Siber Güvenlikte Yapay Zekanın Rolü

Burcu Yarar

13.07.2024

#brcyrr

- Passionate Cyber Security Expert
- Ethical Hacker & Pentester & Application Security Team Lead at VakıfBank

- OSCP | OSWP | eWPTXv2 | eMAPT | CEH | CASE.NET | CTIA

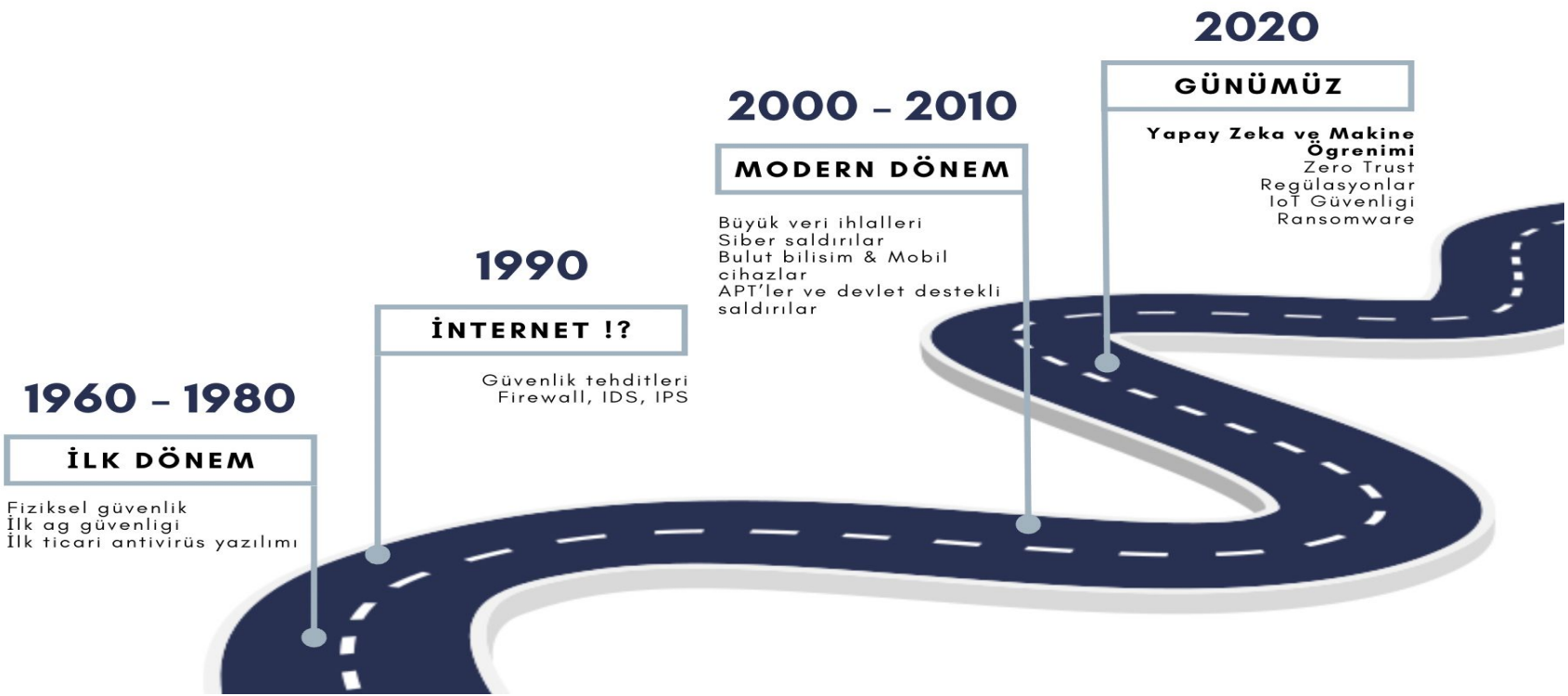
#içindekiler

- siber güvenlik!?
- siber dünya
- siber güvenlikte yapay zeka!?
- problemler & çözümler
- artıları & eksileri
- gelecek trendler
- kariyerimize katkıları
- faydalı kaynaklar & profiller

#siber güvenlik!?

