AI-DRIVEN PENETRATION TEST

KAPT

HEYLEAN

İlk Yayımlanma Tarihi: *14 Ağustos, 2025*
***Sürüm**: v.1.0.0*

TELİF HAKLARI

FERAGATNÂME

Bu beyaz kağıt (whitepaper), Heylean Teknoloji Anonim Şirketi tarafından Yapay Zeka Destekli Ofansif Karakutu Sızma Testi (KAPT) hakkında bilgi vermek amacıyla hazırlanmıştır. Bu belgedeki bilgiler genel bir bakış sunmayı amaçlamaktadır ve özel danışmanlık veya profesyonel tavsiye niteliğinde değildir.

Heylean, belgede yer alan bilgilerin doğruluğu, eksiksizliği veya güncelliği konusunda hiçbir garanti vermez.

İşbu belgede yer alan bilgiler, belirli bir durum için uygun veya geçerli olmayabilir ve işbu belgede yer alan bilgilerde, kasıtlı veya kasıtsız olarak hatalar veya eksiklikler olabilir.

Heylean Teknoloji Anonim Şirketi, bu belgedeki bilgilerin kullanılması veya kullanılmaması sonucunda doğabilecek hiçbir kayıp, hasar veya zarardan sorumlu tutulamaz. İşbu belgedeki bilgilerin kullanımı tamamen okuyucunun kendi sorumluluğundadır.

İşbu belgede bahsedilen KAPT teknolojisi sürekli gelişmektedir. Bu nedenle, bu belgede yer alan bilgiler gelecekte güncellenebilir veya değişebilir. En güncel bilgiler için lütfen Heylean Teknoloji Anonim Şirketi ile doğrudan iletişime geçin.

İşbu belgede bahsi geçen üçüncü taraf ürünler, hizmetler veya şirketler hakkında yapılan açıklamalar, onların onayı anlamına gelmez.

Herhangi bir güvenlik çözümünün etkinliği, birçok faktöre bağlıdır ve garanti edilemez. Bu belge, kapsamlı bir güvenlik stratejisi oluşturmak için yeterli değildir. Kapsamlı bir güvenlik stratejisi oluşturmak için, bir güvenlik uzmanıyla danışmanlık yapılması önerilir.

İşbu belgede yer alan bazı kapasiteler yalnızca Kamu Kurumları tarafından kullanılabilir olup, gerekli sorgulamaların yapılması gerekmektedir.

İÇİNDEKİLER

GİRİŞ

Heylean, kendiliğinden öğrenen (Self-AI) ve makine öğrenmesi (ML) destekli **C5ISR** çözümleriyle; ***Savunma, istihbarat, siber uzay ve kamu güvenliği*** alanlarında dinamik, proaktif ve sürekli adaptif bir güvenlik mimarisi inşa ediyor.

Küresel güvenlik paradigmasının sürekli evrilen asimetrik ve hibrit tehditlerle yeniden şekillendiği bir çağda, Heylean'in varlık amacı stratejik caydırıcılığı yeniden tanımlamaktır. Ulusların egemenliğini ve kurumsal dayanıklılığı korumak üzere, sadece reaksiyon göstermeyi değil; ***Olayları öngörmeyi, tehditleri kaynağında etkisizleştirmeyi ve sonuçları proaktif olarak şekillendirmeyi mümkün kılan karar üstünlüğü sağlıyoruz***. Operasyonlarımızın merkezinde, belirsizliği netliğe, veriyi ise stratejik avantaja dönüştüren yeni nesil çözümler yer alır.

İstihbaratı bir üründen ziyade modern savunma ve güvenliğin merkezi sinir sistemi olarak ele alır. Çok katmanlı veri akışlarını birleştirerek, gürültüyü anlamlı içgörülere dönüştürüyoruz. Bu süreç, iş ortaklarımızın tehditleri yalnızca bertaraf etmelerini değil, aynı zamanda rakiplerinin bir sonraki hamlesini öngörerek inisiyatifi her zaman ellerinde tutmalarını sağlar. Sunduğumuz eyleme dönüştürülebilir istihbarat, belirsizliği mutlak bir netliğe ve stratejik avantaja çevirir.

Teknolojik üstünlüğün pazarlık konusu olamayacağının bilincindeyiz. Bu nedenle, yeni nesil siber-fiziksel sistemlerin ve otonom yeteneklerin mühendisliğine öncülük ediyoruz. Faaliyetlerimiz, ulusların ve işletmelerin savunma duruşlarını güçlendiren, proaktif ve katmanlı bir güvenlik mimarisi oluşturmaya odaklanmıştır. Uzmanlığımız, kritik görevlerde karar döngüsünü optimize ederek, hazırlık seviyesini en üst düzeye çıkarır ve misyon başarısını garanti altına alır.

Heylean'in küresel güvenlik arenasındaki benzersiz konumu, gelişmiş istihbarat kabiliyetlerini teknolojileri ile birlikte kusursuz bir şekilde birleştirme yeteneğimizden kaynaklanmaktadır. Hızla gelişen ve giderek karmaşıklaşan bir dünyada, biz zorlukları sadece öngörmekle kalmıyor; ***Onları ortaya çıkmadan önce etkisiz hale getirecek çözümleri tasarlıyoruz. Bu stratejik sentez, müşterilerimize rakiplerinin asla erişemeyeceği bir operasyonel tempo ve karar kalitesi sunar***.

