Siber Güvenlik ve Üretken Yapay Zeka

Tehdit Tespitinden Otomatik Müdahaleye:
Kurumsal Güvenlik Operasyonlarını Yeniden Şekillendiren Dört Kullanım Alanı

9 Temmuz 2026

Özet

Siber tehditlerin hacmi, hızı ve karmaşıklığı, geleneksel kural tabanlı güvenlik sistemlerinin kapasitesini artık aşıyor. Güvenlik ekipleri; sınırlı personelle giderek büyüyen log hacimlerini, uyarı yorgunluğunu ve daha önce görülmemiş saldırı biçimlerini yönetmek zorunda kalıyor.

Üretken yapay zeka (Generative AI), bu tabloyu değiştiren bir yetenek katmanı sunuyor. Büyük dil modelleri, güvenlik operasyonlarının dört kritik alanına doğrudan katkı sağlıyor: **Tehdit tespiti** ve **analizi**, **otomatik olay müdahalesi**, **güvenlik kodu üretimi** ve **incelemesi**, **oltalama ile saldırı simülasyonu**. Aynı zamanda bu teknoloji saldırganların elinde de gelişiyor; bu nedenle sorumlu ve insan gözetimli bir uygulama yaklaşımı zorunludur.

Dorabase'in bulut güvenlik altyapısı, bu dört kullanım alanını kurumsal ölçekte uygulanabilir kılacak şekilde tasarlanmıştır: **Davranışsal analiz destekli WAF** ve **bot koruma katmanları**, **7/24 izleme** ve **yönetilen güvenlik hizmetleri**, **DevOps süreçlerine entegre API desteği**.

Temel Çıkarım: Güvenlik operasyonlarında yapay zekayı yoğun şekilde kullanan kuruluşlar, ihlalleri ortalama 100 güne yakın daha hızlı tespit ediyor ve milyonlarca dolarlık maliyet tasarrufu sağlıyor.

Genişleyen Tehdit Yüzeyi

Kurumsal ortamlarda üretilen güvenlik verisinin hacmi, insan analistlerin manuel olarak işleyebileceği ölçeği çok geride bıraktı. Akademik literatür, büyük dil modellerinin (LLM) bu ölçek sorununu çözmede somut bir rol oynadığını gösteriyor: Ağ verilerinin gerçek zamanlı analizi, kötü amaçlı yazılım ile oltalama girişimlerinin örüntü tanıma yoluyla tespiti ve olay anında hızlı durum değerlendirmesi bu alanların başında geliyor.

IBM'in kapsamlı ihlal maliyeti araştırması, bu akademik bulguları operasyonel verilerle destekliyor. Güvenlik ekiplerinde yapay zeka ve otomasyonu yoğun şekilde kullanan kuruluşlar, ihlalleri tespit edip durdurma sürecini önemli ölçüde kısaltıyor ve bu kuruluşlarda ortalama ihlal maliyeti, yapay zeka kullanmayan kuruluşlara kıyasla **milyonlarca dolar daha düşük** seyrediyor. Buna karşın, **oltalama** ve **çalıntı kimlik bilgileri kaynaklı ihlaller** hâlâ en uzun **tespit süresine** ve **en yüksek maliyete** sahip kategoriler arasında yer alıyor.

Bu tablo, kurumların güvenlik stratejilerini yalnızca önleyici kontrollerle sınırlamayıp, tespit ve müdahale süreçlerine de yapay zeka destekli otomasyonu dahil etmesini gerekli kılıyor.

Dört Kullanım Alanı

Güvenlik literatürü ve endüstri verileri, üretken yapay zekanın kurumsal güvenlik operasyonlarına katkısını dört ana başlıkta topluyor. Aşağıdaki bölümler her birini akademik kaynaklarla ve Dorabase'in altyapı yaklaşımıyla birlikte ele alıyor.

1. Tehdit Tespiti ve Analizi

Büyük dil modelleri, ağ trafiği, sistem günlükleri ve kullanıcı davranışına ait büyük hacimli veriyi gerçek zamanlı analiz ederek kötü amaçlı yazılım, oltalama girişimi ve olağandışı trafik örüntülerini tespit edebiliyor. Kural tabanlı sistemlerin aksine, bu modeller normal davranışın bir temel çizgisini öğrenerek imzası önceden tanımlanmamış tehditleri de yakalayabiliyor.

- Log ve ağ verisinin ölçekte, gerçek zamanlı korelasyonu
- Bilinen imzalara bağlı kalmadan anomali tabanlı tespit
- Davranışsal temel çizgiden sapmaların erken uyarıya dönüştürülmesi

Dorabase'in **WAF**, **bot koruma** ve **DDoS koruma** katmanları, bu tür davranışsal analiz yeteneklerini **CDN altyapısıyla** birlikte **tek bir güvenlik çevresi** içinde birleştirir.

2. Otomatik Olay Müdahalesi

Bir güvenlik olayı sırasında zaman kritik bir kaynaktır. Üretken yapay zeka modelleri, olay verisini özetleyerek analistlere hızlı durum değerlendirmesi sağlıyor, olası müdahale adımlarını önceliklendiriyor ve tekrarlayan sınıflandırma ile containment görevlerini otomatikleştirebiliyor.

- Olay özetleme ve kök neden analizine hızlı erişim
- Uyarıların otomatik sınıflandırılması ve önceliklendirilmesi
- Rutin, önleme adımlarının otomasyonla hızlandırılması

Bu yaklaşım operasyonel veride de karşılığını buluyor: güvenlik otomasyonunu yoğun kullanan kuruluşlarda ihlal tespit ve durdurma süresi ciddi oranda kısalıyor. Dorabase'in **7/24 izleme** ve **yönetilen hizmetler ekibi**, bu otomasyon katmanını sürekli insan gözetimiyle destekler.

