HILASSOUN A. ROLAND SANOU

Siber Güvenlik Ar-Ge Mühendisi — Uç Nokta Tespit ve Müdahale | Tehdit Analizi | Makine Öğrenmesi Tabanlı Güvenlik
Mersin, Türkiye · +90 536 992 12 17 · rolandS01@outlook.fr
linkedin.com/in/hilassoun-a-roland-sanou · github.com/rolandsanou

PROFESYONEL ÖZET

Türkiye'nin önde gelen uç nokta güvenliği şirketi C-Prot'ta 3 yılı aşkın deneyime sahip, dünya genelinde 5 milyondan fazla kullanıcıya hizmet veren Siber Güvenlik Ar-Ge Mühendisi. EDR ve mobil güvenlik platformları için makine öğrenmesi destekli ve sezgisel tehdit tespit ve müdahale sistemleri geliştirme konusunda uzman. Şu anda bankacılık, enerji ve savunma sektörü müşterileri için %99 tespit doğruluğuna ulaşan Windows EDR çözümleri geliştiriyor. Çekişmeli makine öğrenmesi ve yeni nesil tehdit istihbaratı alanlarında uzmanlaşmak için Yapay Zekâ yüksek lisansına devam ediyor.

PROFESYONEL DENEYİM

Ar-Ge Mühendisi — EDR & Windows Uç Nokta Güvenliği

C-Prot Siber Güvenlik Teknolojileri A.Ş. · Mersin, Türkiye · *Ocak 2025 — Devam ediyor*

- Gelişmiş kalıcı tehditleri (APT), fidye yazılımlarını ve sıfırıncı gün açıklarını tespit etmek üzere makine öğrenmesi tabanlı ve sezgisel tespit motorlarını birleştiren Windows EDR (Uç Nokta Tespit ve Müdahale) çözümleri tasarlıyor ve geliştiriyor.
- Kötü amaçlı yazılım ailelerinde %99 tespit doğruluğuna ulaşan gerçek zamanlı tehdit tespit hatları kurdu; bankacılık ve enerji sektöründeki kurumsal müşteriler için yanlış pozitif oranlarını belirgin biçimde azalttı.
- Tehditleri karantinaya alan, geri alan ve etkisiz hâle getiren otomatik müdahale iş akışları geliştirdi; kullanıcıyı en az düzeyde etkileyerek olay müdahale süresini kısalttı.
- 10 mühendisten oluşan bir Ar-Ge ekibinde, dünya genelinde 5 milyondan fazla kullanıcıya (kurumsal ve bireysel) ulaşan güvenlik çözümleri geliştirdi.
- Dosyasız kötü amaçlı yazılımlar, sistem ikililerinin kötüye kullanımı (LOLBin) ve süreç enjeksiyonu teknikleri dâhil olmak üzere yeni Windows saldırı vektörleri üzerine tehdit istihbaratı araştırması yürüttü.
- Proaktif tehdit avı ile statik ve dinamik analiz hatları için YARA kuralları ve davranışsal imzalar geliştirdi.

Ar-Ge Mühendisi — Android Güvenliği & Tehdit Araştırması

C-Prot Siber Güvenlik Teknolojileri A.Ş. · Mersin, Türkiye · *Eylül 2024 — Ocak 2025*

- Android cihazları hedef alan kimlik avı, kötü amaçlı kod enjeksiyonu, izin istismarı ve ekran kaplama saldırıları gibi farklı saldırı türlerini araştırdı ve sınıflandırdı.
- Kimlik avı URL'lerini ve kötü amaçlı APK'ları yüksek hassasiyetle tespit eden makine öğrenmesi modelleri (sınıflandırma, anormallik tespiti) tasarladı ve eğitti; bunları C-Prot'un mobil güvenlik ürününe entegre etti.
- Daha önce görülmemiş tehditleri belirlemek için davranışsal analizi statik kod incelemesiyle birleştiren sezgisel tespit yöntemleri geliştirdi.
- Tespit yeteneklerini doğrulamak ve kapsamı genişletmek amacıyla Android saldırı yüzeyleri için kavram kanıtı istismarları hazırladı.
- Ar-Ge ekibi için araştırma bulgularını ve model performans ölçümlerini içeren teknik dokümantasyon yazdı.

