

**TÜBİTAK–2209-A ÜNİVERSİTE ÖĞRENCİLERİ ARAŞTIRMA PROJELERİ DESTEĞİ PROGRAMI**

**Başvuru formunun Arial 9 yazı tipinde, her bir konu başlığı altında verilen açıklamalar göz önünde bulundurularak hazırlanması ve ekler hariç toplam 20 sayfayı geçmemesi beklenir (Alt sınır bulunmamaktadır). Değerlendirme araştırma önerisinin özgün değeri, yöntemi, yönetimi ve yaygın etkisi başlıkları üzerinden yapılacaktır.**

**ARAŞTIRMA ÖNERİSİ FORMU**

2024Yılı

1. Dönem Başvurusu

**A. GENEL BİLGİLER**

|  |
| --- |
| **Başvuru Sahibinin Adı Soyadı: Samet Yusuf İçgen, İrem Öner, Batuhan Çakmak** |
| **Araştırma Önerisinin Başlığı: Yapay Zeka ile Anında Tehdit İstihbaratı ve Savunma Sistemi** |
| **Danışmanın Adı Soyadı: Serdar Gündoğdu** |
| **Araştırmanın Yürütüleceği Kurum/Kuruluş: Dokuz Eylül Üniversitesi Bergama Meslek Yüksek Okulu** |

**ÖZET**

|  |
| --- |
| **Özet**  **Projemiz, yapay zeka destekli CTI (Cyber Thread Inteligence) tabanlı olay müdahale otomasyonu olarak tanımlanabilir.**  **Proje amacı siber güvenlikte tehdit istihbaratını etkili bir şekilde kullanarak olay müdahale süreçlerini otomatikleştirmek ve optimize etmektir.**  **Projemiz web scraping ile çektiğimiz CTI verilerini yapay zeka, derin öğrenme ve makine öğrenimi tekniklerini kullanarak gerçek zamanlı olarak analiz eder. Sistemlerde oluşabilecek tehditlere yönelik otomatik kurallar geliştirir ve bu şekilde proaktif savunma sağlar.**  **Bu proje olay müdahale süreçlerini kayda değer şekilde azaltarak siber güvenlik ekiplerinin tehditleri daha hızlı ve etkili bir biçimde önlemesine yardımcı olur.**  **Proje üzerinde tehdit verilerinin toplanması, işlenmesi ve saklanması için veritabanı olarak MongoDB kullanılmaktadır. Belge tabanlı MongoDB veritabanı, tarafımızca tehdit istihbaratı verilerinin genellikle hiyerarşik bir yapıda olması sebebiyle tercih edilmiştir.**  **Kaynak ve vakit verimliliğini arttırmak amacıyla ve bu veri formatının birçok API ile uyumlu çalışması, çoğu moderrn programlama dillerinin ve kütüphanelerin bu veri formatını daha hızlı işlemesi gibi sebeplerden ötürü JSON formatı tercih edilmiştir.**  **Projemizde kullandığımız yapay zeka ve derin öğrenme teknikleri, siber tehdit istihbaratı analizini ve olay müdahale süreçlerini hızlandırarak ve otomatikleştirerek bu alanda büyük bir açığı kapatmayı hedeflemekedir.** |
| **Anahtar Kelimeler: Siber Tehdit İstihbaratı, CTI, Derin Öğrenme, Yapay Zeka** |

* **ÖZGÜN DEĞER**

**1.1. Konunun Önemi, Araştırma Önerisinin Özgün Değeri ve Araştırma Sorusu/Hipotezi**

Araştırma önerisinde ele alınan konunun kapsamı ve sınırları ile önemi literatürün eleştirel bir değerlendirmesinin yanı sıra nitel veya nicel verilerle açıklanır.

Özgün değer yazılırken araştırma önerisinin bilimsel değeri, farklılığı ve yeniliği, hangi eksikliği nasıl gidereceği veya hangi soruna nasıl bir çözüm geliştireceği ve/veya ilgili bilim veya teknoloji alan(lar)ına kavramsal, kuramsal ve/veya metodolojik olarak ne gibi özgün katkılarda bulunacağı literatüre atıf yapılarak açıklanır.