Teknolojimizin ve analizlerimizin arkasında en değerli varlığımız yer alır; Stratejistler, mühendisler, veri bilimcileri ve istihbarat uzmanları ve daha fazlasından oluşan multidisipliner bir ekip. Hepimizi birleştiren tek bir amaç var: ***Daha güvenli, daha emniyetli ve daha dayanıklı bir dünya inşa etmek.***

STRATEJİMİZ VE MİSYONUMUZ

Heylean, küresel güvenlik ve savunma doktrinlerini, yapay zekânın dönüştürücü gücüyle yeniden tanımlamayı hedeflemektedir. Temel amacımız, reaktif savunma paradigmalarının ötesine geçerek; ***Proaktif, öngörüsel ve otonom yeteneklerle donatılmış yeni nesil bir güvenlik mimarisi inşa etmektir***. C5ISR çözümlerimiz; Savunma, istihbarat, siber uzay ve kamu güvenliği alanlarında mutlak durumsal farkındalık ve karar hızı sağlayarak, müttefiklerimize ve ortaklarımıza her koşulda stratejik üstünlük kazandırır.

STRATEJİMİZ

Sadece mevcut teknolojileri uygulamakla kalmıyor, aynı zamanda geleceğin teknoloji haritasını şekillendiriyoruz. Uzmanlarımız, yapay zekâ ve otonom sistemler gibi teknolojilerin potansiyelini analiz ederek, bunları müttefiklerimize ve ortaklarımızın misyonlarına entegre edecek uygulanabilir yol haritaları sunar. Amacımız, teknolojik inovasyonu doğrudan operasyonel değere dönüştürmektir. İnovasyon bizim için bir amaç değil, müttefiklerimizin ve ortaklarımızın en zorlu görevlerini başarmalarını sağlayan bir araçtır. Müşterilerimizin operasyonel gerçekliklerini ve stratejik hedeflerini derinlemesine anlayarak, onlara sadece teknoloji değil, aynı zamanda misyon başarısını garanti eden bütünsel çözümler ve yeni iş modelleri sunarız.

Tehditlerin statik olmadığını biliyoruz. Bu nedenle stratejimiz; Sürekli adaptasyon ve evrim üzerine kuruludur. Geliştirdiğimiz sistemler, yeni tehdit vektörlerini kendiliğinden öğrenerek adapte olur ve geleneksel savunma mekanizmalarının yetersiz kaldığı durumlarda dahi etkili ve caydırıcı bir koruma sağlar.

MİSYONUMUZ

Hızla evrilen ve öngörülemez hale gelen küresel tehditler karşısında misyonumuz nettir: ***Nitelikli insan zekâsını ve üstün teknolojiyle doğru zamanda ve doğru yerde birleştirerek, potansiyel tehditleri birer krize dönüşmeden önce kaynağında etkisiz hale getirmektir****. Heylean olarak, daha güvenli ve istikrarlı bir dünya yaratma taahhüdümüzün arkasında bu stratejik vizyon ve sarsılmaz misyon anlayışı yatmaktadır.*

NEDEN HEYLEAN?

Entropinin Yeni Denklemi: Belirsizliğin Ötesinde

Çünkü biz; ***Güvenlik ve savunma alanında bilinen kuralları yeniden yazıyoruz.*** *Rakiplerimiz sorunları çözerken, biz olasılıkları yeniden şekillendiriyoruz. Bizim için denklem, entropiyi yönetmek, kaosu öngörülebilir bir sisteme dönüştürmek ve belirsizliği müttefiklerimiz ve iş ortaklarımız için stratejik bir avantaja dönüştürmektir.*

DÖRT AŞAMALI ÜSTÜNLÜK

Gürültünün İçerisindeki Sinyal

Her şey veriyle başlar. Ancak veri, tek başına anlamsızdır. Gelişmiş veri füzyonu sistemlerimiz; uydu görüntülerinden (IMINT) siber ağ trafiğine (CYBINT), insan istihbaratından (HUMINT) açık kaynaklara (OSINT) kadar trilyonlarca dağınık veri noktasını tek bir canlı ve bütünsel operasyonel resimde birleştirir.

Reaktif Savunmadan Proaktif Hakimiyete

Sadece olanı görmekle yetinmiyoruz; Olabilecek olanı öngörüyoruz. Bütünsel veri haritası üzerindeki gizli desenleri, anormallikleri ve zayıf korelasyonları analiz ederek, tehditler henüz birer niyetken onları tespit eder. Olası gelecek senaryolarını ve rakip davranışlarını sürekli simüle ederek, iş ortaklarımızın her zaman bir adım önde olmasını ve inisiyatifi ele geçirmesini sağlarız.

Saniyeler İçinde Stratejik Netlik

İnsan zekâsının sınırlarını aşan karmaşıklık seviyelerinde sistemlerimiz en optimal Eylem Planlarını (COA) saniyeler içinde üretir. Her bir planı; Potansiyel risk, başarı olasılığı, kaynak ihtiyacı ve ikincil etkiler gibi kritik metrikler üzerinden analiz eder. Bu, en zorlu anlarda bile komuta kademesine mutlak karar netliği sunarak, karar döngüsünü rakibin algı sınırlarının ötesine taşır.

Her Göreve Özel Çözüm

Teknolojimiz, sahadaki stratejik hedeflerle kusursuz bir uyum içinde çalışmadığı sürece anlamsızdır. Derin teknolojik anlayışımızı, iş ortaklarımızın benzersiz operasyonel ihtiyaçları ve misyon hedefleriyle birleştiriyoruz. Sonuç, sadece teknik olarak çalışan değil, aynı zamanda operasyonel paradigmayı değiştiren, misyon-spesifik çözümlerdir.