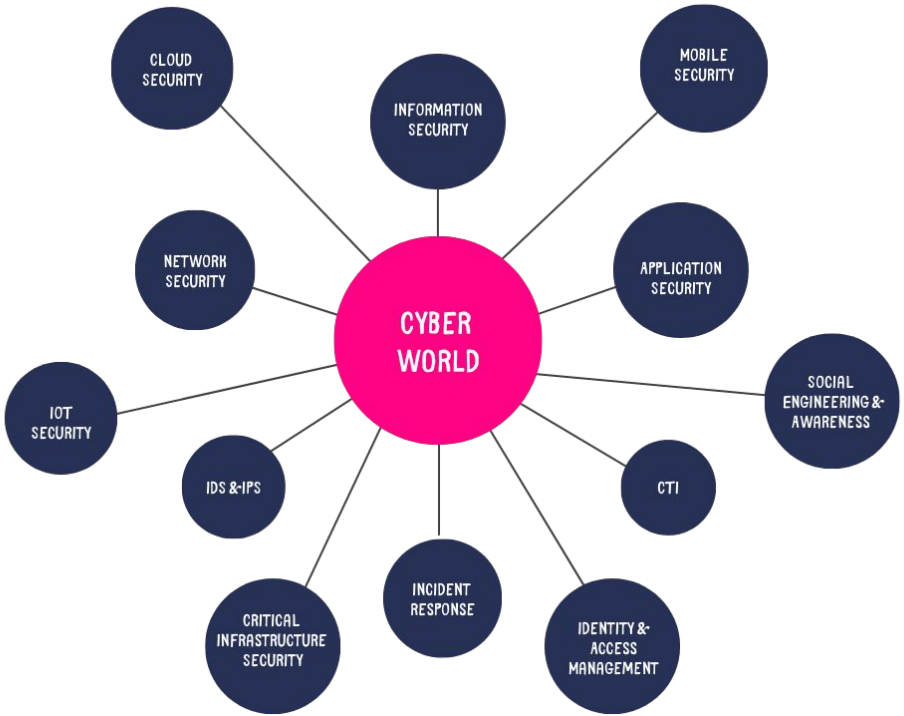
- Bilgisayar sistemleri, ağlar ve verilerin; yetkisiz erişim, saldırı ve hasarlardan korunmasını sağlayan uygulama, teknoloji ve süreçler bütünüdür.

#siber güvenlik!?



#siber dünya

- Siber Güvenlik
- Bilgi Güvenliği
- BT Güvenlik



#siber güvenlikte yapay zeka!?

- Hızlı ve gelişmiş tehdit tespiti
- Otomasyon
- Verimlilik
- Tehdit istihbaratı
- Anomali tespiti

#Problem 1 - Oltalama Saldırıları

- Kurumlara gerçekleştirilen başarılı saldırıların **%91** oltalama e-postaları
- Karmaşık bir oltalama e-postasını farkedemeyenlerin oranı **%25**
- Oltalama e-postalarını farkedip yönetimlerini bilgilendirenlerin oranı **%17**
- Siber suçların ve veri sızıntılarının sektörlere göre toplam maliyetinin 2024 öngörüsü **9.5** trilyon dolar

*** İstatistikler dünya genelidir.

#Çözüm 1 - Oltalama Saldırıları

- E-posta filtreleme ve sınıflandırma

  “Google gibi kuruluşlar, kimlik avı e-postalarının %99,9'unu engellediği bildirilen yapay zeka odaklı spam filtreleri uyguladı.”

- Davranış analizi
- Gerçek zamanlı tehdit istihbaratı
- Kullanıcı eğitimi ve simülasyonu

#Problem 2 - Kaynak Kod Analizi

F/P Oranının Fazla Olması

- Kaynak kod analizi esnasında, güvenlik açıklıklarını tespit etmek genellikle karmaşık bir süreçtir. Statik kod analiz araçları bu aşamada yardımcı olur ancak F/P bulgu oranı fazladır.

- F/P bulgular, analiz sürecinin verimliliğini azaltır ve güvenlik uzmanlarının gerçek açıklıklara odaklanmasını zorlaştırır.

