Analyzer 2025: Proaktif Siber Savunma için Son Teknoloji IP ve URL Analizi

I. Yönetici Özeti

Bu rapor, Analyzer'ın 2025 yılı için proaktif siber güvenlik yeteneklerini geliştirmek amacıyla kritik öneme sahip en iyi 10 gelişmiş IP ve URL analiz tekniğini ve eğilimini ayrıntılarıyla ele almaktadır. Siber güvenlik ortamı, yapay zeka odaklı tehditler, hibrit ortamlar (BT, Nesnelerin İnterneti (IoT), Operasyonel Teknoloji (OT), Tıbbi Nesnelerin İnterneti (IoMT)) genelinde genişleyen saldırı yüzeyleri ve reaktif önlemlerden sürekli tehdit maruziyeti yönetimine doğru temel bir kayma ile hızla gelişmektedir.

Belirlenen eğilimler, gelişmiş tespit ve otomasyon için Yapay Zeka (YZ) ve Makine Öğrenimi'nin (ML) entegrasyonunu, bağlamsal ve risk tabanlı önceliklendirmenin gerekliliğini, kimlik merkezli güvenliğe (Sıfır Güven) geçişi ve dinamik dijital ekosistemler genelinde sürekli izlemenin kritik ihtiyacını vurgulamaktadır. Analyzer, temel IP ve URL analiz yetenekleriyle, daha akıllı, kapsamlı ve eyleme geçirilebilir güvenlik bilgileri sunmak için bu eğilimlerden yararlanmak üzere benzersiz bir konumdadır.

Bu son teknoloji teknikleri benimseyerek, Analyzer geleneksel taramanın ötesine geçerek saldırı vektörleri hakkında daha derin bilgiler sağlayabilir, daha kesin savunma önerileri sunabilir ve yüksek düzeyde bağlamsallaştırılmış risk değerlendirmeleri sunarak kullanıcılarının sofistike siber tehditlere karşı direncini önemli ölçüde güçlendirebilir.

II. Giriş: Gelişen Siber Ortamda Analyzer'ın Vizyonu

Analyzer'ın temel misyonu, siber güvenlik zafiyetlerini proaktif bir şekilde belirlemek, potansiyel saldırı yöntemlerini analiz etmek, somut savunma önerileri sunmak ve risk puanlaması sağlamaktır. Bu amaçla Nmap, Nikto, Gobuster, WPScan, SSLScan, ARP-scan ve Whois gibi popüler güvenlik araçlarını tek bir çatı altında toplayarak tarama sürecini otomatikleştirir ve basitleştirir. Proje, sızma testi uzmanlarına ve sistem yöneticilerine hızlı ve etkili analiz yeteneği sunarken, güvenlik bilinci düşük veya teknik bilgisi olmayan kullanıcılar için de anlaşılır raporlar sunarak güvenlik önlemlerinin alınmasını teşvik etmeyi amaçlamaktadır.

Dijital ortam giderek daha karmaşık hale gelmekte, siber saldırılar her geçen gün daha da sofistikeleşmektedir. Bu durum, savunma stratejilerinin sürekli evrimini zorunlu kılmaktadır. 2025 yılı, Yapay Zeka'nın hem saldırı hem de savunma cephelerinde yaygın etkisi, bulut ve Nesnelerin İnterneti (IoT)/Operasyonel Teknoloji (OT) benimsenmesiyle

saldırı yüzeylerinin genişlemesi ve tedarik zinciri zafiyetlerine artan odaklanma gibi önemli değişimlere tanık olacaktır. Kullanıcı sorgusunda belirtildiği gibi, "Siber saldırılar her geçen gün daha da karmaşıklaşıyor. Analyzer ile web sitenizi ya da kullandığınız cihazları URL veya IP adresleri üzerinden derinlemesine analiz ederek hem saldırı vektörlerini tespit edebilir hem de savunma mekanizmalarınızı güçlendirebilirsiniz. Geleceğin siber güvenlik ihtiyaçlarına bugünden hazırlanın!" Bu aciliyet, "Siber suçun otomasyon, yapay zeka ve gelişmiş sosyal mühendisliği kullanarak saldırıları ölçeklendirmek ve etkiyi maksimize etmek için oldukça verimli bir iş haline geldiği" [3] ve "Dijital ekosistemlerin artan bulut benimsenmesi nedeniyle yayılmaya devam ettiği, tehdit ortamının yeni yeteneklerin saldırganları cesaretlendirmesiyle gelişmeye devam ettiği" [31] raporlarıyla daha da pekişmektedir.

Geleneksel, statik IP ve URL analizi, temel olsa da, artık yeterli değildir. Modern ağların dinamik doğası, bulut hizmetlerinin, IoT cihazlarının yaygınlaşması ve polimorfik ve dosyasız saldırıların artan karmaşıklığı, daha akıllı, gerçek zamanlı ve bağlamsal analiz yetenekleri gerektirmektedir. Fikri mülkiyet ortamının teknolojik gelişmelerle hızla dönüştüğü bir dönemde [32], Analyzer'ın evrimi, proaktif siber savunmanın ön saflarında kalmak için bu gelişmiş teknikleri benimsemeyi zorunlu kılmaktadır.

III. 2025 İçin En İyi 10 Gelişmiş IP ve URL Analiz Tekniği/Eğilimi

Aşağıdaki tablo, 2025 yılı için belirlenen en etkili IP ve URL analiz tekniklerini özetlemektedir. Bu tablo, her bir tekniğin temel işlevini ve Analyzer için sağlayacağı birincil faydayı hızlıca kavramak amacıyla tasarlanmıştır. Bu özet, raporun daha detaylı bölümlerine geçmeden önce okuyucunun genel bir bakış açısı kazanmasına olanak tanır. Bir ürün yöneticisi veya baş geliştirici gibi yoğun bir teknik profesyonelin, raporun kapsamını ve temel önerilerini hızla anlaması için bu tür bir özet büyük değer taşır. Bu yapı, karmaşık teknik bilgilerin anında özümsenmesini sağlayarak bilgi yüklemesini önler ve raporun genel okunabilirliğini ve kullanışlılığını artırır.

Tablo 1: 2025 İçin En İyi 10 IP ve URL Analiz Tekniğinin Özeti

Teknik/Eğilim Başlığı	Kısa Açıklama	Analyzer İçin Birincil Fayda
1. YZ Destekli Davranışsal Anomali Tespiti	YZ/ML kullanarak normal ağ trafiği modellerini belirler ve sapmaları tespit eder, bilinen imzaların ötesinde yeni tehditleri ortaya çıkarır.	Gizli veya bilinmeyen tehditlerin, iç tehditlerin ve sofistike saldırıların gerçek zamanlı tespiti.

2. Büyük Dil Modeli (LLM) Destekli Tehdit İstihbaratı ve Analizi	Ağ verilerini, tehdit istihbaratını ve güvenlik günlüklerini işleyerek anomali tespiti, kimlik avı analizi ve olay müdahalesi için bağlamsal zeka sağlar.	Karmaşık güvenlik verilerinin yorumlanması, gelişen saldırı modellerinin tahmini ve daha kesin risk değerlendirmeleri.
3. Dinamik IP/URL Varlıkları için Sürekli Tehdit Maruziyeti Yönetimi (CTEM)	Siber güvenliği reaktif olmaktan proaktif hale getirerek, saldırı yüzeyinin sürekli tanımlanması, değerlendirilmesi ve azaltılması.	Saldırı yüzeyinin gerçek zamanlı görünürlüğü, dinamik varlık envanteri güncellemeleri ve iş etkisi odaklı önceliklendirme.
4. YZ Otomasyonlu Gelişmiş Harici Saldırı Yüzeyi Yönetimi (EASM)	Kuruluşun internete açık dijital varlıklarının (gölge BT dahil) sürekli tanımlanması, izlenmesi ve azaltılması.	Bilinmeyen veya yönetilmeyen dışa açık varlıkların otomatik keşfi ve saldırı vektörlerinin kapsamlı bir şekilde haritalanması.
5. Cihaz Duruş Değerlendirmesi ile Sıfır Güven Ağ Erişimi (ZTNA)	Tüm kullanıcıların ve cihazların sürekli kimlik doğrulaması ve güvenlik duruşu doğrulamasına dayalı erişim kontrolü.	Ağ etkinliğini kullanıcı ve cihaz güvenilirliği ile ilişkilendirerek daha ayrıntılı risk değerlendirmeleri.
6. IP/URL İstihbaratı Yoluyla Geliştirilmiş Tedarik Zinciri Risk Yönetimi	Üçüncü taraf satıcılar, açık kaynaklı bileşenler ve bulut hizmetleri aracılığıyla tedarik zinciri risklerinin proaktif olarak belirlenmesi ve yönetilmesi.	Üçüncü taraf varlıklarındaki zafiyetlerin tespiti ve tedarik zinciri risklerinin kapsamlı bir görünümü.
7. IoT/OT/IoMT Cihaz Güvenliği Analizi	Operasyonel teknoloji, tıbbi cihazlar ve IoT cihazlarındaki özel zafiyetlerin belirlenmesi ve risklerin azaltılması.	Kritik altyapı ve fiziksel sistemler için özelleştirilmiş güvenlik analizleri ve savunma önerileri.
8. URL/IP Bağlamı ile Gelişmiş Kimlik Avı ve Sosyal Mühendislik Tespiti	YZ destekli içerik analizi ve itibar kontrolleri kullanarak sofistike kimlik avı ve sosyal mühendislik saldırılarının tespiti.	Gelişmiş kimlik avı URL'lerinin ve aldatıcı içeriklerin tespiti, insan faktörüne yönelik tehditlere karşı koruma.