TEKNOLOJİ ALTYAPIMIZ

Egemen, Güvenli ve Hiperskale Bulut Mimarisi

Heylean'in teknolojik omurgası, misyon-kritik operasyonların gerektirdiği en üst düzeyde güvenlik, performans ve ölçeklenebilirlik doktrinleri üzerine inşa edilmiştir. Bu mimari, dünyanın en gelişmiş ve güvenilir bulut sağlayıcıları olan Amazon Web Services (AWS) ve Microsoft Azure'un küresel altyapısı üzerinde, kendi mühendislik katmanlarımızla güçlendirilmiştir. Bu stratejik temel müttefiklerimiz ve iş ortaklarımıza her koşulda kesintisiz ve egemen bir operasyon ortamı sunmamızı sağlar.

GÜVENLİK

Güvenlik, altyapımızın tasarımındaki en temel prensiptir. Yaklaşımımız, en katı devlet ve savunma sanayii standartlarını dahi aşacak şekilde, çok katmanlı ve proaktif bir savunma felsefesine dayanır.

Veri Egemenliği ve Sıfır Güven Mimarisi

Tüm veriler, tesislerimizden ayrılmadan önce, fiziksel katmanda otomatik olarak şifrelenir. AWS ve Microsoft Azure'un küresel ağı üzerinden iletilen tüm trafik, izole ve şifreli tünellerde akar. Bu "Sıfır Güven" (Zero Trust) yaklaşımı, hassas verilerin, düzenlemelere tabi iş yüklerinin ve gizli bilgilerin her an mutlak koruma altında olmasını garanti eder. Her bölge, maksimum güvenlik için tamamen ayrılmış kaynaklar ve izole ağ trafiği kullanır.

Erişim Yönetimi

İzinsiz erişim tehdidini ortadan kaldırmak için, endüstri standartlarının çok ötesinde kimlik doğrulama protokolleri kullanıyoruz. Bunlar arasında yazılım tabanlı (SDN) **4 faktörlü kimlik doğrulama (4FA)** ve fiziksel tabanlı (HDN) **5 faktörlü kimlik doğrulama (5FA)** gibi yöntemler bulunmaktadır. Erişim, sadece "bilinmesi gereken" ve "yetkilendirilmiş" prensiplerine göre en granüler seviyede yönetilir.

PROAKTİFLİK

Altyapımız, gelişmiş yapay zekâ destekli izleme sistemleri tarafından 7/24 gözetim altındadır. Bu sistemler, anormallikleri ve potansiyel tehdit vektörlerini anında tespit ederek, tehditler birer soruna dönüşmeden önce otomatik müdahale mekanizmalarını tetikler. Heylean, tam şeffaflık ve kontrol sağlayan, bütünsel olarak yönetilen bir altyapı sunar.

UYUMLULUK

Operasyonlarımız, en güncel ve önde gelen küresel güvenlik ve uyumluluk standartlarına (ISO, SOC, GDPR vb.) tam bağlılık göstermektedir.

OPERASYONEL ÜSTÜNLÜK

Altyapımız, en yoğun veri işleme ve analiz görevleri için tasarlanmıştır. 100 Tbps'nin üzerinde dış ağ kapasitesi ve 1 Pbps'nin üzerinde iç ağ trafiği ile en karmaşık iş yükleri için dahi ultra düşük gecikme süresi ve yüksek performans sunar.

OPERASYONEL SÜREKLİLİK

İş sürekliliği bir seçenek değil, bir garantidir. %99,99 (SLA) kesintisiz çalışma süresi oranıyla, en kritik anlarda bile operasyonlarınızın kesintiye uğramayacağını taahhüt ediyoruz.

TAAHHÜDÜMÜZ

Heylean, müttefiklerine ve iş ortaklarına sadece bugünün değil, yarının da tehditlerine karşı koyabilecek, güvenli, yüksek performanslı ve ölçeklenebilir bir altyapı sağlamaya kendini adamıştır. Teknolojik gelişmelere ve siber güvenlik alanındaki yeniliklere sürekli yatırım yaparak, altyapımızın her zaman endüstri lideri konumunu korumasını sağlıyoruz.

Bu mükemmellik taahhüdü, verilerinizin ve operasyonlarınızın her zaman en üst düzeyde korunduğundan ve optimum performansta çalıştığından emin olmanızı sağlar.

KAPT NEDİR

SİBER SAVUNMADA PARADİGMA DEĞİŞİMİ

Siber savaş alanı, artık statik kalelerin değil, sürekli değişen ve adapte olan tehditlerin arenasıdır. Bu yeni gerçeklik karşısında, ***geleneksel sızma testi metodolojileri – insan uzmanlığına dayalı, zaman alıcı ve kapsamı sınırlı yaklaşımlar – tehlikeli bir şekilde yetersiz kalmaktadır.*** *Kuruluşları, saldırganın temposuna ayak uyduramayan, reaktif bir savunma döngüsüne hapsetmektedirler.*

KAPT; Bir araç değidir. Yapay zekâ tarafından yönetilen, sürekli öğrenen ve adapte olan otonom bir siber saldırı platformudur. Amacı, savunma sistemlerinin sınırlarını, bir insanın hayal gücünün ve dayanıklılığının ötesinde bir hız, yaratıcılık ve derinlikle test etmektir.

