“Yapay Zeka Sınırlarını Keşfetmek: KOBİ’ler için Yapay Zeka Destekli Siber Risk Yönetimi (AID)” projesi

KA210-VET

Yetkinlik Haritası

Giriş

AID Yetkinlik Haritası, KOBİ’lerin dijital dönüşümü etkin biçimde yönetebilmesi ve yapay zeka kaynaklı riskleri ele alabilmesi için gerekli kritik yetkinlikleri tanımlamak ve sınıflandırmak amacıyla oluşturulmuş yapılandırılmış bir çerçevedir. Avrupa Yeterlilikler Çerçevesi (AYÇ) düzeyleriyle uyumlu olan bu harita, dijital hazırlık ve dayanıklılığın farklı Avrupa bağlamlarında ölçülebilir ve standart hale gelmesini sağlar. Haritanın yapısı üç öncelikli alan etrafında düzenlenmektedir: Siber Güvenlik, Siber Risk Yönetimi ve Veri Analizi. Her alan için çerçeve; davranışlar, beceriler, bilgi ve tutumlar olmak üzere dört boyuta ayrılmış kapsamlı bir analiz sunmaktadır.

- **Davranışlar: Yapılandırılmış risk yönetimi politikalarının uygulanması, algoritmik önyargının anlaşılması ve kişisel verilerin sorumlu biçimde kullanılması gibi gözlemlenebilir eylemleri ve karar alma süreçlerini tanımlar.**
- **Beceriler: Bu boyut; güvenlik ayarlarının yapılandırılması, siber risklerin tespit edilmesi ve önceliklendirilmesi ile farklı kaynaklardan veri toplanması ve temizlenmesi gibi pratik uygulamalara odaklanmaktadır.**
- **Bilgi: Temel siber güvenlik kavramlarının anlaşılması, yaygın siber saldırı türleri, risk yönetimi standartları ve yapay zeka etiği gibi konularda gereken teorik temeli ifade eder.**
- **Tutumlar: Harita; risk önlemeye yönelik proaktif yaklaşım, kanıta dayalı kararlar için analitik düşünme biçimi ve veri bütünlüğünün korunmasına ilişkin kararlılık gibi temel zihinsel tutumları ön plana çıkarmaktadır.**

Yetkinlik haritasının oluşturulma sürecine genel bir bakış için İtalya, Letonya ve Türkiye’yi kapsayan “KOBİ’lerde Dijital Uyum ve Büyüme için Yetkinlik Araştırması” (Çıktı 1) ile “KOBİ Dijital Yetkinlik Açığı Anket Sonuçlarına İlişkin Uluslararası Rapor” (Çıktı 2) adlı çalışmaların okunması önerilmektedir. Bu belgelere proje web sitesinden ulaşabilirsiniz: https://www.bda.lv/en/ai-driven-cyber-risk-management-for-smes/

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the State Education Development Agency (VIAA). Neither the European Union nor VIAA can be held responsible for them.

Yetkinlik Alanı ve Açıklaması	Davranışlar	Beceriler	Bilgi	Tutumlar
Siber Güvenlik **Güvenli uygulamaları hayata geçirerek, gizliliğe saygı göstererek ve yapay zeka dahil mevcut ile gelişmekte olan teknolojilerin kullanımına ilişkin bilinçli kararlar alarak; şirketin dijital cihazlarını, sistemlerini, verilerini ve kişisel çevrimiçi faaliyetlerini tehdit ve risklerden koruma; güvenli ve güvenilir bir dijital ortam oluşturma becerisi.**	1. Şirketin cihazlarını ve içeriklerini dijital tehdit ve risklerden koruma 2. Dijital araçlara duyulan güveni pekiştirmek için temel siber güvenlik ve gizlilik uygulamalarını bilme 3. Dijital ortamlarda kişisel verilere ve mahremiyete saygı gösterilmesini sağlama 4. Kişisel verileri sorumlu bir şekilde kullanma ve paylaşma 5. Gizlilik politikalarını ve bunların etkilerini anlama 6. Stres, yorgunluk veya diğer dijital sağlık risklerinden kaçınma 7. Zararlı çevrimiçi davranışları (ör. siber zorbalık) tanıma ve önleme 8. Teknoloji aracılığıyla dijital kapsayıcılığı ve sosyal refahı teşvik etme 9. Yapay zeka sistemlerindeki algoritmik önyargıyı ve açıklanabilirliği anlama 10. Yapay zeka tabanlı siber güvenlik araçlarının güvenilirliğini ve etkinliğini değerlendirme Tehdit tespitinde yapay zeka kullanımına ilişkin bilinçli kararlar alma	Cihazlara ve verilere yönelik güvenlik risklerini tespit etme ve bunlara yanıt verme 1. Cihazların güvenlik ayarlarını yapılandırma 2. Çok faktörlü kimlik doğrulama ve güvenli parola kullanımı 3. Verilerin güvenli şekilde depolanması ve yedeklenmesi 4. Yapay zeka araçlarının güvenilirliğini ve güvenilebilirliğini değerlendirme	1. Temel siber güvenlik kavramlarına ilişkin bilgi (kimlik doğrulama, şifreleme, veri yedekleme) 2. Yaygın siber saldırı türlerine ilişkin bilgi (kötü amaçlı yazılım, kimlik avı, fidye yazılımı vb.) 3. İş ve kişisel kullanım için güvenli dijital uygulamalar 4. Dijital verileri etkileyen başlıca yasalar ve düzenlemeler (GDPR, ulusal mevzuat vb.) 5. Makine öğrenmesinin temelleri ve yapay zekanın güvenli kullanımı; yapay zekanın kullanımına ilişkin etik ve hukuki boyutlar	1. Siber güvenlik ve risk önleme konusunda proaktif tutum 2. Şirkete ve kişiye ait verilerin sorumlu şekilde işlenmesi 3. Yeni teknolojileri öğrenmeye açıklık 4. İletişimler ile dijital araç ve ortamların kullanımında sağlıklı bir şüphecilik

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the State Education Development Agency (VIAA). Neither the European Union nor VIAA can be held responsible for them.