Önerilen çalışmanın araştırma sorusu ve varsa hipotezi veya ele aldığı problem(ler)i açık bir şekilde ortaya konulur.

|  |
| --- |
| Projemizin kapsam alanı dahilinde mekanizmamızın sağladığı kural oluşturma işleminin öncesi ve sonrasındaki süreçleri yapay zeka üzerinden otomatik olarak yapacak bazı çözümler geliştirilmiş fakat kural oluşturma işlemini yapay zeka üzerinden sağlayacak bir mekanizma geliştirilmemiş olmakla birlikte bu işlem hala insan gücü ile sağlanmaktadır.  Örneğin; Benzer bir amaçla geliştirilmiş Torq Socrates isimli çözüm, SOC süreçlerini hızlandırmak ve Tier-1 seviyesindeki bildirimlerin %90'ına otonom olarak yanıt verebilmek için tasarlanmıştır. Sonuç olarak bu çözüm L1 Siber Tehdit Analistlerinin alarmları yanıtlandırma işini sağlar fakat bu alarmları oluşturan kuralları yazabilme yetisine sahip değildir. Bizim geliştirdiğimiz bu mekanizma, oluşabilecek potansiyel siber tehditleri analiz ederek EDR sistemlerine yönelik yapay zeka ve derin öğrenme tabanlı gerçek zamanlı bir otomatik kural oluşturma çözümüdür.  Teorik olarak kural oluşturma işleminin yapay zeka üzerinden sağlanabileceğiyle ilgili birkaç makale yazılmış, fakat bu makaleler pratiğe dökülmemiş, bu işlevi sağlayacak bir mekanizma oluşturulmamıştır.  Bu makalelere bir örnek verecek olursak mekanizmamızın çalışma prensibine en yakın teorik inceleme Autonomous Threat Hunting: AI-Driven Threat Intelligence isimli makaledir;  Bu makale, tehdit avlama süreçlerini yapay zekâ destekli bir otomasyonla geliştirmeyi ele almaktadır. Özellikle geleneksel tehdit istihbaratında karşılaşılan ölçeklenebilirlik ve güvenilirlik zorluklarını vurgulamakta. Yapay zekâ algoritmalarının, özellikle makine öğrenimi ve derin öğrenme modellerinin, güvenlik operasyonlarını hızlandırmada ve proaktif savunma sağlamada nasıl işlev gördüğünü inceleyen çalışma; denetimli ve denetimsiz öğrenme yöntemleriyle false positive kuralları azaltmayı ve tehditleri tanımlama sürecini hızlandırmayı önermektedir fakat bu fikri faaliyete geçirmemiştir.  İlgii süreçlerde maksimum hız, minimum iş gücü, bunun dolayısıyla da minimum maliyetle kural oluşturma işlemini sağlayarak olay müdahale sürecini hızlandıracak bu yazılım, şuan insan gücü ile yapılan bir işlemin otomatik olarak bir makine tarafından yapılması olanağını sağladığından siber güvenlik sektöründe büyük bir açığı kapatacaktır. |

* **Amaç ve Hedefler**

Araştırma önerisinin amacı ve hedefleri açık, ölçülebilir, gerçekçi ve araştırma süresince ulaşılabilir nitelikte olacak şekilde yazılır.

|  |
| --- |
| Amacımız olay müdahale süreçlerini hızlandırmak ve tehditlere karşı proaktif savunma sağlamak adına tehdit istihbaratını işleyen ve bunları baz alarak processler için kural yazan yapay zeka sistemi geliştirmek. Bu amaçla hedef kitlemiz Siber Güvenlik analistleri, SOC (Güvenlik Operasyon Merkezi) çalışanları ve Tehdit İstihbaratı uzmanlarıdır. Bu proje kapsamında sağlamayı amaçladığımız fayda, otomasyon ve yapay zeka desteği ile insan müdahalesini minimuma indirmek, manuel inceleme süreçlerini hızlandırmak ve oluşabilecek siber tabanlı saldırıları en erken aşamada engellemek. |

* **YÖNTEM**

Araştırma önerisinde uygulanacak yöntem ve araştırma teknikleri (veri toplama araçları ve analiz yöntemleri dahil) ilgili literatüre atıf yapılarak açıklanır. Yöntem ve tekniklerin çalışmada öngörülen amaç ve hedeflere ulaşmaya elverişli olduğu ortaya konulur.