BİLİNENİ AVLA, BİLİNMEYENİ KEŞFET

KAPT'ın ezber bozan gücü, insan beyninden ilham alan yapay zekâ çekirdeğinden gelir.

Öngürü Avcısı – Denetimli Öğrenme Algoritması

Öngürü avcısı, bilinen tüm saldırı vektörleri, taktikleri, teknikleri ve prosedürleri (TTPs) üzerinde eğitilmiş bir siber stratejist gibi çalışır. OWASP Top 10 ve CWE Top 25 gibi bilinen zafiyetleri, insan hatasına yer bırakmadan, sistematik ve amansız bir şekilde avlar.

Anomali Kâşifi – Denetimsiz Öğrenme Algoritması

İşte bu, oyunun kurallarının yeniden yazıldığı yerdir. *Bu çekirdek, ne aradığını bilmez; neyin "normal" olduğunu bilir. Sistem davranışlarındaki en ufak anormallikleri, standart dışı veri akışlarını ve beklenmedik korelasyonları tespit ederek, henüz tanımlanmamış "**sıfır gün**" (zero-day) zafiyetlerini ve geleneksel tarayıcıların asla göremeyeceği karmaşık, çok aşamalı saldırı yollarını ortaya çıkarır.*

YANILSAMADAN GERÇEK DAYANIKLILIĞA

*Geleneksel testler, genellikle ~%70'lik bir nüfuz derinliğiyle yetinerek tehlikeli bir "**güvenlik yanılsaması**" yaratır. Bu, sistemlerin duvarlarının sağlam olduğunu düşünürken, gizli tünellerin farkında olmamak gibidir.*

KAPT ise, yapay zekâ ve gerçek zamanlı istihbaratın birleşimiyle bu oranı ***~%96.8*** *gibi devrimsel bir seviyeye taşıyarak,* ***görünmez olanı görünür kılar****.*

KAPT AŞAMALARI

KAPT, statik bir kontrol listesini takip etmez. Her aşaması bir sonrakini besleyen, yapay zekâ tarafından yönetilen dinamik bir operasyonel süreçtir.

I. PLANLAMA VE HAZIRLIK

Bu aşama, KAPT sürecinin temelini oluşturur ve başarılı bir test için kritik öneme sahiptir. Detaylı bir planlama ve hazırlık süreci, olası riskleri minimize eder ve testin verimliliğini maksimize eder.

I.I: KAPSAM BELİRLENMESİ

Hedef sistemlerin belirlenmesi bu aşamanın en önemli adımıdır. Müşteri ile yapılan görüşmeler sonucunda, test kapsamına dahil edilecek sistemler net bir şekilde tanımlanır. Bu aşamada, sistemlerin topolojisi, keypair, şifre, IP bypass gibi hassas bilgileri talep etmiyoruz. Odak noktamız, hangi sistemler üzerinde çalışacağımızı genel hatlarıyla belirlemektir.

I.II: İLETİŞİM PLANLAMASI

Test süreci boyunca kesintisiz ve etkili bir iletişim akışı sağlamak esastır. Bu nedenle, müşteri ile iletişim kanalları (e-posta, telefon, video konferans vb.) belirlenir ve düzenli iletişim planı oluşturulur. Aynı zamanda, beklenmedik durumlar için iletişim protokolleri de tanımlanır.

I.III: ACİL DURUM EYLEM PLANI (ADEP)

Sızma testi sırasında oluşabilecek olası olumsuz durumlar (örneğin, sistemin çökmesi, veri kaybı) için önceden bir eylem planı hazırlanır. Bu plan, olası senaryoları, sorumlulukları ve alınacak önlemleri detaylı bir şekilde içerir.

I.IV: RİSK DEĞERLENDİRMESİ

Hedef sistemler ve test metodolojisi ile ilgili potansiyel riskler, bir risk matrisi kullanılarak değerlendirilir. Risk matrisi, olası risklerin olasılık ve etkisini değerlendirerek, önceliklendirme ve risk azaltma stratejilerinin belirlenmesine yardımcı olur.

I.V: RAPORLAMA

Müşteriye düzenli olarak raporlama yapmak, testin ilerleyişi hakkında bilgi sağlamak ve olası sorunları zamanında ele almak için önemlidir. Bu nedenle, raporlama sıklığı (günlük, haftalık, aylık) müşteri ile birlikte belirlenir.

I.VI: YASAL VE ETİK UNSURLARIN BELİRLENMESİ

KAPT süreci, tüm yasal ve etik kurallara uygun olarak gerçekleştirilir. Test öncesinde, gerekli izinler alınır ve gizlilik politikaları gözden geçirilir.

II. KEŞİF VE BİLGİ TOPLAMA

Bu aşamada, hedef sistemler hakkında mümkün olduğunca fazla bilgi toplanır. Bu bilgi, daha sonraki aşamalarda gerçekleştirilecek saldırıların etkinliğini artırmak için kullanılır. Heylean Teknoloji Anonim Şirketi'nin geliştirdiği Tümleşik İstihbarat Ağı, bu aşamada önemli bir rol oynar.