Temel Çıkarım: Otomasyon, insan analistin yerini almaz; tekrarlayan görevleri üstlenerek ekibin karmaşık tehditlere odaklanmasını sağlar.

3. Güvenlik Kodu Üretimi ve İncelemesi

Güvenlik ekipleri için bir diğer kritik kullanım alanı, yazılım geliştirme sürecinin güvenliğidir. Üretken yapay zeka, kod tabanlarını tarayarak potansiyel güvenlik açıklarını işaretleyebiliyor, düzeltme önerileri sunabiliyor ve güvenli kod geliştirme pratiklerinin otomasyonuna katkı sağlıyor. Bu, özellikle yama yönetimi ve uyumluluk kontrolleri gibi tekrar eden görevlerde belirgin verimlilik kazancı sunuyor.

- Kod tabanında otomatik güvenlik açığı taraması
- Yama önceliklendirmesi ve düzeltme önerileri
- CI/CD hattına entegre sürekli güvenlik kontrolü

Dorabase'in **API** destekli entegrasyon yaklaşımı, bu tür güvenlik kontrollerinin DevOps iş akışına minimum sürtünmeyle yerleşmesini sağlar.

4. Oltalama(Phishing) ve Saldırı Simülasyonu

Oltalama, kurumların en sık karşılaştığı ve en maliyetli tehdit kategorilerinden biri olmayı sürdürüyor. Üretken yapay zeka modelleri, e-posta metnini gönderen davranışı, dil tonu ve alan adı yapısı gibi çok boyutlu sinyallerle analiz ederek önceden tanımlanmış kurallara bağlı kalmadan hem yaygın hem de hedefli saldırıları işaretleyebiliyor.

Aynı teknoloji, güvenlik ekiplerinin savunmalarını kontrollü bir ortamda test etmesine de imkan tanıyor: gerçekçi saldırı senaryoları ve sentetik oltalama örnekleri üreterek red-teaming ve çalışan farkındalık eğitimlerini güçlendiriyor.

- Gönderen davranışı ve mesaj yapısının çok boyutlu analizi
- Sentetik oltalama senaryolarıyla farkındalık eğitimi
- Kontrollü ortamda saldırı simülasyonu ve savunma testi

Endüstri verileri bu alanın önceliğini doğruluyor: Oltalama ve çalıntı kimlik bilgisi kaynaklı ihlaller, tüm kategoriler arasında en uzun tespit süresine ve en yüksek maliyet etkisine sahip.

Aynı Teknoloji, İki Taraflı Bir Araç

Üretken yapay zekanın savunma tarafına sağladığı her yetenek, saldırganlar için de bir fırsat penceresi açıyor. Akademik literatür, saldırganların bu modelleri daha **ikna edici oltalama** içeriği üretmek, **kötü amaçlı kod otomasyonu** geliştirmek ve **savunma modellerini prompt injection** veya **veri zehirlenmesi** gibi tekniklerle manipüle etmek için kullanabildiğini gösteriyor.

Bu ikili doğa, güvenlik stratejisinin iki temel ilkeye bağlı kalmasını gerektiriyor: otomasyonun her aşamasında insan gözetiminin korunması ve modellerin kendisinin de bir güvenlik varlığı olarak değerlendirilip izlenmesi. Dorabase'in yönetilen hizmetler yaklaşımı, teknolojiyi tek başına bırakmak yerine yerel uzman desteğiyle birlikte sunar.

Temel Çıkarım: Otomasyonu artırmak, gözetimi azaltmak anlamına gelmemelidir. En dayanıklı güvenlik stratejileri, ikisini birlikte ölçekler.

Güvenlik Operasyonlarınızı Yeniden Şekillendirme

Tehdit tespiti, olay müdahalesi, güvenli kod incelemesi ve saldırı simülasyonu alanlarında üretken yapay zekadan yararlanmak, artık rekabetçi bir avantajdan çok operasyonel bir gereklilik haline geldi. Bu dönüşümün getirisi, doğru altyapı ve doğru insan gözetimiyle birleştiğinde ortaya çıkıyor.

Dorabase, **CDN**, **bulut güvenliği** ve **yönetilen hizmetler portföyüyle**, bu dört kullanım alanını kurumunuzun mevcut altyapısına minimum sürtünmeyle entegre eder. Yerel uzman ekibimiz, teknolojiyi otomasyonla sınırlamaz; her aşamada gözetim ve danışmanlık sağlar.

Kaynakça

1.Ferrag,M.A., Alwahedi, F., Battah, A., Cherif, B., Mechri, A., Tihanyi, N., Bisztray, T., Debbah, M. (2024). Generative AI in Cybersecurity: A Comprehensive Review of LLM Applications and Vulnerabilities. https://arxiv.org/abs/2405.12750

2. Sai, S., Yashvardhan, U., Chamola, V., Sikdar, B. (2024). Generative AI for Cyber Security: Analyzing the Potential of ChatGPT, DALL-E, and Other Models for Enhancing the Security Space. IEEE Access, 12, 53497- 53516. https://ieeexplore.ieee.org/document/10491270

3. Radanliev, P., Santos, O., Ani, U.D. (2025). Generative AI Cybersecurity and Resilience. Frontiers in Artificial Intelligence. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC12171450/

4. IBM (2024-2025). Cost of a Data Breach Report. https://www.ibm.com/reports/data-breach