
**T.C**

**DOKUZ EYLÜL ÜNİVERSİTESİ**

**FEN FAKÜLTESİ**

**BİLGİSAYAR BİLİMLERİ BÖLÜMÜ**

# VORPAL: ÇOKLU AJAN TABANLI OTONOM SİBER GÜVENLİK TARAMA VE RAPORLAMA SİSTEMİ

**Berkay ÇAKIBEY — 2022280124**

**Talha GÖKGÖZ — 2022280094**

**Egemen AZAY — 2022280076**

**Danışman: Prof. Dr. Efendi NASİBOĞLU**

**Mayıs, 2026**

**İZMİR**

## ÖZET

Siber güvenlik keşif ve zafiyet analizi süreçleri, çok sayıda aracın birlikte kullanılmasını, farklı çıktı formatlarının yorumlanmasını, kapsam sınırlarının korunmasını ve elde edilen bulguların kanıta dayalı biçimde raporlanmasını gerektirir. Bu süreçler manuel yürütüldüğünde araç seçimi, çıktı normalizasyonu, bulgu önceliklendirme ve rapor üretimi gibi adımlar hem zaman alıcı hem de hataya açık hale gelmektedir.

Bu çalışmada geliştirilen **Vorpal**, komut satırı üzerinden çalışan, Pydantic AI tabanlı çoklu ajan mimarisine sahip bir siber güvenlik keşif, analiz ve raporlama sistemidir. Sistem kullanıcıdan bir hedef alır; hedefi doğrular, tarama kapsamını değerlendirir, uygun güvenlik araçlarını seçer, bu araçları Docker tabanlı izole bir çalışma ortamında çalıştırır, ham araç çıktılarını standart veri modellerine dönüştürür, bulguları kanıtlarla ilişkilendirir ve sonuçta yapılandırılmış güvenlik raporları üretir.

Vorpal'ın temel mimarisi merkezi bir Orchestrator Agent ve ona bağlı uzman ajanlardan oluşur. Tool Executor Agent harici güvenlik araçlarının seçimi ve yürütülmesinden; Signal Agent ham ve normalize edilmiş verilerden güvenlik sinyali üretiminden; Explain Agent bulguların teknik ve sade dille açıklanmasından; Remediation Agent çözüm planlarının hazırlanmasından; Reporter Agent ise nihai rapor verisinin ve çıktı dosyalarının oluşturulmasından sorumludur. Sistem ayrıca API Auth, Browser, OSINT, Analyst ve Regression gibi yardımcı ajanlarla genişletilebilir bir analiz yapısı sunar.

Çalışmanın öne çıkan teknik katkıları; LLM destekli araç orkestrasyonu, konteyner izolasyonu, kapsam ve onay kontrolleri, dosya tabanlı artifact saklama, araç çıktı adaptörleri, kanıt zinciri korunarak sinyal üretimi ve çok formatlı raporlama altyapısıdır. Bu sayede sistem, güvenlik tarama sürecini yalnızca araç çalıştıran bir komut katmanı olmaktan çıkarıp, izlenebilir ve denetlenebilir bir analiz hattı haline getirir.



**Anahtar kelimeler:** Siber güvenlik, çoklu ajan mimarisi, LLM, Docker sandbox, zafiyet tarama, keşif otomasyonu, kanıta dayalı raporlama.