9. Buluta Özgü Zafiyet Tarama ve Duruş Yönetimi	Bulut ortamlarındaki (IaaS, PaaS, kapsayıcılar) yanlış yapılandırmaların ve zafiyetlerin sürekli izlenmesi ve yönetimi.	Bulut tabanlı varlıklar için kapsamlı zafiyet tespiti ve bulut güvenlik duruşunun iyileştirilmesi.
10. İş Bağlamı ve Tahmine Dayalı Analiz ile Otomatik Risk Puanlaması	Risk değerlendirmelerini gerçek zamanlı veriler, iş önemi ve tahmine dayalı modellerle dinamik olarak günceller.	Teknik zafiyetleri iş etkisiyle ilişkilendirerek eyleme geçirilebilir, öncelikli risk değerlendirmeleri.

---

1. YZ Destekli Davranışsal Anomali Tespiti (IP ve URL Trafiği İçin)

Bu teknik, Yapay Zeka (YZ) ve Makine Öğrenimi (ML) algoritmalarını kullanarak belirli IP'ler ve URL'lerle ilişkili "normal" ağ trafiği modellerinin temel çizgilerini oluşturmayı ve bu temel çizgilerden sapmaları tespit etmeyi içerir. Geleneksel imza tabanlı tespitin aksine, bilinen kalıplarla eşleşmeyen yeni tehditleri, iç tehditleri ve sofistike saldırıları belirleyebilir. Bu, olağandışı oturum açma zamanları, veri transferleri, sistem erişim kalıpları veya harici alan adlarıyla/IP'lerle iletişim gibi durumları içerir.[1] YZ ve ML, güvenlik otomasyonunu ve tehdit tespitini artırmak için giderek daha fazla kullanılmaktadır.[2]

2024-2025 yıllarında siber tehditler daha karmaşık hale geldikçe ve tespitlerin önemli bir kısmı kötü amaçlı yazılım içermedikçe (%79'u kötü amaçlı yazılım içermeyen tespitler [3]), YZ destekli anomali tespiti gerçek zamanlı tehdit belirleme için hayati önem taşımaktadır. Bu yaklaşım, Analyzer'ın geleneksel port/hizmet taramasının (Nmap gibi) ötesine geçerek bağlı cihazların ve erişilen URL'lerin *davranışını* analiz etmesini sağlar. Bu sayede Analyzer, yanal hareket [4], veri sızdırma veya botnet etkinliği gibi gizli ihlal göstergelerini, başlangıçtaki erişim meşru olsa bile tespit edebilir. Büyük Dil Modelleri (LLM'ler) de büyük ağ verilerini gerçek zamanlı olarak analiz ederek anormallikleri ve potansiyel tehditleri tespit edebilir.[5] Bu tekniğin uygulaması, finansal işlemlerde dolandırıcılık tespiti ve iletişim modellerindeki değişiklikleri izleyerek ele geçirilmiş cihazların belirlenmesini kapsar.[1]

Bu alandaki gelişmeler, Analyzer'ın geleneksel imza tabanlı tarama yöntemlerinin sınırlamalarının ötesine geçme zorunluluğunu ortaya koymaktadır. Analyzer'ın mevcut araçları (Nmap, Nikto, WPScan gibi) genellikle bilinen zafiyet imzalarına dayanır. Ancak, modern saldırıların %79'unun kötü amaçlı yazılım içermediği gözlemi [3], bu geleneksel yöntemlerin güncel tehdit ortamında yetersiz kalabileceğini açıkça göstermektedir. Bu durum, yalnızca bilinen kötü amaçlı yazılım imzalarına güvenmek yerine, davranışsal

anormalliklere odaklanmanın neden kritik olduğunu vurgular. Siber saldırganlar, imzaları atlatmak için sürekli yeni yöntemler geliştirdiğinden, savunma mekanizmalarının da bu evrime ayak uydurması gerekmektedir.

Ayrıca, "normal" davranışın tanımlanması, IP ve URL trafiği için oldukça bağlamsal ve dinamik bir zorluktur. Bu durum, doğru bir tespit için önemli bir engel teşkil etse de, iç tehditlere ve gizli ihlallere karşı güçlü bir savunma mekanizması sunar.[1] Analyzer'ın "risk puanlaması ile güvenlik durumunun genel bir değerlendirmesini sağlama" ve "siber bağlamıyla analizler gerçekleştirme" hedefleri göz önüne alındığında, bu bağlamsal "normalliği" tanımlama yeteneği büyük önem taşır. Örneğin, bir ağ yöneticisinin normal çalışma saatleri dışında hassas verilere erişmesi, belirli bir bağlamda meşru olabilirken, başka bir bağlamda şüpheli bir davranış olarak algılanabilir. Analyzer'ın YZ/ML yetenekleri, farklı kullanıcılar, cihazlar ve ağ segmentleri için bağlamsal "normalliği" öğrenme ve buna adapte olma konusunda yeterince sofistike olmalıdır. Bu, yanlış pozitifleri en aza indirmek ve gerçek anormallikleri doğru bir şekilde işaretlemek için sürekli öğrenme modellerine veya kullanıcı tanımlı temel çizgilere ihtiyaç duyulduğu anlamına gelir.

2. Büyük Dil Modeli (LLM) Destekli Tehdit İstihbaratı ve Analizi

Büyük Dil Modelleri (LLM'ler), büyük miktardaki ağ verilerini, tehdit istihbaratı akışlarını ve güvenlik günlüklerini gerçek zamanlı olarak işlemek ve analiz etmek için uyarlanmaktadır. Bu yetenek, anormalliklerin tespit edilmesini, metni kötü niyetli amaçlar açısından analiz ederek kimlik avı girişimlerinin belirlenmesini, olay müdahalesinde hafifletme stratejileri önermeyi ve hatta saldırı nedenlerini belirlemek için günlükleri ayrıştırarak siber adli bilişime yardımcı olmayı mümkün kılar.[5] Ayrıca, kırmızı takım (red teaming) çalışmaları için saldırı örnekleri üretebilir ve Saldırı Tespit Sistemlerinin (IDS) sağlamlığını artırabilirler.[6]

2024-2025 yıllarında LLM'ler, Analyzer'ın karmaşık güvenlik verilerini yorumlama yeteneğini önemli ölçüde artırarak, ham tarama sonuçlarının ötesinde bağlamsal tehdit istihbaratı sağlamasına olanak tanıyacaktır. IP ve URL analizi için LLM'ler, Whois aramalarından [77] elde edilen bilgileri, Nmap taramalarını ve web içeriğini (WPScan, Nikto) küresel tehdit istihbaratıyla [24] ilişkilendirerek gelişmekte olan saldırı modellerini belirleyebilir, zafiyetleri tahmin edebilir ve daha ayrıntılı risk değerlendirmeleri sunabilir. Özellikle kimlik avı tespitinde [5] URL özelliklerini ve e-posta içeriğini analiz ederek oldukça etkilidirler ve hatta savunmaları test etmek için simüle edilmiş saldırı trafiği üretebilirler.[6] Saldırganların sosyal mühendislik ve YZ tarafından oluşturulan e-postalar ve web siteleri için üretken YZ'yi giderek daha fazla kullanması [3], LLM destekli savunmayı kritik hale getirmektedir.