Stajyer Mühendis — Android Geliştirme

C-Prot Siber Güvenlik Teknolojileri A.Ş. · Mersin, Türkiye · *Şubat 2023 — Ağustos 2024*

- C-Prot'un Android antivirüs ve mobil güvenlik uygulamasının geliştirilmesine ve bakımına katkıda bulundu.
- Gerçek zamanlı tarama, tehdit uyarıları ve kötü amaçlı yazılım karantinası gibi güvenlik özelliklerini uyguladı.
- Mobil ekip içinde kod incelemelerine, sprint planlamasına ve çevik geliştirme süreçlerine katıldı.
- Kapsamlı tehdit korumasını sürdürürken uygulama performansını ve pil tüketimini optimize etti.

TEKNİK YETKİNLİKLER

Alan	Teknolojiler
Güvenlik Araçları	Wireshark, Metasploit, Burp Suite, YARA, IDA Pro, Ghidra, Frida, SIEM (Splunk, ELK), Nmap, OWASP ZAP
EDR / Uç Nokta	Tehdit tespit motorları, davranışsal analiz, statik ve dinamik analiz, kum havuzu, olay müdahalesi, tehdit avı
Güvenlik için ML	scikit-learn, TensorFlow, PyTorch, anormallik tespiti, kötü amaçlı yazılım sınıflandırma, kimlik avı için NLP
Programlama Dilleri	Python, C/C++, Java, Kotlin, C#, Bash, SQL, Go, JavaScript
Platformlar	Windows (çekirdek düzeyi hata ayıklama, PE analizi), Linux, Android (AOSP, APK tersine mühendisliği)
Bulut / DevOps	AWS, GCP, Azure, Docker, Kubernetes, CI/CD (Jenkins, GitHub Actions), Git
Tersine Mühendislik	PE dosya analizi, disassembly (IDA Pro, Ghidra), dinamik enstrümantasyon (Frida), Android APK decompile
Ağ	TCP/IP, DNS, HTTP/TLS analizi, paket yakalama, güvenlik duvarı kuralları, VPN, ağ adli bilişimi

EĞİTİM

Yüksek Lisans, Bilgisayar Bilimleri — Yapay Zekâ

Mersin Üniversitesi, Mersin, Türkiye · *2025 — 2027 (devam ediyor)*

Araştırma: çekişmeli makine öğrenmesi, yapay zekâ destekli tehdit tespiti, siber güvenlikte LLM uygulamaları.

Lisans, Bilgisayar Mühendisliği

Mersin Üniversitesi, Mersin, Türkiye · *2020 — 2024*

SERTİFİKALAR

- Sızma Testi — Coursera (sertifikalı)
- Makine Öğrenmesi Uzmanlığı — Coursera (sertifikalı)

ÖNE ÇIKAN PROJELER

ML Destekli Kimlik Avı ve Kötü Amaçlı Yazılım Tespit Motoru — C-Prot Ar-Ge

Kimlik avı URL'lerini ve kötü amaçlı Android APK'larını %99 doğrulukla tespit eden sınıflandırma modelleri tasarladı. Milyonlarca kullanıcıya hizmet veren üretimdeki mobil güvenlik ürününe entegre edildi.

Windows EDR Tehdit Tespit ve Müdahale Hattı — C-Prot Ar-Ge

Windows uç noktalarında fidye yazılımı, dosyasız kötü amaçlı yazılım ve APT'ler için makine öğrenmesi modelleri ile sezgisel kuralları birleştiren gerçek zamanlı bir tespit motoru kurdu. Bankacılık ve enerji sektöründeki kurumsal müşterilere dağıtıldı.

Duygu Tespiti Mobil Uygulaması

Android üzerinde çalışan, CNN mimarisi ve cihaz üstü çıkarım için TensorFlow Lite kullanan bir yüz ifadesi tanıma derin öğrenme modeli geliştirdi.

Güneş Paneli Temizleme Robotu Denetleyicisi

Endüstriyel bir güneş paneli temizleme robotunun Bluetooth/WiFi üzerinden gerçek zamanlı uzaktan kontrolü için telemetri panosu ve otomatik temizlik programları içeren bir Android uygulaması geliştirdi.

DİLLER

Fransızca: Anadil · **Dioula**: Anadil · **İngilizce**: C1 (İleri) · **Türkçe**: Akıcı

İLGİ ALANLARI

CTF yarışmaları, tehdit istihbaratı araştırması, açık kaynak güvenlik araçları, siber güvenlikte YZ/ML, IoT güvenliği.