II.I: TÜMLEŞİK İSTİHBARAT AĞI

STRAINT, OPINT, TACINT, SSBI, CYBINT, SIGINT, GEOPOLINT, ELINT, COMINT, GEOINT, OSINT, FININT, MASINT ve RISKINT gibi istihbarat disiplinleri kullanılarak hedef sistemler hakkında kapsamlı bir bilgi toplama süreci yürütülür. Hangi istihbarat disiplinlerinin kullanılacağı, hedef sistemlerin özelliklerine ve testin kapsamına göre belirlenir. Her sistem için tüm disiplinlerin kullanılması gerekmeyebilir.

II.II: YAPAY ZEKA DESTEĞİ

Denetimli ve Denetimsiz Öğrenme Algoritmaları, toplanan verilerin analiz edilmesi ve anlamlı bilgiler çıkarılması için kullanılır. Bu algoritmalar, büyük veri kümelerini hızlı bir şekilde işleyebilir ve gizli kalmış bağlantıları ortaya çıkarabilir. Örneğin, Denetimsiz Öğrenme algoritmaları, sistemlerdeki anormallikleri tespit etmek için kullanılabilirken, Denetimli Öğrenme algoritmaları, bilinen saldırı kalıplarını tanımak için kullanılabilir.

III. TARAMA VE SINIFLANDIRMA

Bu aşamada, hedef sistemler üzerinde otomatik, manuel tarama ve yapay zeka destekli tarama işlemleri gerçekleştirilir. Tespit edilen güvenlik açıkları, ciddiyetlerine göre sınıflandırılır.

III.I: OTOMATİK TARAMA

Otomatik tarama araçları kullanılarak, sistemlerdeki bilinen güvenlik açıkları tespit edilir. Bu araçlar, hızlı ve etkili bir şekilde geniş bir yelpazede güvenlik açığını tarayabilir.

III.II: YAPAY ZEKA DESTEKLİ TARAMA

Denetimli Öğrenme Algoritması, Denetimsiz Öğrenme Algoritması kullanılarak yapay zeka destekli tarama işlemi gerçekleştirilir. Denetimli Öğrenme Algoritmasında önceden hazırlanan veri setleri üzerinde çalışılır. Denetimsiz Öğrenme Algoritması ile daha önce keşfedilmemiş (Sıfır- Gün) güvenlik zaafiyetleri keşfedilmeye çalışır.

III.III: MANUEL DOĞRULAMA

Otomatik ve Yapay Zeka Destekli Tarama sürecinden sonra en son aşamada güvenlik açıkları manuel olarak taranır ve buna ek olarak otomatik ve yapay zeka destekli tarama süreçlerinde keşfedilen güvenlik açıklıklarının doğrulaması (verification) ve yeniden üretimi (re-produce) işlemi yapılır. Bu sayede yanlış-pozitif (false-positive) hareketler elimine edilir.

IV. RAPORLAMA

Bu aşamada, test sonuçları detaylı bir rapor halinde sunulur. Rapor, tespit edilen güvenlik açıklarını, açıkların etkilerini ve önerilen çözümleri içerir. Rapor, teknik detaylar, açıklamalar ve ekran görüntüleri ile zenginleştirilerek, müşterinin güvenlik açıklarını anlamasını ve gerekli önlemleri almasını sağlar. Rapor, ayrıca, kullanılan metodoloji, test kapsamı ve sınırlamalar hakkında bilgi içerir.

Rapor, tespit edilen her güvenlik açığı için önerilen çözümler ve iyileştirme önerileri sunar. Bu öneriler, müşterinin güvenlik duruşunu güçlendirmesine ve gelecekteki saldırılara karşı korunmasına yardımcı olur.

KAPT, geleneksel sızma testlerine göre daha kapsamlı, hızlı ve etkili bir yaklaşım sunar. Yapay zeka destekli algoritmalar, büyük veri kümelerini analiz ederek gizli kalmış tehditleri ortaya çıkarır ve güvenlik uzmanlarının daha stratejik kararlar almasını sağlar.

KAPT ile müşterilerinin siber güvenlik duruşunu güçlendirmeye ve dijital varlıklarını korumaya yardımcı olur.

KAPT KAPASİTELERİ

OWASP TOP 10

OWASP Top 10, Açık Web Uygulama Güvenligi Projesi (OWASP) tarafından web uygulamalarındaki en kritik güvenlik risklerinin bir listesidir. Bu liste, geliştiricilere, güvenlik uzmanlarına ve kuruluşlara web uygulamalarını daha güvenli hale getirmeleri için farkındalık yaratmayı ve rehberlik etmeyi amaçlamaktadır.

CWE TOP 25

CWE Top 25, yazılım güvenliğinde yaygın olarak görülen ve büyük etkiye sahip 25 güvenlik açığıdır. Bu liste, Common Weakness Enumeration (CWE) tarafından oluşturulmuştur. CWE, yazılım zayıflıklarını ve güvenlik açıklarını kategorize etmek ve tanımlamak için kullanılan bir endüstri standartıdır.

SIFIRINCI GÜN

Sıfırıncı gün açığı, yazılım ve donanımda bulunan ve geliştiriciler tarafından bilinmeyen bir güvenlik açığıdır. Bu açıklar, siber suçlular tarafından sistemlere yetkisiz erişim sağlamak veri çalmak veya diğer kötü amaçlı faaliyetlerde bulunmak için kullanılır.

İÇ RÖLE SALDIRISI

İç Röle Saldırısı bir siber saldırganın, kurbanın iç ağına yetkisiz erişim elde etmek için bir cihazı (genellikle bir bilgisayari veya sunucuyu) bir aracı veya “Röle” olarak kullandığı bir siber saldırı türüdür.