LLM'lerin bu alandaki kullanımı, Analyzer'ın statik zafiyet analizinin ötesine geçerek dinamik ve adaptif bir analiz katmanı sunmasını sağlar. Geleneksel araçlar, teknik zafiyetleri (örneğin, SQL enjeksiyonu, XSS) tespit etmeye odaklanırken, LLM'ler bir URL'nin veya e-posta içeriğinin arkasındaki aldatıcı *niyeti* ve bağlamı anlayabilir. Bu, sofistike sosyal mühendislik ve kimlik avı saldırılarıyla mücadele etmek için hayati öneme sahiptir. Analyzer'ın, LLM'leri entegre ederek URL'lerin ve ilişkili içeriklerin (web kazıma veya e-posta analizinden elde edilenler gibi) daha derin, anlamsal bir analizini gerçekleştirmesi mümkündür. Bu yetenek, yalnızca teknik kontrolleri aşan sosyal mühendislik taktiklerini belirlemesini sağlayarak, Analyzer'ın "siber saldırı ve savunma önerileri" yeteneklerine önemli bir boyut katacaktır.

Ancak, LLM'ler güçlü savunma araçları olsalar da, kendileri de yeni zafiyetler (örneğin, istem enjeksiyonu, veri zehirlenmesi) sunmaktadır ve saldırganlar bu zafiyetleri istismar edebilirler.[5] Bu durum, Analyzer'ın kendi LLM entegrasyonunun da güvenli olması gerektiği anlamına gelir. Eğer Analyzer LLM'leri entegre ederse, bu zafiyetler Analyzer'ın kendi sisteminin zafiyetleri haline gelebilir. Bir saldırgan, Analyzer'ın LLM'sini manipüle ederek yanlış pozitifler üretmesine, gerçek tehditleri gözden kaçırmasına veya hatta Analyzer sistemini ele geçirmesine neden olabilir. Bu nedenle, Analyzer'ın geliştirme ekibi, entegre edilen herhangi bir LLM için sağlam güvenlik önlemleri uygulamaya öncelik vermelidir. Bu, girdi doğrulama, çıktı temizleme ve modelin kendisine yönelik düşmanca saldırıları tespit etmek için LLM'nin davranışının ve performansının sürekli izlenmesini içermelidir.

3. Dinamik IP/URL Varlıkları için Sürekli Tehdit Maruziyeti Yönetimi (CTEM)

CTEM, siber güvenliği reaktif olay müdahalesinden, tehditlerin sürekli tanımlanması, değerlendirilmesi ve azaltılmasına yönelik proaktif bir yaklaşıma dönüştüren beş aşamalı bir metodolojidir (Kapsam Belirleme, Keşif, Önceliklendirme, Doğrulama, Mobilizasyon).[9] Bu, bir kuruluşun dış saldırı yüzeyini ve SaaS güvenlik duruşunu sürekli olarak değerlendirmeyi, yalnızca CVE'lerin (Ortak Zafiyetler ve Maruziyetler) ötesinde varlıkları keşfetmeyi ve riskleri değerlendirmeyi (yanlış yapılandırmalar dahil), ve tehditleri yalnızca teknik puanlara göre değil, iş etkisi ve istismar edilebilirliğe göre önceliklendirmeyi içerir.[10]

2024-2025 yıllarında dijital ortamların hızla değişmesi [12] ve bulut ile üçüncü taraf hizmetlerinin yayılması [13] göz önüne alındığında, bir kuruluşun saldırı yüzeyinin güncel bir şekilde anlaşılmasını sürdürmek için CTEM hayati önem taşımaktadır. Analyzer için bu, tek seferlik taramaların ötesine geçerek IP adresleri, URL'ler ve ilişkili cihazların sürekli izlenmesi anlamına gelir. Bu, Analyzer'ın varlık envanterini dinamik olarak güncellemesine, yeni ortaya çıkan hizmetleri veya yanlış yapılandırmaları tespit

etmesine ve YZ destekli risk puanlaması ve saldırı yolu analizi [9] kullanarak zafiyetleri gerçek dünya istismar edilebilirliği ve iş kritikliği temelinde önceliklendirmesine olanak tanır. Bu, Analyzer'ın proaktif tanımlama ve risk puanlama özelliklerini doğrudan geliştirir.

CTEM, Analyzer'ın operasyonel modelini, geleneksel Nmap/Nikto taramaları gibi "anlık görüntü" zafiyet değerlendirmeleri sunmaktan, bir kuruluşun güvenlik duruşunun sürekli, yaşayan bir görünümünü sunmaya doğru temelden değiştirmektedir. Bu, dinamik bulut ve hibrit ortamlarda kritik öneme sahiptir. Geleneksel zafiyet tarama araçları, genellikle belirli aralıklarla taramalar yaparak o *anlık* zafiyet durumunu yansıtır. Ancak, bulut ortamları ve modern ağlar sürekli değişmektedir.[12] Bu durum, geleneksel tarama yöntemlerinin yetersiz kalmasına neden olur. Analyzer'ın, IP/URL varlık envanterinin ve zafiyet durumunun sürekli izlenmesini ve gerçek zamanlı güncellemelerini desteklemek için mimarisini geliştirmesi gerekmektedir. Bu, bir "tarama-ve-raporlama" modelinden, "izleme-değerlendirme-önceliklendirme-doğrulama-mobilizasyon" döngüsüne geçiş yaparak, periyodik raporlar yerine sürekli güvenlik duruşu yönetimi sağlaması anlamına gelir.

Zafiyetlerin önceliklendirilmesinde iş etkisi ve varlık kritikliğine yapılan vurgu [10], Analyzer'ın "risk puanlaması"nın yalnızca teknik CVSS puanlarının ötesine geçerek kurumsal bağlamı da içerecek şekilde evrilmesi gerektiğini göstermektedir. Analyzer'ın mevcut tanımında "Risk puanlaması ile güvenlik durumunun genel bir değerlendirmesini sağlar" ifadesi yer almaktadır. Eğer bu risk puanlaması sadece teknik ise, bir kuruluşun gerçek iş öncelikleriyle uyumlu olmayabilir. Bu durum, Analyzer'ın risk puanlama algoritmasının, kullanıcıların farklı varlıklar veya veri türleri için iş kritikliğini (örneğin, "crown jewels" olarak kabul edilen varlıklar, gelir için kritik uygulamalar, belirli hizmetler için kesinti süresinin etkisi) tanımlamasına ve girmesine izin verecek şekilde yapılandırılması gerektiğini gösterir. Çıktı, hem teknik ciddiyeti hem de iş etkisini yansıtan bir risk puanı sunmalı ve potansiyel olarak belirli bir zafiyetin *kendi* kuruluşları için neden kritik olduğunu açıklayan net bir anlatım içermelidir. Bu, Analyzer'ı teknik bir araçtan siber güvenlik için stratejik bir iş kolaylaştırıcıya dönüştürecektir.

4. YZ Otomasyonlu Gelişmiş Harici Saldırı Yüzeyi Yönetimi (EASM)

EASM, bir kuruluşun internete açık dijital varlıklarının sürekli olarak tanımlanması, izlenmesi ve azaltılması sürecidir. Bu, alan adlarını, IP adreslerini, web uygulamalarını ve bulut hizmetlerini içerir; bunların çoğu (gölge BT, üçüncü taraf hizmetleri veya yanlış yapılandırmalar nedeniyle) kuruluş tarafından bilinmeyebilir.[12] EASM araçları, tüm dışa

dönük altyapıyı haritalamak ve saldırganların istismar edebileceği potansiyel giriş noktalarını vurgulamak için keşif ve tarama gibi otomatik keşif süreçlerinden yararlanır.[12]

2024-2025 yıllarında kuruluşlar bulut ve üçüncü taraf hizmetlerini giderek daha fazla benimsediğinden, dış saldırı yüzeyleri hızla genişlemektedir.[12] Bu büyümeye ve gölge BT'nin ortaya çıkışına ayak uydurmak için, özellikle YZ destekli otomasyonla EASM, isteğe bağlı olmaktan çıkmıştır.[13] Analyzer, bilinmeyen internete açık varlıkları hedef IP veya URL'ye bağlı olarak otomatik olarak keşfetmek için EASM prensiplerini entegre edebilir ve bir kuruluşun dijital ayak izinin daha eksiksiz bir resmini sağlayabilir. Bu, alt alan adlarının, ilişkili bulut kaynaklarının ve yanlış yapılandırılmış halka açık uygulamaların belirlenmesini içerir. EASM'nin geleceği, otomasyon odaklı tehdit tespitinde ve daha geniş risk yönetimi platformlarıyla entegrasyonda yatmaktadır.[12]

EASM, Analyzer'ın yalnızca *belirlenen* hedefleri analiz etme kapsamının ötesine geçerek, bir kuruluşun *bilinmeyen* veya *yönetilmeyen* internete açık varlıklarını (gölge BT, üçüncü taraf hizmetleri, yanlış yapılandırmalar) keşfetmesine odaklanmaktadır. Bu bilinmeyen varlıklar, saldırganlar için genellikle ilk giriş noktalarıdır.[12] Analyzer'ın mevcut tanımı, "belirlenen hedefler üzerindeki potansiyel güvenlik açıklarını hızlı ve etkili bir şekilde analiz etme yeteneği sunmaktır" ifadesini içermektedir. Eğer Analyzer sadece kendisine bildirilen hedefleri tararsa, saldırı yüzeyinin önemli bir bölümünü gözden kaçırabilir.