Yöntem bölümünün araştırmanın tasarımını, bağımlı ve bağımsız değişkenleri ve istatistiksel yöntemleri kapsaması gerekir. Araştırma önerisinde herhangi bir ön çalışma veya fizibilite yapıldıysa bunların sunulması beklenir. Araştırma önerisinde sunulan yöntemlerin iş paketleri ile ilişkilendirilmesi gerekir.

|  |
| --- |
| Yapay Zeka Anında Tehdit İstihbaratı ve Savunma Sistemi, toplam 4 aşamadan oluşacak bir proje olmakla beraber adımları ve kullanılacak kütüphaneler, diller ve araçlar şu şunlardır:  Python Dili: bu proje için seçtiğimiz bu dil; geniş kütüphane desteği, veri analizi ve işleme için kullanabileceğimiz en ideal dildir. Ayrıca, doğal dil işleme ve yapay zeka uygulamaları için sunduğu popüler kütüphaneler sayesinde projedeki verimliliğimizi arttıracaktır.  Veri toplama araçları olarak BeautifulSoup ve Scrapy kütüphaneleri, onaylanmış veri güvenliği ve siber tehdit istihbaratı raporları paylaşan kaynaklardan veri toplamak için kullanacak, Requests kütüphanesi ile de çeşitli tehdit istihbaratı API’lerinden veriler çekilecektir.  Veri depolama ve veri formatı kısmında veriler JSON formatında depolanacaktır. JSON, metin tabanlı bir veri formatı olması sayesinde; erişilebilen, düzenlenebilen ve toplanılan verilerin hızlı bir biçimde işlenilmesine imakn sağlar. Depolama olarak ise MongoDB kullanılacaktır. NoSQL tabanlı bir veritabanı olan MongoDB, verileri BSON formatında depolayarak hızlı erişim sağlar. Ürün çıkışı (kural yazımı) sonrası bu ürünler JSON formatında ana depoda saklanır. Böylece okunabilir ve kullanıma hazır olurlar.  Tehdit istihbaratı verilerinin analizini gerçekleştirmek ve potansiyel kurallar oluşturmak için OpenAI API’si kullanılacaktır. Bu sayede, gelen tehdit verileri doğal dil işleme (NLP) modellerimiz tarafından analiz edilecek ve anlamlandırılacaktır. OpenAI’ın modeli, tehdit istihbaratı verilerini yorumlayarak en son tehdit bilgileri doğrultusunda hangi kuralların oluşturulması gerektiğini tespit eder.  Kural yazma sürecinde ise yapay zeka tarafından analiz edilen ve özetlenen tehdit bilgileri, KQL (Kusto Query Language) dili ile tanımlı kurallara dönüştürülerek, belirlenen process bazlı güvenlik önlemlerine çevrilecektir. KQL, Azure Sentinel veya benzeri sistemlerde kullanabileceğimiz güçlü bir sorgulama dilidir ve güvenlik olaylarının tespiti için idealdir. GPT tarafından yapılan analizler sonucunda, KQL formatında kurallar yazılır. Kurallar, processin isimlendirmesi, IoC değerleri ve tehdit tanımlarına göre oluşturulacaktur. Bu kuralları JSON formatında saklanacak ve gerektiğinde güncellenebilir, analiz edilebilir ve kullanılabilir olacaktır.  Yazılan kuralların fazla False-Positive (Sahte Alarm) çıkarmaması için yapay zeka tarafından üretilen kurallar, analiz edilecektir. Analiz edilen verilerin doğruluğunu, performansını ve tehdit tespiti açısından başarısını değerlendirmek için Scikit-Learn kütüphanesi kullanılacaktır. AUC-ROC skorları, hassasiyet ve doğruluk ölçümleri gibi metrikler yardımı ile modelin güvenlirliği değerlendirilir.  Test ve yeni kurallar kapsamında ise elde edilen yeni tehdit bilgileri, yapay zeka tarafından analiz edilip KQL kurallarına dönüştürelecektir. Bu kurallar önce test veritabanında denenip, başarı kriterlerine göre düzenlendikten sonra ana veritabanında saklanacaktır.  Bu süreç içerisinde Python ile baraber; MongoDB, JSON, OpenAI ve KQL gibi araç ve teknolojiler kullanılarak verimli, hızlı ve güvenilir bir kural yazma süreci sağlanacaktır. |