YAN AĞ SALDIRISI

Yapay zeka, bir ağa sızdıktan sonra, hedef sistemlere ulaşmak ve erişim ayrıcalıklarını arttırmak için otomatik olarak yan ağ hareketi gerçekleştirebilir.

SİBER ESPİYONAJ

Siber casusluk olarak da bilinen siber espiyonaj, bir devletin veya devletin desteklediği bir grubun, başka bir devlete, şirkete veya kuruluşa ait bilgisayar sistemlerine ve ağlarına gizlice girerek hassas bilgi ve veri toplama eylemidir.

POLİMORFİK VE METAMORFİK SALDIRILAR

Polimorfik ve metamorfik saldırılar, zararlı yazılımların tespit edilmeyi zorlaştırmak için kullandığı sofistike tekniklerdir.

STEGANOGRAFİ SALDIRISI

Steganografi saldırısı, hassas bilgileri, görünürde zararsız bir taşıyıcı dosyanın (örneğin resim, ses dosyasi, video veya metin) içine gizleyerek yapılan bir siber saldırı türüdür. Bu gizleme işlemi, verilerin varlığını gizlemek ve tespit edilmesini önlemek amacıyla yapılır.

KANALLAMA SALDIRISI

Kanallama saldırısı, bir sistemin güvenlik mekanizmalarını atlatmak için kullanılan dolaylı bir saldırı yöntemidir. Bu saldırılar, bir sistemin performansı, zamanlaması veya diğer görünür yan etkileri gibi "yan kanalları" analiz ederek gizli bilgileri elde etmeye çalışır. Örneğin, bir saldırgan şifreleme anahtarını veya diğer hassas verileri çalmak için bir cihazın güç tüketimindeki küçük değişiklikleri izleyebilir.

HEDEFLEME SALDIRISI

Hedefleme saldırısı, saldırganların belirli bir kişi, kuruluş veya sistemi hedef alarak gerçekleştirdiği siber saldırıdır. Bu saldırılarda, saldırganlar rastgele hedefler yerine belirli bir hedefi seçer ve saldırı o hedefe göre özelleştirilir. Kişi bazında veya kurum bazında gerçekleştirilir.

ZEHİRLENME SALDIRISI

Zehirlenme saldırısı, makine ögrenimi modellerini manipüle etmek için kullanılan bir saldırı türüdür. Saldırgan, modelin eğitim verilerine zararlı veriler enjekte ederek modelin yanlış tahminlerde bulunmasına veya beklenmedik şekilde davranmasına neden olur.

FIREWARE | DONANIM SALDIRISI

Fireware - Donanım saldırısı, kötü niyetli kişilerin bir cihazin fireware ‘ine erişim sağlayıp, kontrol altına alarak gerçekleştirilen bir siber saldırı türüdür. Bu saldırılar genellikle zorlu ve karmaşık olsalar da başarılı olduklarında yıkıcı sonuçlar doğurabilir.

APT SALDIRISI

APT (Advanced Persistent Threat), yani Gelişmiş Kalıcı Tehdit, kuruluşlara veya sistemlere yetkisiz erişim elde etmek ve uzun bir süre boyunca fark edilmeden kalmak amacıyla kullanılan hedefli siber saldırı türüdür. Bu saldırılarda amaç genellikle veri hırsızlığı, casusluk veya sistemlerin sabote edilmesidir.

TEDARİK ZİNCİRİ SALDIRISI

Tedarik zinciri saldırısı, bir kuruluşun ürünlerini veya hizmetlerini sunmak için güvendiği harici tarafları hedef alan bir siber saldırı türüdür.

WATERING-HOLE SALDIRISI

Watering Hole saldırısı, hedeflenen bir gruba veya kuruluşa ait bireyleri enfekte etmek için kullanılan bir siber saldırı yöntemidir. Bu saldırıda, saldırganlar, hedef kitlenin sıklıkla ziyaret ettiği web sitelerini (örneğin, bir sektör forumu veya popüler bir haber sitesi) belirler ve bu sitelere kötü amaçlı yazılımlar yerleştirir. Hedef kitledeki bir kullanıcı bu enfekte web sitesini ziyaret ettiğinde, cihazına kötü amaçlı yazılım bulaşır.

MOBİL CİHAZ SALDIRISI

Mobil cihaz saldırısı, akıllı telefonlar ve tabletler gibi mobil cihazları hedef alan herhangi bir siber saldırı türüdür. Bu saldırılar, cihazda depolanan hassas verilere erişmek, cihazı kontrol etmek, zararlı yazılımlar yüklemek veya cihazın kaynaklarını kullanarak diğer saldırıları gerçekleştirmek amacıyla düzenlenir.

IOT/OT SALDIRISI

IOT/OT saldırıları, internet erişimli cihazların (IOT) ve operasyonel teknoloji (OT) sistemlerinin güvenlik açiklarından yararlanarak gerçekleştirilen siber saldırılardır.

Nesnelerin Interneti (Internet of Things): Günlük hayatta kullandığımız ve internete bağlanılabilen cihazlar (akıllı ev sistemleri, giyilebilir teknolojiler, akıllı şehir altyapıları, tıbbi cihazlar, endüstriyel sensörler vb.)

Operasyonel Teknoloji: Kritik altyapıları, endüstriyel süreçleri ve üretim hatlarını kontrol eden donanım ve yazılımlar (SCADA sistemleri, PL'ler, DCSl'er vb.)