Bu durum, Analyzer'ın EASM'nin keşif yeteneklerini (örneğin, pasif DNS numaralandırması, sertifika şeffaflık günlükleri, açık kaynak istihbarat toplama) proaktif olarak bir kuruluşun *tüm* harici dijital ayak izini, hatta farkında olmadıkları varlıkları bile keşfetmek ve haritalamak için entegre etmesi gerektiğini göstermektedir. Bu, Analyzer'ı yalnızca bir "zafiyet tarayıcısı" olmaktan çıkarıp, daha kapsamlı bir "saldırı yüzeyi keşif" aracına dönüştürecektir. Bu genişleme, Analyzer'ın sunduğu güvenlik değerlendirmelerinin kapsamını ve doğruluğunu önemli ölçüde artıracaktır.

5. Cihaz Duruş Değerlendirmesi ile Sıfır Güven Ağ Erişimi (ZTNA)

Sıfır Güven, "asla güvenme, her zaman doğrula" ilkesine dayanan kapsamlı bir siber güvenlik stratejisidir.[7] ZTNA, tüm kullanıcıların, cihazların, uygulamaların ve hizmetlerin, uygulamalara ve verilere erişim izni verilmeden veya sürdürülmeden önce güvenlik duruşları açısından sürekli olarak kimlik doğrulaması ve doğrulanmasını gerektiren bir BT teknoloji çözümüdür.[14] Bu yaklaşım, geleneksel çevre tabanlı modelden, erişimin yalnızca IP adreslerine değil, gelişmiş kimlik doğrulama tekniklerine dayandığı sıkı erişim kontrolleri ve en az ayrıcalık ilkesine geçişi temsil eder.[15] Cihaz Duruş Değerlendirmesi, cihaz uyumluluğunu ve güvenlik duruşunu (örneğin, işletim

sistemi/sensör yapılandırmaları, USB bağlantıları, Wi-Fi ağları) gerçek zamanlı olarak kontrol ederek koşullu erişim kararları için bir güven puanı oluşturan kritik bir bileşendir.[16]

2025 yılı için Sıfır Güven benimsenmesi önemli bir eğilimdir ve kuruluşların %96'sı bu yaklaşımı desteklemektedir.[7] Saldırganların geçerli hesapları giderek daha fazla kullanması ve geleneksel çevre savunmalarını atlatması [24] nedeniyle, ZTNA ve cihaz duruş değerlendirmesi kritik hale gelmektedir. Analyzer için bu, IP/URL analizinin yalnızca ağ düzeyindeki zafiyetleri belirlemekle kalmayıp, aynı zamanda bu IP'lere bağlı *cihazların* ve bu URL'lere erişen *kullanıcıların* güvenlik duruşunu da değerlendirmesi gerektiği anlamına gelir. Analyzer, cihaz duruşu kontrollerini (örneğin, işletim sistemi sürümü, yama durumu, güvenlik yazılımının varlığı) entegre ederek, bağlı her varlık için daha ayrıntılı bir risk değerlendirmesi sağlayabilir ve basit ağ segmentasyonunun ötesinde koşullu erişim önerileri sunabilir. Bu, mobil ve IoT/OT cihazlarının güvenliğini sağlamak için hayati öneme sahiptir.[17]

Sıfır Güven prensibi, güvenlik odağını ağ *çevresini* korumaktan (geleneksel güvenlik duvarı/VPN, IP tabanlı erişim), kimlik ve cihaz duruşuna dayalı *her erişim isteğini* güvence altına almaya kaydırmaktadır. Bu, Analyzer'ın IP/URL analizinin gerçek etkinlik için kimlik ve cihaz bağlamıyla entegre olması gerektiği anlamına gelir. [15]'de belirtildiği gibi, ZTNA'nın erişim kontrolü "kullanıcının IP adresine değil, gelişmiş kimlik doğrulama tekniklerine" dayanmaktadır. [14] ise "tüm varlıkların sürekli doğrulanması ve onaylanması"nı vurgulamaktadır. Analyzer'ın mevcut odak noktası IP/URL analizi olup, bu ağ merkezlidir. Eğer erişim artık yalnızca IP tarafından yönetilmiyorsa, Analyzer'ın analizinin daha derinlemesine gitmesi gerekmektedir.

Bu durum, Analyzer'ın IP/URL etkileşimleri için kullanıcı ve cihaz bağlamını çekmek amacıyla kimlik sağlayıcılarla (örneğin, Okta, Azure AD) ve uç nokta yönetim çözümleriyle (örneğin, MDM, EDR) entegrasyonu hedeflemesi gerektiğini göstermektedir. Bu entegrasyon, Analyzer'ın yalnızca "bu IP'de açık bir port var" demek yerine, "bu IP, bu uyumsuz cihazdaki bu kullanıcı tarafından kullanılıyor ve açık bir portu var, bu da yüksek risk oluşturuyor" gibi daha ayrıntılı bilgiler sunmasını sağlayacaktır. Bu, Analyzer'ın risk değerlendirmesini ve savunma önerilerini önemli ölçüde yükseltecektir.

6. IP/URL İstihbaratı Yoluyla Geliştirilmiş Tedarik Zinciri Risk Yönetimi

Tedarik zinciri saldırıları hızlanmakta ve üçüncü taraf satıcılar, açık kaynaklı kütüphaneler ve ticari yazılım ikili dosyalarındaki zafiyetleri hedef alarak gelişmektedir.[7] Bu, sızdırılmış geliştirici sırlarını (API anahtarları, kimlik bilgileri) ve ticari yazılımlardaki güvensiz tasarımları içermektedir. Üçüncü taraf ihlalleri, veri ihlallerinin ve fidye yazılımı

saldırılarının birincil kaynağıdır.[21] Tedarik Zinciri Risk Yönetimi (SCRM), harici varlıklardan kaynaklanan bu riskleri tanımlama, değerlendirme, izleme ve azaltma sürecidir.

Geleneksel zafiyet yönetiminin (NVD sorunları gibi) "çökmesi" [19], tedarik zinciri risklerine daha geniş bir odaklanmayı zorunlu kılmaktadır. Analyzer, hedef sistem tarafından kullanılan üçüncü taraf hizmetler, bulut sağlayıcıları ve açık kaynak bileşenlerle ilişkili IP adreslerini ve URL'leri belirleyerek bu alana katkıda bulunabilir. Bu, satıcı ekosistemlerini haritalamayı, güvenlik duruşlarını (açıkta kalan IP'leri/URL'leri aracılığıyla) değerlendirmeyi ve dijital varlıklarındaki bilinen zafiyetleri veya ihlalleri izlemeyi içerir. Analyzer'ın Whois yetenekleri, barındırma sağlayıcılarını ve alan adı kayıtçılarını belirlemek için genişletilebilir ve tedarik zinciri haritalaması için kritik bağlam sağlayabilir. YZ, Üçüncü Taraf Risk Yönetimi'nde (TPRM) giderek daha fazla kullanılacaktır.[22]

Tedarik zinciri risk yönetimi, kuruluşları (ve Analyzer'ı) doğrudan kontrolleri dışında ancak operasyonel ekosistemleri içinde yer alan varlıklardan kaynaklanan zafiyetleri ve tehditleri dikkate almaya zorlamaktadır. Bu durum, yalnızca dahili taramadan, üçüncü taraflar hakkında harici istihbarat toplamaya doğru bir kaymayı gerektirmektedir. [21], "geçen yılki tüm veri ihlallerinin %35,5'inin üçüncü taraf ihlallerinden kaynaklandığını" belirtirken, [7] SolarWinds'ı bir tedarik zinciri saldırısı örneği olarak vurgulamaktadır. Analyzer'ın mevcut odak noktası, kullanıcının *kendi* sistemlerinin ve ağlarının güvenliğini artırmaktır. Ancak, saldırıların önemli bir kısmı *üçüncü taraflar* aracılığıyla gelmektedir.