Yetkinlik Alanı ve Açıklaması	Davranışlar	Beceriler	Bilgi	Tutumlar
Siber Risk Yönetimi **Dijital varlıklara, bilgi sistemlerine ve verilere yönelik riskleri tespit etme, analiz etme ve önceliklendirme; güvenlik, maliyet ve operasyonel ihtiyaçlar arasında denge kurarak hem bireyi hem de kurumu korumak ve stratejik hedefleri desteklemek amacıyla iş odaklı, bilinçli kararlar alma becerisi.**	1. BT sistemlerinde yapılandırılmış risk yönetimi politikaları uygulama 2. Dijital varlıklara yönelik riskleri değerlendirme ve uygun stratejiler planlama 3. Siber risk kararlarını desteklemek için maliyet-fayda analizi sunma 4. Risk yönetimi kararlarını iş ve teknoloji hedefleriyle uyumlandırma 5. Mevcut siber güvenlik durumunu değerlendirme ve KOBİ'ye özgü hedefler belirleme 6. Siber güvenlik eylemleri planlanırken riskleri, maliyetleri ve zafiyetleri tanımlama 7. Şirkete ait veri ve bilgi varlıklarına ilişkin riskleri yönetme	1. Siber riskleri tespit etme, sınıflandırma ve önceliklendirme 2. Nitel ve nicel risk değerlendirmeleri yapma 3. Teknik riskleri iş açısından anlamlı içgörülere dönüştürme 4. Gerçekçi risk azaltma stratejileri ve eylem planları oluşturma 5. Siber riskleri ve ilgili stratejileri teknik ve teknik olmayan paydaşlara iletme	1. İlgili risk yönetimi çerçeveleri ve kalite standartlarına ilişkin bilgi 2. Siber güvenlik ortamı ve şirkete yönelik önemli siber risklere ilişkin bilgi 3. Risk olaylarının analiz edilmesi, iletilmesi ve bunlara müdahale edilmesinin önemi 4. Maliyet-fayda ve risk temelli karar alma modelleri 5. Veriler ve sistemler için düzenleyici, yasal ve uyumluluk gereksinimleri	1. Güvenlik, maliyet ve kullanılabilirlik arasında dengeli bir yargı yürütme 2. Sadece teknolojiyi değil, iş değerini koruma konusunda sorumluluk bilinci 3. Ayrıntılara dikkat eden ve kanıta dayalı kararlar için analitik düşünme biçimi 4. Güvenlik, BT ve iş fonksiyonları arasında iş birliği 5. Ortaya çıkan riskleri öngörmeye yönelik ileriye dönük yaklaşım

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the State Education Development Agency (VIAA). Neither the European Union nor VIAA can be held responsible for them.

Yetkinlik Alanı ve Açıklaması	Davranışlar	Beceriler	Bilgi	Tutumlar
Veri Analizi **Analitik yöntemler uygulayarak, veri bütünlüğünü ve gizliliğini koruyarak ve karmaşık bilgileri bilinçli karar almayı destekleyen anlamlı, eyleme dönüştürülebilir içgörülere dönüştürerek veri toplama, işleme, yorumlama ve iletme becerisi.**	1. Kişisel verilerin nasıl işlendiğini ve korunduğunu anlama 2. Veri bağlamlarında maliyet-fayda analizi ve risk değerlendirmesi uygulama 3. Farklı kaynaklardan kaliteli veri toplama ve hazırlama 4. Verileri anlamak ve içgörü çıkarmak için istatistiksel yöntemler kullanma 5. Verileri net iletişim ve karar alma amacıyla görsel olarak sunma 6. Karmaşık veri bulgularını açık ve eyleme dönüştürülebilir biçimde açıklama 7. Kritik sorular sorma ve gizli veri örüntülerini tespit etme 8. Yeni araçlar, yöntemler ve en iyi uygulamalarla becerileri sürekli güncelleme	1. Farklı kaynaklardan veri toplama, temizleme ve yapılandırma 2. Veri analizi için istatistiksel ve analitik teknikler kullanma 3. Karar almada kullanılacak verileri görselleştirme (grafikler, şemalar, sunumlar vb.) 4. Veriye dayalı sonuçlar çıkarma ve karar alma 5. Eleştirel düşünme yoluyla veri eğilimlerini ve korelasyonları tespit etme	1. Veri yaşam döngüsü, kalitesi ve yönetim ilkelerine ilişkin bilgi 2. Veri işleme için istatistiksel ve analitik yöntemler 3. Veri yönetiminde kişisel verilerin gizliliği ve etik kullanımı (GDPR, veri anonimleştirme) 4. Veri görselleştirme araçları ve teknikleri 5. Veriye dayalı kararlar için maliyet-fayda ve risk analizi modellerinin kullanımı	1. Verileri keşfetme ve mevcut varsayımları sorgulamaya yönelik istek ve yetenek 2. Verilerin doğruluğunu ve bütünlüğünü koruma kararlılığı 3. Sezgisel yaklaşım yerine analize ve veriye dayalı nesnellik 4. Verilerin iletimi ve yorumlanmasında sorumluluk bilinci

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the State Education Development Agency (VIAA). Neither the European Union nor VIAA can be held responsible for them.