Tarafından Oluşturulan Kötü Amaçlı Yazılım	Kötü amaçlı kod üretimi, saldırı kampanyalarını optimize etme	YZ destekli tehdit tespiti, polimorfik kötü amaçlı yazılım tespiti	9
Veri Zehirlenmesi	Eğitim veri kümelerine kötü amaçlı veri enjekte etme	Düşmanca eğitim, YZ davranışının sürekli izlenmesi, veri doğrulama	10
Düşmanca Girdiler	YZ modellerini yanlış kararlar vermeye zorlama	Düşmanca eğitim, YZ davranışının gerçek zamanlı izlenmesi	6
Model Tersine Çevirme ve Çıkarma	Eğitim verilerinden veya modelin kendisinden hassas bilgileri ortaya çıkarma	Modellere ve verilere güvenli erişim, güvenlik açığı testi	16
İstem Enjeksiyonu	Üretken YZ sistemlerini zararlı	YZ davranışının izlenmesi, YZ'ye özgü	16

	talimatlarla manipüle etme	sızma testi	
Güvenli Olmayan API'ler ve Uç Noktalar	Zayıf kimlik doğrulama veya izleme eksikliği olan API'leri istismar etme	Modellere ve verilere güvenli erişim, çok faktörlü kimlik doğrulama, düzenli denetim	[16]

YZ Benimsenmesi ve Savunma İçin Stratejik Öneriler

YZ'nin siber güvenlik ortamında artan rolü göz önüne alındığında, kuruluşların proaktif ve stratejik bir yaklaşım benimsemesi zorunludur.

Sağlam YZ Yönetim Çerçeveleri Oluşturma

YZ kullanımı için gizlilik, uyumluluk ve etik hususları ele alan açık politikalar geliştirilmelidir.[6] YZ riskine yönelik gözetim ve hesap verebilirliği sağlayarak YZ yönetimini genel güvenlik stratejilerine entegre etmek önemlidir.[16] Ayrıca, benimseme oranları, doğruluk ve operasyonel verimlilik gibi temel metriklerle YZ olgunluğunun izlenmesi, sürekli iyileştirme için kritik öneme sahiptir.[6]

NIST Yapay Zeka Risk Yönetimi Çerçevesi ve Google'ın Güvenli YZ Çerçeveleri gibi çerçevelerin [3] ve "Düzenleyici ve Etik Hususlar"ın [16] açıkça tartışılması, YZ benimsenmesinin yalnızca teknik bir zorluk değil, aynı zamanda düzenleyici bir zorluk olduğunu göstermektedir. AB YZ Yasası ve GDPR gibi düzenlemeler [16], resmi yönetim ihtiyacını artırmaktadır. Bu, kuruluşların yalnızca teknik uygulamaya odaklanmakla kalmayıp, aynı zamanda veri gizliliğini, açıklanabilirliği ve YZ sistemlerinde hesap verebilirliği sağlayarak yasal ve etik uyumluluğa da odaklanması gerektiği anlamına gelir; bu da cezaları önlemek ve güveni sürdürmek için önemlidir.

YZ Farkında Savunma Mekanizmaları Uygulama

Gelişen YZ odaklı tehditlere karşı koymak için YZ destekli savunma çözümlerinin proaktif olarak benimsenmesi gerekmektedir.[5] YZ tarafından oluşturulan eserleri tanımlayabilen YZ destekli tespit ve tehdit istihbarat sistemlerinden yararlanılmalıdır.[14] Kimlik doğrulama protokolleri, sesli, görüntülü ve metinsel aldatmaları hesaba katacak şekilde güncellenmelidir.[14] YZ modellerini manipülasyona karşı daha dirençli hale getirmek için düşmanca eğitim kullanılmalıdır.[16] Son olarak, olağandışı çıktılar veya yetkisiz istem yanıtlarını tespit etmek için YZ davranışının gerçek zamanlı olarak izlenmesi önemlidir.[16]

"YZ farkında savunmalar" [14] ve YZ'ye özgü güvenlik açıklarına karşı "özel savunmalar" [6] üzerindeki sürekli vurgu, geleneksel güvenlik kontrollerinin yetersiz olduğunu göstermektedir. Bu, kuruluşların mevcut güvenlik araçlarında YZ'yi kullanmanın ötesine geçerek, YZ tarafından oluşturulan tehditleri ve YZ sistemlerindeki güvenlik açıklarını anlamak, tespit etmek ve bunlara yanıt vermek için baştan sona tasarlanmış "YZ-yerel" güvenlik stratejileri geliştirmesi gerektiği anlamına gelir. Bu, YZ'nin iç işleyişi ve saldırı vektörleri hakkında daha derin bir anlayış gerektirmektedir.

Güvenlik Operasyonlarında İnsan-YZ İşbirliğini Teşvik Etme

YZ rutin görevleri yerine getirebilir ve büyük miktarda veriyi analiz edebilirken, stratejik kararlar için insan sezgisi ve uzmanlığı kritik önemini korumaktadır.[3] YZ'nin insan yeteneklerini tamamen değiştirmek yerine, özellikle Güvenlik Operasyonları (SecOps) ve SOC iş akışlarında insan yeteneklerini artırmak için kullanılması önemlidir.[2] YZ teknolojisini insan uzmanlığıyla birleştiren Yönetilen Tespit ve Yanıt (MDR) hizmetlerinin uygulanması, gelişmiş dayanıklılık sağlar.[3]