Bu durum, Analyzer'ın üçüncü taraf IP'leri ve URL'leri hakkında pasif istihbarat toplama yeteneklerini entegre etmesi gerektiğini göstermektedir. Bu, Analyzer tarafından doğrudan taranmasa bile, üçüncü taraf yazılım bileşenlerinin bilinen zafiyetleri için genel veritabanlarını sorgulamayı, ele geçirilmiş satıcı kimlik bilgileri için karanlık web'i izlemeyi veya üçüncü taraf risk yönetimi platformlarıyla entegre olarak IP'ler/URL'lerle ilgili harici güvenlik duruşu verilerini almayı içerebilir. Bu, Analyzer'ın kapsamlı savunma önerileri sunma yeteneğini önemli ölçüde artıracaktır.

7. IoT/OT/IoMT Cihaz Güvenliği Analizi

Operasyonel ortamlar (OT) giderek daha fazla dijitalleşmekte ve IoT teknolojileriyle entegre olmakta, genellikle buluta bağlanarak saldırı yüzeyini önemli ölçüde genişletmektedir.[23] IoMT cihazları da giderek daha savunmasız hale gelmekte ve sağlık hizmetleri ağları için endişe yaratmaktadır.[18] Yönlendiriciler, NVR'ler, VoIP, IP kameralar, NAS, PoS sistemleri, ADC'ler, IPMI'ler, Güvenlik Duvarları ve Alan Adı Denetleyicileri özellikle yüksek riskli cihazlar olarak tanımlanmıştır.[18] Saldırılar, iş kesintilerine neden

olmaktan, kritik altyapıyı hedefleyerek fiziksel zarara yol açmaya doğru kaymaktadır.[23]

Modern kuruluşlarda saldırı yüzeyi BT, IoT, OT ve IoMT'yi kapsadığından, tek kategorili bir güvenlik odağı yetersiz kalmaktadır.[18] Analyzer, IP/URL analizi ve cihaz listeleme yetenekleriyle (ARP-scan, Nmap), bu konuyu ele almak için iyi bir konumdadır. Cihaz keşfini özellikle IoT/OT/IoMT cihazlarını (örneğin, MAC adresleri, açık portlar, banner'lar veya bu cihaz türlerine özgü bilinen zafiyetler temelinde) tanımlamak ve sınıflandırmak için geliştirebilir. Analyzer daha sonra bu kritik, genellikle güvensiz tasarımlı cihazlar için özel zafiyet tespit kuralları uygulayabilir ve özel savunma önerileri sunabilir. Gömülü işletim sistemlerinin yükselişi [18] ve güvensiz IoT cihazlarından kaynaklanan DDoS botnet saldırıları potansiyeli [23] aciliyeti vurgulamaktadır.

BT/OT/IoT/IoMT'nin birbirine bağlılığı, siber saldırıların artık doğrudan fiziksel zarara veya kritik altyapı kesintisine yol açabileceği anlamına gelmektedir.[23] Analyzer'ın bu cihazlardaki zafiyetleri belirlemedeki rolü, yalnızca veri güvenliği için değil, fiziksel güvenlik ve ulusal güvenlik için de hayati önem taşımaktadır. Analyzer'ın mevcut odak noktası, "siber güvenlik zafiyetlerini proaktif bir şekilde belirleyerek sistemlerin ve ağların güvenliğini artırmaktır." Bu, öncelikle dijital güvenliği ifade etmektedir. Ancak, eğer "sistemler" OT/IoT cihazlarını içeriyorsa, etki fiziksel dünyaya yayılmaktadır.

Bu durum, Analyzer'ın raporlarında OT/IoT/IoMT cihazlarıyla ilişkili riskleri açıkça vurgulaması ve farklılaştırması gerektiğini göstermektedir. Analyzer'ın "savunma önlemleri" fiziksel sistemlerin güvenliğini sağlamaya yönelik özel önerileri içermelidir; örneğin, OT için ağ segmentasyonu, endüstriyel protokoller için güvenli yapılandırmalar ve bu ortamlarda sıkça bulunan eski donanımlar için özel değerlendirmeler. Bu, Analyzer'ın değer teklifini kritik altyapı korumasına yükseltecektir.

8. URL/IP Bağlamı ile Gelişmiş Kimlik Avı ve Sosyal Mühendislik Tespiti

Kimlik avı ve sosyal mühendislik, saldırganların daha kişiselleştirilmiş ve ikna edici kampanyalar için YZ'den yararlanmasıyla [3] en büyük tehditler arasında yer almaya devam etmektedir. Bilgi hırsızı kötü amaçlı yazılımlar, 2024'te kimlik avı yoluyla %84 oranında artmıştır.[24] "Sneaky 2FA" gibi saldırılar, ortadaki adam (AiTM) tekniklerini kullanarak çok faktörlü kimlik doğrulamayı (MFA) atlamaktadır.[25] Bulut barındırma, kitlesel kimlik avı kampanyaları için giderek daha fazla kullanılmakta, güvenilir URL'ler/IP'ler sağlamaktadır.[24] Kötü amaçlı spam'de doğrudan kötü amaçlı yazılım eklerinin yerini PDF'ler ve URL'ler almaktadır.[24]

2024-2025 yıllarında teknolojik gelişmelere rağmen insan faktörü en zayıf halka olmaya devam etmektedir.[26] Analyzer, gerçek zamanlı itibar kontrolleri [36], YZ/ML tabanlı

kötü amaçlı URL modellerinin tespiti [34] ve alan adı özelliklerinin (örneğin, yazım hatası, yaşı, Whois'ten kayıt detayları) analizi dahil olmak üzere gelişmiş URL analizini entegre ederek kimlik avı tespit yeteneklerini önemli ölçüde artırabilir. Ayrıca, Analyzer şüpheli URL'leri/IP'leri bilinen kimlik avı kampanyaları ve saldırgan taktikleri hakkındaki tehdit istihbaratıyla ilişkilendirebilir.[24] Öneriler, kullanıcı eğitimini ve yüksek riskli hesaplar için FIDO uygulamasını içermelidir.[25]

Kimlik avı saldırıları giderek daha sofistike hale gelmekte, güvenilir altyapıları (bulut barındırma) ve YZ tarafından oluşturulan içerikleri [3] kullanmaktadır. Bu durum, Analyzer'ın URL analizinin yalnızca basit kara listelemeyi veya yapısal anormallikleri aşarak, barındırma IP'si meşru olsa bile URL'nin arkasındaki *bağlamı* ve *niyeti* değerlendirmesi gerektiği anlamına gelir. Eğer saldırganlar meşru bulut altyapısını ve YZ'yi ikna edici içerik oluşturmak için kullanırlarsa, geleneksel URL analizi (örneğin, bilinen kötü amaçlı IP'leri veya bariz yazım hatalarını kontrol etme) başarısız olabilir.

Bu durum, Analyzer'ın URL analizinin gerçek zamanlı içerik analizi (Trend 2'de tartışıldığı gibi LLM'ler kullanılarak), IP/alan adının son davranışını dikkate alan dinamik itibar kontrolleri [36] ve potansiyel olarak kimlik avı kitlerini ve AiTM hizmetlerini izleyen tehdit istihbaratı akışlarıyla entegrasyon gibi gelişmiş teknikleri içermesi gerektiğini göstermektedir. Bu, Analyzer'ı *kötü* URL'leri tanımlamaktan, *aldatıcı* URL'leri tanımlamaya doğru bir adım atacaktır.