#Çözüm 2 - Kaynak Kod Analizi

F/P Oranının Fazla Olması

- ML ile güvenlik açığı tespiti
- F/P oranının azaltılması için AI kullanımı
- Dinamik ve statik analiz sürecinin birleştirilmesi
- Kendi kendine öğrenme ve gelişim

#Problem 3 - Pentest & Vulnerability Scanning

Verimlilik ve Kapsam

- Geleneksel sızma testleri zaman alıcı olabilir ve genellikle insan kısıtlamaları nedeniyle kapsamı sınırlı olabilir.

- Manuel sızma testleri esnasında bazı güvenlik açıklıkları gözden kaçırılabilir ve çoğu zaman sürekli olarak gerçekleştirilemez.

#Çözüm 3 - Pentest & Vulnerability Scanning

Verimlilik ve Kapsam

- Otomatize edilmiş güvenlik açığı taramaları
- Akıllı istismar tespiti

Sonuç;

- Artan verimlilik
- Geniş ve Güncel Kapsam
- Sürekli İyileştirme

#Problem 4 - Zafiyet Yönetimi

Zafiyet Yönetiminde Önceliklendirme ve Etkili Müdahale

- Geleneksel yöntemler, kritik zafiyetlerin önceliklendirme sürecinde sınırlı veri ve analiz kapasitesine dayanarak, zafiyetlerin etkisini ve riskini tam olarak değerlendiremeyebilir.

- Bu durum, kaynakların yetersiz kullanılmasına ve kritik zafiyetlerin gözden kaçırılmasına neden olabilir.

#Çözüm 4 - Zafiyet Yönetimi

Zafiyet Yönetiminde Önceliklendirme ve Etkili Müdahale

- Risk ve etki analizi
- Önceliklendirme ve sınıflandırma
- Dinamik tehdit verileri ile entegrasyon
- Otomatik çözüm önerileri ve rehberlik
- Sürekli öğrenme ve adaptasyon

#artıları & eksileri

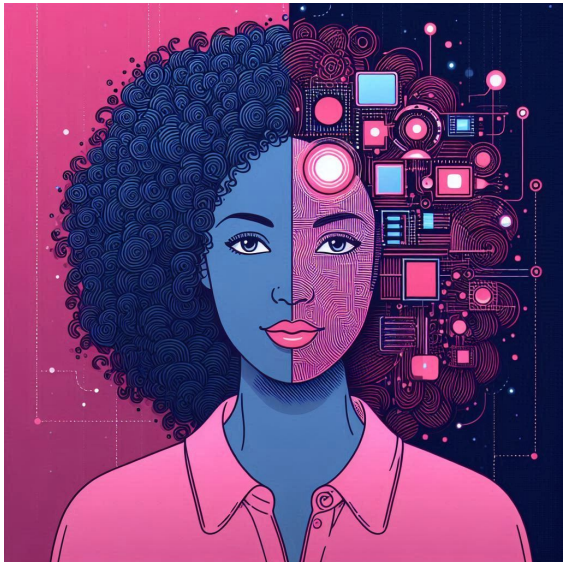
ARTILARI	EKSİLERİ
Gelişmiş tehdit tespiti	F/P'ler ve F/N'ler
Otomasyon ve verimlilik	Eğitim ve veri ihtiyacı
F/P oranının azalması	Yapay zeka saldırıları
Gelişmiş analitik yetenekler	Yüksek maliyet
Sürekli öğrenme ve adaptasyon	Gizlilik, güvenlik ve etik sorunlar

#gelecek trendler

- AI tabanlı tehdit tespit sistemlerinin pazar büyüklüğünün **10** milyar doları aşması
- Otonom güvenlik çözümlerinin siber güvenlik pazarındaki payının **%30**'a çıkması
- Davranışsal analiz pazarının **2.5** milyar doları aşması
- Kötü amaçlı yazılım analizi pazarının **4.5** milyar doları aşması
- Veri gizliliği teknolojilerinin pazarının **3** milyar doları aşması
- Güvenlik eğitim araçlarının pazar büyüklüğünün **2** milyar doları aşması

#kariyerimize katkıları !?

- Zaman yönetimi
- Verimlilik ve üretkenlik
- Daha iyi karar verme
- Yeni beceri ve bilgi kazanımı
- Kullanıcı deneyimini iyileştirme
- Kariyer fırsatları



#faydalı kaynaklar & profiller

Oya Geron · 1.