* **PROJE YÖNETİMİ**
* **İş- Zaman Çizelgesi**

Araştırma önerisinde yer alacak başlıca iş paketleri ve hedefleri, her bir iş paketinin hangi sürede gerçekleştirileceği, başarı ölçütü ve araştırmanın başarısına katkısı “İş-Zaman Çizelgesi” doldurularak verilir. Literatür taraması, gelişme ve sonuç raporu hazırlama aşamaları, araştırma sonuçlarının paylaşımı, makale yazımı ve malzeme alımı ayrı birer iş paketi olarak gösterilmemelidir.

Başarı ölçütü olarak her bir iş paketinin hangi kriterleri sağladığında başarılı sayılacağı açıklanır. Başarı ölçütü, ölçülebilir ve izlenebilir nitelikte olacak şekilde nicel veya nitel ölçütlerle (ifade, sayı, yüzde, vb.) belirtilir.

**İŞ-ZAMAN ÇİZELGESİ (\*)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **İP No** | **İş Paketlerinin Adı ve Hedefleri** | **Kim(ler) Tarafından Gerçekleştirileceği** | **Zaman Aralığı**  **(..-.. Ay)** | **Başarı Ölçütü ve Projenin Başarısına Katkısı** |
| 1 | Proje Planlanması | Yürütücü | 1 ay | Projenin genel yönelimi için sağlam temel sağlama |
| 2 | Veri toplama | Yürütücü/Araştırmacı | 1 ay | Elde edilen verilerin kalitesi ile modelin başarısı |
| 3 | Veri Depolama Tasarımı | Yürütücü/Araştırmacı | 2 ay | Veri erişim hızı ve düzeni için optimize edilmesi |
| 4 | Yapay zeka modelinin geliştirilmesi | Yürütücü/Araştırmacı | 4 ay | Verileri algılama, anlamlandırma ve tehdit algılama yeteneğini kazandırma |
| 5 | Kural Yazma | Yürütücü/Araştırmacı | 2 ay | Otomatik kural üretimi |
| 6 | Test Süreci | Yürütücü/Araştırmacı | 1 ay | Yazılan modelin ve kuralların güvenilirliğinin sağlanması |
| 7 | Sonuç analizi | Yürütücü/Araştırmacı | 0.5 ay | Sorunların giderilmesi ve projenin en uygun hale getirilmesi |
| 8 | Uygulama ve Sunum | Yürütücü/Araştırmacı | 0.5 ay | Sonuç raporunun yazılması ve sunulması |

(\*) Çizelgedeki satırlar ve sütunlar gerektiği kadar genişletilebilir ve çoğaltılabilir.

* **Risk Yönetimi**

Araştırmanın başarısını olumsuz yönde etkileyebilecek riskler ve bu risklerle karşılaşıldığında araştırmanın başarıyla yürütülmesini sağlamak için alınacak tedbirler (B Planı) ilgili iş paketleri belirtilerek ana hatlarıyla aşağıdaki Risk Yönetimi Tablosu’nda ifade edilir. B planlarının uygulanması araştırmanın temel hedeflerinden sapmaya yol açmamalıdır.

**RİSK YÖNETİMİ TABLOSU\***

|  |  |  |
| --- | --- | --- |
| **İP No** | **En Önemli Riskler** | **Risk Yönetimi (B Planı)** |
| 1 | Sitemin fazla False Positive (Sahte Alarm) alarm üretilmesi. | Scikit-Learn kütüphanesi ile gerekli ölçümler ve testler sonrası bu fazla Sahte Alarm üretimini en aza indirmek. |
| 2 |  |  |

(\*) Tablodaki satırlar gerektiği kadar genişletilebilir ve çoğaltılabilir.

* **Araştırma Olanakları**

Bu bölümde projenin yürütüleceği kurum ve kuruluşlardavar olan ve projede kullanılacak olan altyapı/ekipman (laboratuvar, araç, makine-teçhizat, vb.)olanakları belirtilir.