9. Buluta Özgü Zafiyet Tarama ve Duruş Yönetimi

İşletmeler bulut altyapısını ve hibrit bulut çözümlerini giderek daha fazla benimsediğinden [29], bu ortamlardaki yanlış yapılandırmalar ve zafiyetler önemli riskler oluşturmaktadır. Buluta özgü zafiyet taraması, Bulut Altyapı Hizmetleri (IaaS), Platform Hizmetleri (PaaS) ve kapsayıcılı iş yükleri dahil olmak üzere bulut ortamlarındaki güvenlik zafiyetlerinin sürekli olarak tanımlanması, risk değerlendirmesi ve giderilmesini içerir. Bu, tam bulut görünürlüğü elde etmeye, sürekli taramaya, otomatik yama düzeltmesine ve kapsamlı raporlamaya odaklanır.[27]

Bulut güvenliği 2025 için önemli bir eğilimdir.[26] Analyzer, IP/URL analizini bulutta barındırılan varlıkları hedef alacak şekilde genişletebilir, yanlış yapılandırmaları (örneğin, açık S3 kovaları, açıkta kalan Kubernetes API'leri) ve bulut iş yüklerindeki ve kapsayıcılardaki zafiyetleri [37] belirleyebilir. Bu, belirli IP'ler veya URL'lerle ilişkili bulut kaynakları hakkında görünürlük elde etmek için bulut sağlayıcı API'leriyle [27] entegrasyon gerektirir. Analyzer daha sonra, otomatik düzeltme politikaları ve sızıntıları önlemek için veri akışlarının sürekli denetimi dahil olmak üzere, bulut güvenlik duruşu yönetimi için özel öneriler sunabilir.[27]

Bulut ortamlarında, yanlış yapılandırmalar (örneğin, aşırı izinli ayarlar, halka açık S3 kovaları) geleneksel yazılım zafiyetleri kadar, hatta onlardan daha yaygın ve kritik olabilir.[27] Analyzer'ın IP/URL analizinin bu yapılandırma hatalarını özel olarak belirlemesi gerekmektedir. Geleneksel zafiyet tarayıcıları (Nmap, Nikto, WPScan gibi) öncelikle yazılım hatalarını veya bilinen CVE'leri arar. Bunlar, bulut yanlış yapılandırmalarını tespit etmek için tasarlanmamıştır.

Bu durum, Analyzer'ın "özelliklerini" bulut güvenlik duruşu yönetimi (CSPM) yeteneklerini içerecek şekilde genişletmesi gerektiğini göstermektedir. Bu, taranan IP'ler/URL'lerle ilişkili bulut hizmetlerinin (örneğin, S3 kovaları, güvenlik grupları, IAM politikaları) yapılandırmasını değerlendirmek ve yanlış yapılandırmaları yüksek öncelikli zafiyetler olarak işaretlemek için bulut API'leriyle entegrasyon anlamına gelir. Bu genişleme, Analyzer'ın bulut güvenliği alanındaki kapsamını ve değerini önemli ölçüde artıracaktır.

10. İş Bağlamı ve Tahmine Dayalı Analiz ile Otomatik Risk Puanlaması

Otomatik risk puanlaması, statik, teknik değerlendirmelerden (CVSS gibi) gerçek zamanlı verileri, iş bağlamını, varlık kritikliğini ve istismar tahmin puanlarını (EPSS) içeren dinamik sistemlere doğru evrilmektedir.[11] YZ ve makine öğrenimi, büyük veri kümelerini analiz ederek, kalıpları belirleyerek ve gelecekteki riskleri tahmin ederek bu alanda devrim yaratmaktadır.[30] Bu, yalnızca uyumluluk kontrol listelerinin ötesine geçerek stratejik karar almayı yönlendiren daha kapsamlı ve eyleme geçirilebilir risk değerlendirmelerine olanak tanır.

Zafiyet hacmi arttıkça [8] ve bağlamları (örneğin, bulut, IoT/OT) daha karmaşık hale geldikçe, kuruluşların akıllı önceliklendirmeye ihtiyacı vardır. Analyzer'ın mevcut "risk puanlaması" özelliği, iş bağlamını (örneğin, varlığın önemi, veri sınıflandırması, mevzuat uyumluluk gereksinimleri) ve potansiyel sorunları tahmin etmek için tahmine dayalı analizi [30] entegre eden dinamik risk puanlaması dahil edilerek önemli ölçüde geliştirilebilir. Bu, Analyzer'ın yalnızca teknik ciddiyete değil, en yüksek *iş* riskini oluşturan zafiyetleri vurgulayarak gerçekten eyleme geçirilebilir savunma önerileri sunmasını sağlar. Triyaj ve düzeltmedeki otomasyon [11] süreci daha da kolaylaştırır.

Risk puanlamasının yalnızca teknik (CVSS) olmaktan iş bağlamlı hale gelmesi [11], ham zafiyet verilerini karar vericiler için eyleme geçirilebilir istihbarata dönüştürmektedir. Bu, Analyzer'ın "anlaşılır raporlar" sağlama ve "güvenlik önlemlerinin alınmasını teşvik etme" vaadini yerine getirmesi için kritik öneme sahiptir. [11], CVSS puanlarının "bağlamdan yoksun" olduğunu ve "paydaşlarla iletişim kurmanın zor olduğunu" belirtmekte ve önceliklendirme için "iş bağlamı"nı önermektedir. [30] ise "dinamik risk

puanlaması" ve "tahmine dayalı analiz"den bahsetmektedir.

Eğer risk puanları sadece teknik ise, teknik olmayan kullanıcılar *iş etkisini* ve dolayısıyla düzeltmenin aciliyetini anlamakta zorlanabilirler. Bu durum, Analyzer'ın risk puanlama algoritmasının, kullanıcının farklı varlıklar veya veri türleri için iş kritikliğini girmesine izin verecek şekilde yapılandırılması gerektiğini göstermektedir. Çıktı, hem teknik ciddiyeti hem de iş etkisini yansıtan bir risk puanı sunmalı ve potansiyel olarak belirli bir zafiyetin *kendi* kuruluşları için neden kritik olduğunu açıklayan net bir anlatım içermelidir. Bu, Analyzer'ı teknik bir araçtan siber güvenlik için stratejik bir iş kolaylaştırıcıya dönüştürecektir.

IV. Analyzer İçin Stratejik Entegrasyon ve Geliştirme

Analyzer'ın gelecekteki etkinliği, IP ve URL analizindeki temel yeteneklerini, ortaya çıkan siber güvenlik eğilimleriyle stratejik olarak entegre etme becerisine bağlıdır. Bu entegrasyon, Analyzer'ın sadece mevcut tehditleri tespit etmekle kalmayıp, aynı zamanda gelecekteki saldırı vektörlerini tahmin etmesini ve bunlara karşı savunma yapmasını sağlayacaktır.

YZ/ML'den Temel Yetenekler İçin Yararlanma:

- **Gelişmiş Keşif ve Cihaz Listeleme (Nmap, ARP-scan):** Geleneksel taramanın ötesinde cihazları tanımlamak için YZ destekli ağ anomali tespitini (Trend 1) ve Kullanıcı ve Varlık Davranış Analizi'ni (UEBA) [4] entegre etmek gerekmektedir. Bu, gizli cihazları, gölge BT'yi (Trend 4) ve anormal cihaz davranışlarını (örneğin, olağandışı iletişim kuran IoT cihazları [18]) içerir. Büyük Dil Modelleri (LLM'ler), barındırma ve alan adı hizmetleri için Whois verilerini bağlamsal tehdit istihbaratıyla zenginleştirebilir (Trend 2).
- **Daha Derin Zafiyet Analizi (Nikto, WPScan, SSLScan):** Bu araçları, web uygulaması zafiyetlerinin bağlamını anlamak, sofistike kimlik avı URL'lerini tespit etmek [34] ve buluta özgü uygulamalardaki ve kapsayıcılardaki yanlış yapılandırmaları belirlemek [27] için LLM odaklı analizle (Trend 2) geliştirmek önemlidir. Bu, imza tabanlı kontrollerin ötesine geçerek davranışsal ve bağlamsal analize doğru bir ilerlemeyi temsil eder.
- **Proaktif Saldırı Simülasyonu ve Savunma Önerileri:** Sürekli Tehdit Maruziyeti Yönetimi (CTEM) (Trend 3) ve Harici Saldırı Yüzeyi Yönetimi (EASM) (Trend 4) aracılığıyla belirlenen potansiyel saldırı yollarını simüle etmek için LLM'leri saldırı sentezi için kullanmak [6] büyük fayda sağlayacaktır. Bu, Analyzer'ın tedarik zinciri riskleri (Trend 6) ve OT/IoT cihazlarının güçlendirilmesi (Trend 7) dahil olmak üzere daha kesin ve eyleme geçirilebilir savunma önerileri sunmasını sağlar.