SOSYAL MÜHENDİSLİK

Sosyal mühendislik saldırıları, teknik açıkları değil insan zaaflarını hedef alan siber saldırı türleridir. Saldırganlar, kurbanlarını kandırmak, manipüle etmek ve onlardan bilgi çalmak veya sistemlere yetkisiz erişim sağlamak için psikolojik manipülasyon, aldatma ve güven oluşturma taktikleri kullanırlar.

DEZENFORMASYON SALDIRISI

Dezenformason saldırısı, belirli bir amaca ulaşmak için kasıtlı olarak yanlış bilginin yayılmasıdır. Genellikle bir kitleyi manipüle etmek, kafa karışıklığı yaratmak veya belirli bir görüşü desteklemek için kullanılır. Dezenformasyon, propaganda, karalama kampanyaları ve psikolojik savaş gibi çeşitli şekillerde olabilir.

TEMPEST SALDIRISI

Tempest saldırısı, bir cihazin yaydığı elektromanyetik dalgaları analiz ederek bilgi almaya çalışan bir yan kanal saldırısıdır. Normalde bilgisayarlar, monitörler, klavyeler gibi elektronik cihazlar çalışırken elektromanyetik dalgalar yayarlar. Bu dalgalar görünmez olsalar da özel ekipmanlarla algılanabilir ve analiz edilebilirler.

SİBER PANİK SALDIRISI

Siber panik saldırısı, bir sistem veya ağa yönelik gerçek bir siber saldırı tehdidinin yanlış bir şekilde abartılması veya tamamen uydurulmasıyla gerçekleştirilen bir sosyal mühendislik alt dal saldırısıdır. Amaç, korku ve panik yaratarak kurbanların mantıklı düşünme yeteneğini zayıflatmak ve onları aceleci ve hatalı kararlar almaya zorlamaktır.

DÜŞMAN YAPAY ZEKA SALDIRISI

Düşman yapay zeka (DYA) saldırısı, bir saldırganın yapay zeka (YZ) sistemlerini ve algoritmalarını hedef alarak, işlevlerini bozmak, manipüle etmek veya kontrol altına almak için kullandığı kötü amaçlı bir eylemdir.

FİZİKSEL HACKING SALDIRISI

Fiziksel hacking saldırısı, bir sistemin güvenliğini aşmak için fiziksel erişim, sosyal mühendislik taktikleri veya her ikisinin bir kombinasyonunu kullanan bir siber saldırı türüdür. Bu saldırı türü, saldırganın dogrudan bilgisayar sistemine, ağ donanımına veya verilere fiziksel olarak erişmesiyle karakterizedir.

KUANTUM SALDIRISI

Kuantum saldırısı, kuantum bilgisayarların gücünü kullanarak günümüz kriptografi algoritmalarını kırmaya yönelik teorik bir saldırı türüdür. Klasik bilgisayarlar, bilgileri 0 veya 1 bitleri olarak temsil eden transistörler kullanırken, kuantum bilgisayarlar kubitleri kullanırlar. Kubitler, süperpozisyon ilkesiyle aynı anda hem 0 hem de 1 olabilme yeteneğine sahiptir. Bu durum, kuantum bilgisayarların belirli hesaplamaları klasik bilgisayarlardan çok daha hızlı gerçekleştirmesine olanak tanır.

SİBER DRONE SALDIRISI

Drone ile gerçeklestiriten siber saldırılar, saldırganların bir hedefe karşı siber saldırı başlatmak veya kolaylaştırmak için insansız hava araçlarını (IHA'lar) kullandığı durumlardır. Bu saldırılar çeşitli şekillerde olabilir ve giderek artan bir tehdit oluşturmaktadır.

OSI KATMANLARI

KAPT, OSI modelinin tüm yedi katmanında ve TEMPEST saldırıları dahil olmak üzere kapsamlı sızma testleri gerçekleştirebilir. KAPT, gelişmiş yapay zeka algoritmaları kullanarak geleneksel sızma testi yöntemlerinin ötesine geçer ve daha hızlı, daha etkili ve daha kapsamlı güvenlik analizleri sağlar. Aşağıda, her katman için KAPT'ın yeteneklerinin detaylı bir açıklaması yer almaktadır.

FİZİKSEL KATMAN (PYHSICAL LAYER)

KAPT, fiziksel katmanda TEMPEST saldırıları gibi tehditleri tespit etmek ve analiz etmek için kullanılabilir. Bu, elektromanyetik emisyonları analiz ederek veri sızıntılarını tespit etmeyi ve ağ kablolarına fiziksel erişimle gerçekleştirilebilecek saldırıları simüle etmeyi içerir. Ayrıca, fiber optik kablolar üzerindeki ışık sızıntılarını analiz ederek veri hırsızlığı girişimlerini tespit edebilir.

VERİ BAĞLANTI KATMANI (DATA LINK LAYER)

Bu katmanda, KAPT MAC adresi sahteciliği, ARP zehirlenmesi, VLAN atlama ve STP manipülasyonu gibi saldırıları simüle edebilir. KAPT, ağ trafiğini analiz ederek anormallikleri tespit edebilir ve potansiyel saldırı vektörlerini belirleyebilir. Örneğin, KAPT, aynı MAC adresine sahip birden fazla cihaz tespit ederek MAC adresi sahteciliğini ortaya çıkarabilir veya ARP istek ve yanıtlarını izleyerek ARP zehirlenmesi saldırılarını tespit edebilir. KAPT ayrıca, ağ segmentleri arasında yetkisiz erişimi tespit etmek için STP konfigürasyonlarını analiz edebilir.