**ARAŞTIRMA OLANAKLARI TABLOSU (\*)**

|  |  |
| --- | --- |
| **Kuruluşta Bulunan Altyapı/Ekipman Türü, Modeli**  (Laboratuvar, Araç, Makine-Teçhizat, vb.) | **Projede Kullanım Amacı** |
| Bilgisayar | Projeyi yazacağımız ve projede asıl rolü olacak makine. |

**(\*)** Tablodaki satırlar gerektiği kadar genişletilebilir ve çoğaltılabilir.

* **YAYGIN ETKİ**

Önerilen çalışma başarıyla gerçekleştirildiği takdirde araştırmadan elde edilmesi öngörülen ve beklenen yaygın etkilerin neler olabileceği, diğer bir ifadeyle yapılan araştırmadan ne gibi çıktı, sonuç ve etkilerin elde edileceği aşağıdaki tabloda verilir.

**ARAŞTIRMA ÖNERİSİNDEN BEKLENEN YAYGIN ETKİ TABLOSU**

|  |  |
| --- | --- |
| **Yaygın Etki Türleri** | **Önerilen Araştırmadan Beklenen Çıktı, Sonuç ve Etkiler** |
| **Bilimsel/Akademik**  (Makale, Bildiri, Kitap Bölümü, Kitap) | Yapay zekanın siber güvenlik alanında kullanımını genişletir. |
| **Ekonomik/Ticari/Sosyal**  (Ürün, Prototip, Patent, Faydalı Model, Üretim İzni, Çeşit Tescili, Spin-off/Start- up Şirket, Görsel/İşitsel Arşiv, Envanter/Veri Tabanı/Belgeleme Üretimi, Telife Konu Olan Eser, Medyada Yer Alma, Fuar, Proje Pazarı, Çalıştay, Eğitim vb. Bilimsel Etkinlik, Proje Sonuçlarını Kullanacak Kurum/Kuruluş, vb. diğer yaygın etkiler) | Ekonomik olarak otomatik tehdit istihbaratı analizi ve kural yazımı sayesinde siber güvenlik maliyetlerini önemli ölçüde azaltır. Ayrıca, bu otomatikleştirilmiş yapı sayesinde siber güvenlik operasyonlarının hızını arttırır ve daha az kaynak kullanarak daha fazla güvenlik elde edilmesini sağlar. Ticari olarak otomatik veri istihbaratı ve kural yazımı olan bir sistem özellikle büyük işletmelere yönelik cazip bir siber güvenlik ürünü olabilir. Sosyal olarak kullanıcı verilerinin korunmasına ve daha hızlı önlem alınmasına olanak sağlar. |
| **Araştırmacı Yetiştirilmesi ve Yeni Proje(ler) Oluşturma**  (Yüksek Lisans/Doktora Tezi, Ulusal/Uluslararası Yeni Proje) | Proje yeni geliştirmelere açık olacak ve bu konuda uzmanların proje hakkında görüşleri alınacaktır. |

**5. BÜTÇE TALEP ÇİZELGESİ**

|  |  |  |
| --- | --- | --- |
| **Bütçe Türü** | **Talep Edilen Bütçe Miktarı (TL)** | **Talep Gerekçesi** |
| **Sarf Malzeme** | 0 |  |
| **Makina/Teçhizat (Demirbaş)** | 0 |  |
| **Hizmet Alımı** | 9.000.00 TL | Projemizde kullanacağımız verileri depolamak için ihtiyacımız olan veritabanı. (MongoDB) |
| **Ulaşım** | 0 |  |
| **TOPLAM** | 0 |  |

**NOT:** Bütçe talebiniz olması halinde hem bu tablonun hem de TÜBİTAK Yönetim Bilgi Sistemi (TYBS) başvuru ekranında karşınıza gelecek olan bütçe alanlarının doldurulması gerekmektedir. Yukardaki tabloda girilen bütçe kalemlerindeki rakamlar ile, TYBS başvuru ekranındaki rakamlar arasında farklılık olması halinde TYBS ekranındaki veriler dikkate alınır ve başvuru sonrasında değiştirilemez.

**6. BELİRTMEK İSTEDİĞİNİZ DİĞER KONULAR**

Sadece araştırma önerisinin değerlendirilmesine katkı sağlayabilecek bilgi/veri (grafik, tablo, vb.) eklenebilir.

|  |
| --- |
|  |

**7. EKLER**

**EK-1: KAYNAKLAR**

Buraya makaleler eklenecek.