YZ'nin "insan yeteneklerini artıracağı" ve "siber güvenlik işlerini tamamen değiştirmeyeceği" [2] yönündeki tutarlı mesaj, güvenlik profesyonelinin rolünün önemli bir evrimine işaret etmektedir. Analistler, "günlük sıkıcı ve tekrarlayan görevler"le boğuşmak yerine, "daha üst düzey stratejik girişimlere ve karmaşık problem çözmeye" odaklanmakta özgürleşeceklerdir.[10] Bu, analistlerin üretken YZ ile etkili bir şekilde etkileşim kurmak için yeni becerilere sahip olmalarını [11] ve stratejik iş ortakları olarak işlev görmelerini gerektirmektedir.[1]

Proaktif Tehdit Avcılığı ve Sürekli İzleme

Reaktif bir yaklaşımdan proaktif tehdit avcılığına geçiş yapılmalı, YZ kullanılarak potansiyel saldırıların zarar vermeden önce tahmin edilmesi ve önlenmesi sağlanmalıdır.[3] Gerçek zamanlı tespit ve otomatik yanıt için YZ destekli sürekli izleme çözümleri uygulanmalıdır.[5] Son olarak, savunma açıklarını belirlemek için YZ odaklı tehditlerin (örneğin, derin sahtecilik kimlik avı, adaptif kötü amaçlı yazılım) düzenli simülasyonları yapılmalıdır.[6]

Sonuç: YZ Merkezli Bir Siber Güvenlik Geleceğine Hazırlanmak

2025 ve sonrası için siber güvenlik duruşunu geliştirmek amacıyla YZ vazgeçilmez bir araçtır. Kuruluşlar, giderek daha sofistike ve gelişen siber tehditlere karşı savunma yapmak için gelişmiş tehdit tespiti, otomatik yanıt ve akıllı kimlik yönetimi için YZ destekli çözümleri benimsemelidir.

YZ büyük avantajlar sunarken, benimsenmesi özel yönetim, YZ farkında savunmalar ve

sürekli uyanıklık gerektiren benzersiz riskler ve güvenlik açıkları da beraberinde getirmektedir. Bilgili kalmak, adaptif YZ teknolojilerine yatırım yapmak, insan-YZ sinerjisini teşvik etmek ve sağlam yönetim çerçeveleri oluşturmak, dinamik, YZ odaklı siber güvenlik ortamında güvenli bir duruşu sürdürmek için temel adımlardır.

Alıntılanan çalışmalar

1. RSA Conference 2025: A Barometer for Cybersecurity's Future | TFiR, erişim tarihi Haziran 5, 2025, https://tfir.io/rsa-conference-2025-a-barometer-for-cybersecuritys-future/
2. RSA Conference 2025: Emerging Trends and Key Insights ..., erişim tarihi Haziran 5, 2025, https://www.whoisxmlapi.com/blog/rsa-conference-2025-emerging-trends-and-key-insights
3. The future of cyber security and AI in 2025 - Grey Matter, erişim tarihi Haziran 5, 2025, https://greymatter.com/content-hub/the-future-of-cyber-security-and-ai-in-2025/
4. Why Artificial Intelligence is the Future of Cybersecurity - Darktrace, erişim tarihi Haziran 5, 2025, https://www.darktrace.com/blog/why-artificial-intelligence-is-the-future-of-cybersecurity
5. AI-Driven Cybersecurity Threats in 2025 | Netrix Global - Netrix, LLC, erişim tarihi Haziran 5, 2025, https://netrixglobal.com/blog/cybersecurity/ai-driven-cyber-threats-what-to-expect-in-2025/
6. AI Considerations for 2025: Preparing for the Future of ... - Optiv, erişim tarihi Haziran 5, 2025, https://www.optiv.com/insights/discover/blog/ai-trends-in-cybersecurity
7. (PDF) Predictive Analytics in Cybersecurity: Using AI to Prevent ..., erişim tarihi Haziran 5, 2025, https://www.researchgate.net/publication/387371545_Predictive_Analytics_in_Cybersecurity_Using_AI_to_Prevent_Threats_Before_They_Occur
8. How AI Is Transforming Endpoint Security In 2025 | Cyble, erişim tarihi Haziran 5, 2025, https://cyble.com/knowledge-hub/how-ai-is-transforming-endpoint-security/
9. Emerging AI Trends in Cybersecurity: A Guide for 2025, erişim tarihi Haziran 5, 2025, https://overturepartners.com/it-staffing-resources/emerging-ai-trends-in-cybersecurity
10. How Can Generative AI be Used in Cybersecurity - Swimlane, erişim tarihi Haziran 5, 2025, https://swimlane.com/blog/how-can-generative-ai-be-used-in-cybersecurity/
11. Next-Gen SOAR with AI: redefining Cyber Security orchestration, erişim tarihi Haziran 5, 2025,

https://telefonicatech.com/en/blog/next-gen-soar-with-ai-redefining-cyber-security-orchestration
12. 5 IAM Trends to Watch in 2025 - ID Dataweb, erişim tarihi Haziran 5, 2025, https://www.iddataweb.com/iam-trends-2025/
13. Identity and Access Management in the AI Era: 2025 Guide | Identity ..., erişim tarihi Haziran 5, 2025, https://www.idsalliance.org/blog/identity-and-access-management-in-the-ai-era-2025-guide/
14. AI Security Report 2025: Understanding threats and building smarter ..., erişim tarihi Haziran 5, 2025, https://blog.checkpoint.com/research/ai-security-report-2025-understanding-threats-and-building-smarter-defenses/
15. 11th ACM Workshop on Adaptive and Autonomous Cyber Defense (AACD 2024), erişim tarihi Haziran 5, 2025, https://aacd24.github.io/
16. Understanding the Biggest AI Security Vulnerabilities of 2025 ..., erişim tarihi Haziran 5, 2025, https://www.blackfog.com/understanding-the-biggest-ai-security-vulnerabilities-of-2025/