Bağlamsal İstihbarat ve Risk Önceliklendirme:

- **Risk Puanlaması Evrimi:** Analyzer'ın risk puanlamasını yalnızca teknik (CVSS) olmaktan çıkarıp, dinamik, iş bağlamlı bir modele [11] dönüştürmek kritik öneme sahiptir. Kullanıcıların varlık kritikliğini ve iş etkisini tanımlamasına izin vermek, Analyzer'ın en yüksek *kurumsal* riski oluşturan zafiyetleri önceliklendirmesini sağlayacaktır.
- **Tehdit İstihbaratıyla Entegrasyon:** Küresel ve sektöre özgü tehdit istihbaratını [24] Analyzer'ın analiz motoruna sürekli olarak beslemek, özellikle IP ve URL itibarı [36], kötü amaçlı yazılım kampanyaları ve tehdit aktör faaliyetleri için proaktif bilgiler sağlayacaktır. Bu, ortaya çıkan saldırı vektörleri hakkında önleyici bilgiler sunar.

Sürekli Güvenliği Benimseme:

- **Sürekli İzlemeye Geçiş:** Analyzer'ı periyodik taramalardan IP adresleri, URL'ler ve ilişkili varlıkların sürekli izlenmesine geçirmek için CTEM (Trend 3) ve EASM (Trend 4) prensiplerini uygulamak gereklidir. Bu, gelişen saldırı yüzeyine gerçek zamanlı görünürlük ve yeni maruziyetlerin anında tespit edilmesini sağlar.
- **Cihaz Duruşu ve Kimlik Entegrasyonu:** Ağ etkinliğini kullanıcı ve cihaz güvenilirliği ile ilişkilendiren bütünsel bir risk görünümü sağlamak için cihaz duruş değerlendirmesini [16] dahil etmek ve kimlik yönetimi çözümleriyle entegre olmak önemlidir. Bu, Sıfır Güven prensiplerini (Trend 5) destekler.

Kullanıcı Deneyimi ve Eyleme Geçirilebilirlik:

- **Basitleştirilmiş Raporlama:** Karmaşık teknik bulguları açık, iş odaklı bilgilere dönüştürerek "anlaşılır raporlar" (Kullanıcı Sorgusu) sunmaya devam etmek, potansiyel olarak YZ tarafından oluşturulan özetler ve görselleştirmeler kullanılarak sağlanabilir.
- **Otomatik Düzeltme Rehberliği:** Analyzer'ın savunma önerilerini, düzeltme için otomatik mantıkla [11] geliştirerek, belirli adımlar önermek veya mümkün olduğunda yama yönetimi sistemleriyle entegrasyon sağlamak faydalı olacaktır.

Tablo 2: Analyzer'ın 2025 Trendleri Aracılığıyla Özellik Geliştirme Yol Haritası

- **Konum:** Bölüm IV içinde.
- **Değer:** Bu tablo, teorik eğilimleri pratik ürün geliştirmeyle doğrudan ilişkilendirerek, Analyzer'ın mevcut özelliklerinin nasıl evrilebileceğini ve yeni yeteneklerin nasıl entegre edilebileceğini gösterir. Bu, Analyzer geliştirme ekibi için açık, eyleme geçirilebilir bir yol haritası sunar.
- **Chain of Thought Reasoning:**
    1. **Kullanıcı İhtiyacı:** Kullanıcı, bir Ürün Yöneticisi veya Baş Geliştirici olarak,

belirlenen eğilimleri kendi ürünlerine nasıl uygulayacaklarına dair somut fikirlere ihtiyaç duymaktadır.

2. **Eyleme Geçirilebilirlik:** Bu tablo, soyut eğilimleri belirli özellik geliştirmelerine dönüştürerek raporu son derece eyleme geçirilebilir kılar.
3. **Stratejik Uyum:** Her bir geliştirmenin Analyzer'ın mevcut güçlü yönleri ve gelecekteki stratejik hedefleriyle (kullanıcı sorgusunda belirtildiği gibi) nasıl uyumlu olduğunu gösterir.
4. **Netlik ve Organizasyon:** Bir tablo, mevcut özellikleri, ilgili eğilimleri, önerilen geliştirmeleri ve beklenen etkileri açıkça ayırarak planlama ve tartışmayı kolaylaştırır.

Mevcut Analyzer Özelliği/Yetenek	**İlgili 2025 Eğilimi**	**Önerilen Geliştirme/Entegrasyon**	**Analyzer'ın Etkinliğine Beklenen Etki**
Ağdaki Cihaz Listesi (ARP-scan, Nmap)	1. YZ Destekli Davranışsal Anomali Tespiti, 7. IoT/OT/IoMT Cihaz Güvenliği Analizi	YZ/ML tabanlı davranışsal anomali tespiti ve IoT/OT/IoMT cihaz sınıflandırması ekleme.	Bilinmeyen cihazların, anormal davranışların ve kritik altyapı zafiyetlerinin tespiti.
IP/URL Analizi (Nmap, Nikto, Gobuster, WPScan, SSLScan)	2. LLM Destekli Tehdit İstihbaratı ve Analizi, 8. Gelişmiş Kimlik Avı ve Sosyal Mühendislik Tespiti	LLM'leri kullanarak URL'lerin anlamsal analizi, kimlik avı niyeti tespiti ve gelişmiş tehdit istihbaratı korelasyonu.	Daha sofistike kimlik avı ve sosyal mühendislik saldırılarının tespiti, bağlamsal tehdit bilgisi.
Hosting ve Alan Adı Bilgileri (Whois)	6. Geliştirilmiş Tedarik Zinciri Risk Yönetimi	Whois verilerini üçüncü taraf risk değerlendirmeleri ve tedarik zinciri haritalaması ile entegre etme.	Üçüncü taraf risklerinin belirlenmesi ve tedarik zinciri zafiyetlerine karşı görünürlük.
Siber Saldırı ve Savunma Önerileri	3. CTEM, 4. EASM, 5. ZTNA, 7. IoT/OT/IoMT Cihaz Güvenliği Analizi	Sürekli izleme, dış saldırı yüzeyinin otomatik keşfi, Sıfır Güven prensiplerinin entegrasyonu ve cihaza özel güvenlik önerileri.	Proaktif güvenlik duruşu, bilinmeyen saldırı vektörlerinin azaltılması ve fiziksel sistemler için hedeflenmiş savunmalar.

Sunucuya İlişkin Açıkların Tespiti	9. Buluta Özgü Zafiyet Tarama ve Duruş Yönetimi	Bulut ortamlarındaki (IaaS, PaaS, kapsayıcılar) yanlış yapılandırmaların ve zafiyetlerin tespiti için bulut API entegrasyonu.	Bulut tabanlı varlıklar için kapsamlı zafiyet tespiti ve bulut güvenlik duruşunun iyileştirilmesi.
Risk Puanlaması	10. İş Bağlamı ve Tahmine Dayalı Analiz ile Otomatik Risk Puanlaması	Teknik zafiyet puanlarını iş kritikliği ve tahmine dayalı analizle birleştiren dinamik risk puanlama sistemi.	İş öncelikleriyle uyumlu, eyleme geçirilebilir risk değerlendirmeleri ve daha akıllı önceliklendirme.
Profesyonel PDF Raporlama	Genel olarak tüm eğilimler	Teknik bulguları iş bağlamında açıklayan, YZ destekli özetler ve görselleştirmeler içeren geliştirilmiş raporlar.	Teknik ve teknik olmayan kullanıcılar için daha anlaşılır, eyleme geçirilebilir ve etkili güvenlik raporları.

V. Sonuç

2025 yılındaki siber güvenlik ortamı, Yapay Zeka'nın yaygın etkisi, hibrit BT/OT/IoT ortamlarında saldırı yüzeyinin genişlemesi ve proaktif, sürekli güvenlik metodolojilerine (CTEM ve EASM gibi) doğru temel bir kayma ile tanımlanacaktır. Kimlik merkezli güvenlik (Sıfır Güven) ve kapsamlı tedarik zinciri risk yönetimi, bu yeni paradigmada hayati öneme sahip olacaktır.

Analyzer, IP ve URL analizindeki güçlü temeliyle, bu eğilimleri benimsemek için olağanüstü bir konumdadır. Davranışsal anomali tespiti ve LLM destekli tehdit istihbaratı için YZ/ML'yi stratejik olarak entegre ederek, sürekli izleme ve bağlamsal risk puanlamasını benimseyerek ve kapsamını cihaz duruşu ve tedarik zinciri bilgilerini içerecek şekilde genişleterek, Analyzer proaktif siber savunma için öncü bir çözüme dönüşebilir.