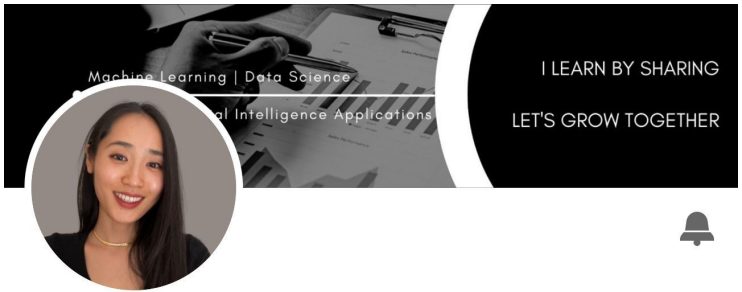
AI Change Strategist and Trainer | Founder at Reshape Consulting

Top Artificial Intelligence (AI) Voice

RESHAPE CONSULTING · Orta Doğu Teknik Üniversitesi
Londra, İngiltere, Birleşik Krallık

All Links to Connect

24.535 takipçi · 500+ bağlantı



Alex Wang · 2.

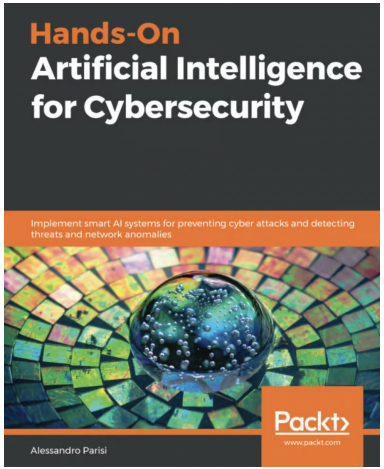
Learn AI Together - I share my learning journey into AI and Data Science here, 90% buzzword-free. Follow me and let's grow together!

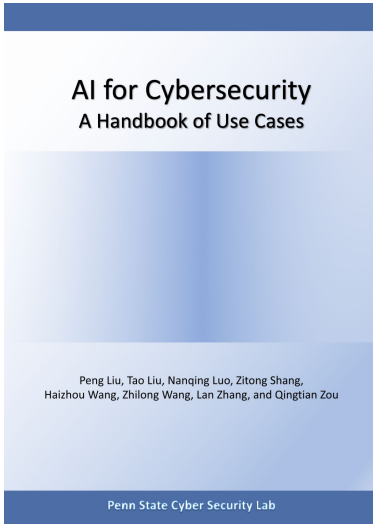
Top Voice

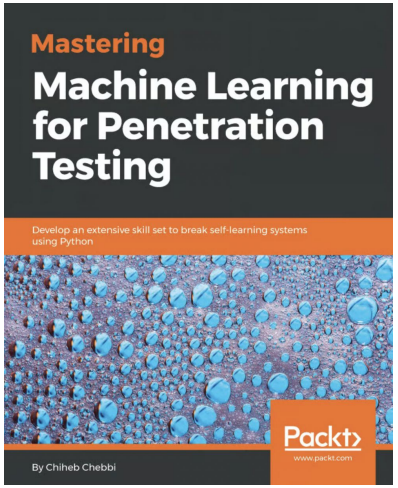
AI4Diversity · University of Sydney
Avustralya

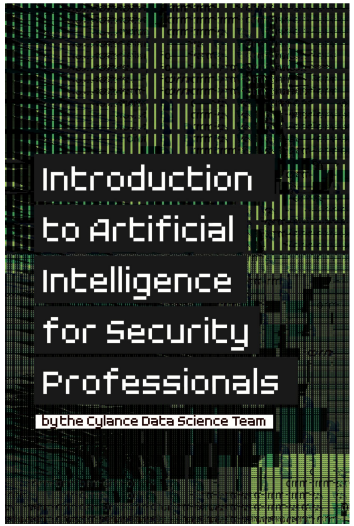
929.073 takipçi

#faydalı kaynaklar & profiller









Sorular & Teşekkürler!

LinkedIn/Twitter/Medium/GitHub: @brcyrr