AĞ KATMANI (NETWORK LAYER)

KAPT, IP sahteciliği, ICMP tünelleme, yönlendirme protokolü saldırıları ve hizmet reddi (DoS) saldırıları gibi ağ katmanı saldırılarını simüle edebilir ve tespit edebilir. KAPT, ağ trafiğini analiz ederek anormal IP adreslerini veya paket akışlarını tespit edebilir ve potansiyel saldırı kaynaklarını belirleyebilir. Ayrıca, yönlendirme tablolarını analiz ederek ve manipüle edilmiş yönlendirme güncellemelerini tespit ederek yönlendirme protokolü saldırılarına karşı koruma sağlayabilir.

TAŞIMA KATMANI (TRANSPORT LAYER)

KAPT, TCP SYN flood, UDP flood, bağlantı noktası tarama ve bağlantı ele geçirme gibi taşıma katmanı saldırılarını tespit edebilir ve analiz edebilir. KAPT, ağ trafiğini gerçek zamanlı olarak izleyerek ve anormal bağlantı girişimlerini veya paket akışlarını tespit ederek bu tür saldırıları belirleyebilir. Ayrıca, sistem kaynaklarını tüketen ve hizmet kesintilerine neden olan DoS saldırılarını tespit edebilir ve analiz edebilir.

OTURUM KATMANI (SESSION LAYER)

KAPT, oturum yönetimi protokollerindeki güvenlik açıklarını tespit etmek için kullanılabilir. Bu, yetkisiz oturum açma girişimlerini tespit etmeyi, oturum ele geçirme saldırılarını simüle etmeyi ve oturum yönetimi mekanizmalarındaki zayıflıkları belirlemeyi içerir.

KAPT, oturum verilerini analiz ederek ve anormallikleri tespit ederek potansiyel güvenlik açıklarını belirleyebilir.

SUNUM KATMANI (PRESENTATION LAYER)

KAPT, veri şifreleme ve kod çözme mekanizmalarındaki güvenlik açıklarını tespit edebilir. Bu, zayıf şifreleme algoritmalarını tespit etmeyi, şifreleme anahtarlarını kırmaya çalışmayı ve veri bütünlüğünü doğrulamayı içerir.

KAPT, farklı şifreleme algoritmalarını test edebilir ve bunların kırılmaya karşı direncini değerlendirebilir.

UYGULAMA KATMANI (APPLICATION LAYER)

KAPT, web uygulaması güvenlik açıklarını (SQL enjeksiyonu, çapraz site komut dosyası oluşturma, oturum yönetimi açıkları vb.), API güvenlik açıklarını ve diğer uygulama katmanı saldırılarını tespit edebilir ve analiz edebilir. KAPT, web uygulamalarına otomatik olarak saldırılar gerçekleştirebilir ve güvenlik açıklarını tespit etmek için sonuçları analiz edebilir.

Ayrıca, API'leri test ederek ve yetkisiz erişimi veya veri sızıntılarını tespit ederek API güvenliğini değerlendirebilir.

KAPT, yapay zeka ve makine öğrenmesi algoritmalarını kullanarak bu katmanlardaki saldırıları tespit etmede ve analiz etmede üstün performans gösterir. Sürekli öğrenme yeteneği sayesinde, yeni tehditleri ve saldırı yöntemlerini hızla adapte edebilir ve daha etkili savunma stratejileri geliştirebilir.

KAPT vs RAKİPLERİMİZ

KAPT, yapay zeka destekli C5ISR çözümleri alanında yenilikçi ve ileri seviye teknolojiler geliştirmekteyiz. Yapay zeka destekli sızma testi hizmetimiz, rakiplerimizden farklılaşan benzersiz özellikler sunmaktadır.

Statik ve kural tabanlı yaklaşımlara bağımlıdır

Bu yaklaşımlar, bilinen zafiyetleri tespit etmede etkili olabilir ancak sıfırıncı gün açıkları ve gelişmiş kalıcı tehditler gibi karmaşık saldırılara karşı yetersiz kalmaktadır.

KAPT ise, sürekli öğrenen ve dinamik tehdit ortamına adapte olabilen yapay zeka algoritmaları kullanarak daha kapsamlı ve proaktif bir sızma testi hizmeti sunar.

Sınırlı otomasyon sunar

Manuel sızma testi süreçleri zaman alıcı ve pahalıdır.

KAPT, yapay zeka destekli otomasyon sayesinde test sürecini hızlandırır, maliyetleri düşürür ve insan kaynaklı hataları minimize eder.

İstihbaratı entegre etmede yetersiz kalır

Rakiplerimizin birçoğu, güncel tehdit verilerini sızma testlerine entegre etmede zorlanır.

KAPT, gerçek zamanlı istihbarat kullanarak saldırı simülasyonlarını daha gerçekçi ve etkili hale getirir.

Raporlama ve görselleştirme konusunda eksiktir

Karmaşık verileri anlaşılır bir şekilde sunmak, etkili bir sızma testi için kritik öneme sahiptir.

KAPT, kullanıcı dostu arayüzü ve özelleştirilebilir raporlama özellikleriyle, güvenlik açıklarını ve riskleri net bir şekilde ortaya koyar ve aksiyon alınabilir bilgiler sunar.