Giderek karmaşıklaşan siber tehditler karşısında dayanıklılığın anahtarı, sürekli adaptasyon, akıllı otomasyon ve saldırı yüzeyinin bütünsel bir şekilde anlaşılmasında yatmaktadır. Bu gelişmiş tekniklere yatırım yaparak, Analyzer kuruluşları yalnızca daha etkili bir şekilde korumakla kalmayacak, aynı zamanda daha güvenli ve dirençli bir

dijital gelecek inşa etmeleri için onları güçlendirecektir.

Alıntılanan çalışmalar

1. Network Anomaly Detection: A Complete Guide - SearchInform, erişim tarihi Haziran 6, 2025, https://searchinform.com/cybersecurity/measures/security-monitoring/network-anomaly-detection/
2. Comparative Analysis of AI-Driven Security Approaches in DevSecOps: Challenges, Solutions, and Future Directions - arXiv, erişim tarihi Haziran 6, 2025, https://arxiv.org/html/2504.19154v1
3. 2025 Global Threat Report | Latest Cybersecurity Trends & Insights ..., erişim tarihi Haziran 6, 2025, https://www.crowdstrike.com/en-us/global-threat-report/
4. Top 15 UEBA Use Cases for Today's SOCs in 2025 - Research AIMultiple, erişim tarihi Haziran 6, 2025, https://research.aimultiple.com/ueba-use-cases/
5. Generative AI in Cybersecurity: A Comprehensive Review of LLM Applications and Vulnerabilities - arXiv, erişim tarihi Haziran 6, 2025, https://arxiv.org/html/2405.12750v2
6. TrafficLLM: Enhancing Large Language Models for Network Traffic Analysis with Generic Traffic Representation - arXiv, erişim tarihi Haziran 6, 2025, https://arxiv.org/html/2504.04222v1
7. 5 Cybersecurity Trends to Watch in 2025, erişim tarihi Haziran 6, 2025, https://sps.wfu.edu/articles/top-cybersecurity-trends/
8. Analysis of AI Tools Shows 85 Percent Have Been Breached - Security Today, erişim tarihi Haziran 6, 2025, https://securitytoday.com/articles/2025/06/02/analysis-of-ai-tools-shows-85-percent-have-been-breached.aspx
9. Understanding Continuous Threat Exposure Management (CTEM) - Balbix, erişim tarihi Haziran 6, 2025, https://www.balbix.com/insights/what-is-continuous-threat-exposure-management-ctem/
10. What Is Continuous Threat Exposure Management (CTEM)? - CrowdStrike.com, erişim tarihi Haziran 6, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/exposure-management/continuous-threat-exposure-management-ctem/
11. Seven Steps to Building a Mature Vulnerability Management ..., erişim tarihi Haziran 6, 2025, https://www.infosecurity-magazine.com/news/infosec2025-seven-steps/
12. What Is External Attack Surface Management? | Zpedia - Zscaler, erişim tarihi Haziran 6, 2025, https://www.zscaler.com/zpedia/what-is-external-attack-surface-management
13. What Is Attack Surface Management in 2025? Mapping, Reducing, and Controlling Risk, erişim tarihi Haziran 6, 2025, https://www.wiz.io/academy/attack-surface-management
14. 10 Zero Trust Solutions for 2025 - SentinelOne, erişim tarihi Haziran 6, 2025,

https://www.sentinelone.com/cybersecurity-101/identity-security/zero-trust-solutions/
15. What is ZTNA? Zero Trust Network Access - CrowdStrike.com, erişim tarihi Haziran 6, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/zero-trust-security/zero-trust-network-access-ztna/
16. Device Posture | Citrix Product Documentation, erişim tarihi Haziran 6, 2025, https://docs.citrix.com/en-us/device-posture/device-posture.pdf
17. CrowdStrike Falcon for Mobile Gains Android Enterprise and Zero Trust Integrations, erişim tarihi Haziran 6, 2025, https://www.crowdstrike.com/en-us/blog/crowdstrike-strengthens-mobile-security-with-new-integrations/
18. Forescout's 2025 report reveals surge in device vulnerabilities ..., erişim tarihi Haziran 6, 2025, https://industrialcyber.co/reports/forescouts-2025-report-reveals-surge-in-device-vulnerabilities-across-it-iot-ot-and-iomt/
19. The 2025 Software Supply Chain Security Report, erişim tarihi Haziran 6, 2025, https://ntsc.org/wp-content/uploads/2025/03/The-2025-Software-Supply-Chain-Security-Report-RL-compressed.pdf
20. The 2025 Software Supply Chain Security Report: Threats Growing and Evolving - ISACA, erişim tarihi Haziran 6, 2025, https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2025/the-2025-software-supply-chain-security-report
21. Conducting a Third-Party Security Risk Assessment, 2025 Complete Guide | Isora GRC, erişim tarihi Haziran 6, 2025, https://www.saltycloud.com/blog/conducting-a-third-party-security-risk-assessment-complete-guide/
22. What is Third-Party Risk Management (TPRM)? - Panorays, erişim tarihi Haziran 6, 2025, https://panorays.com/blog/third-party-risk-management/
23. Trends and expectations for OT security in 2025 | Nomios Group, erişim tarihi Haziran 6, 2025, https://www.nomios.com/news-blog/trends-ot-security-2025/
24. IBM X-Force 2025 Threat Intelligence Index | IBM, erişim tarihi Haziran 6, 2025, https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/2025-threat-intelligence-index
25. What's Trending: Top Cyber Attacker Techniques, December 2024–February 2025, erişim tarihi Haziran 6, 2025, https://reliaquest.com/blog/whats-trending-top-cyber-attacker-techniques-december-2024-february-2025/
26. Siber Güvenlikte 2025 Trendleri: Yeni Tehditler ve Çözümler - Vitriol Bilişim, erişim tarihi Haziran 6, 2025, https://vitriol.ltd/siber-guvenlikte-2025-trendleri-yeni-tehditler-ve-cozumler/
27. Cloud Vulnerability Management [Best Practices 2025] - Sentra, erişim tarihi Haziran 6, 2025, https://www.sentra.io/learn/cloud-vulnerability-management
28. A Guide to Vulnerability Management - Orca Security, erişim tarihi Haziran 6, 2025, https://orca.security/resources/blog/what-is-vulnerability-management/

29. 2025'TE ŞİRKETLERİ BEKLEYEN SİBER GÜVENLİK TEHDİTLERİ VE ÇÖZÜM ÖNERİLERİ, erişim tarihi Haziran 6, 2025, https://bilginc.com/tr/blog/2025-te-sirketleri-bekleyen-siber-guvenlik-tehditleri-ve-cozum-onerileri-6068/
30. Best 9 Compliance Risk Assessment Tools for 2025 - Centraleyes, erişim tarihi Haziran 6, 2025, https://www.centraleyes.com/best-7-compliance-risk-assessment-tools/
31. Top Cybersecurity Trends to Tackle Emerging Threats - Gartner, erişim tarihi Haziran 6, 2025, https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends
32. IP Trends in 2025: What to Expect and How to Prepare - IamIP, erişim tarihi Haziran 6, 2025, https://iamip.com/ip-trends-in-2025-what-to-expect-and-how-to-prepare/
33. Securonix Threat Labs Monthly Intelligence Insights – March 2025 ..., erişim tarihi Haziran 6, 2025, https://www.securonix.com/blog/securonix-threat-labs-monthly-intelligence-insights-march-2025/
34. Employing Machine Learning Algorithms to Detect Phishing URL Websites - DOI, erişim tarihi Haziran 6, 2025, https://doi.org/10.1109/ICICNIS64247.2024.10823220
35. URLGuard: A Holistic Hybrid Machine Learning Approach for Phishing Detection, erişim tarihi Haziran 6, 2025, https://www.mecs-press.org/ijieeb/ijieeb-v17-n2/v17n2-5.html
36. 7 Best IP Reputation Checkers for Email in 2025, erişim tarihi Haziran 6, 2025, https://www.emailvendorselection.com/ip-reputation-checkers/
37. Top 10 Container Runtime Security Tools for 2025 - SentinelOne, erişim tarihi Haziran 6, 2025, https://www.sentinelone.com/cybersecurity-101/cloud-security/container-runtime-security-tools/
38. Top Container Scanning Tools in 2025 - Aikido, erişim tarihi Haziran 6, 2025, https://www.aikido.dev/blog/top-container-scanning-tools
39. What is User and Entity Behavior Analytics (UEBA)? - SentinelOne, erişim tarihi Haziran 6, 2025, https://www.sentinelone.com/cybersecurity-101/cybersecurity/what-is-ueba/