Siber Sınırı Gezinmek: URL ve IP Tabanlı Sistemler İçin 2025 Yılında Saldırı ve Savunma Analizi Alanındaki En Son 10 Trend

I. Giriş: 2025'te Siber Analizin Gelişen Manzarası

2025 yılına girerken, siber güvenlik ortamı, "hız farkı" olarak adlandırılan bir durumla karakterize edilmektedir; burada, genellikle saldırgan tarafın yapay zeka (YZ) kullanımıyla yönlendirilen gerçek zamanlı tehdit evrimi, statik güvenlik test döngülerini geride bırakarak artan bir risk yaratmaktadır.[1] Siber suç maliyetlerinin 2025 yılına kadar yıllık 10,5 trilyon dolara ulaşması beklenmekte olup, veri ihlallerinin %80'inden fazlası giderilmemiş güvenlik açıklarından kaynaklanmaktadır.[2] Tehditlerin bu giderek artan karmaşıklığı, kuruluşların siber saldırılara karşı daha dirençli olmalarını sağlamak için gelişmiş araçlar ve proaktif stratejiler benimsemelerini zorunlu kılmaktadır.

Bu bağlamda, URL ve IP adresleri aracılığıyla siber güvenlik zafiyetlerini proaktif olarak belirleyerek sistem ve ağ güvenliğini artırmaya yönelik program geliştirme kritik bir rol oynamaktadır. Bu tür bir programın temel amacı, sızma testi uzmanlarına ve sistem yöneticilerine, belirlenen hedefler üzerindeki potansiyel güvenlik açıklarını hızlı ve etkili bir şekilde analiz etme yeteneği sunmaktır. Popüler güvenlik araçlarını tek bir çatı altında toplayarak tarama sürecini otomatize etmek ve basitleştirmek, yalnızca zafiyet tespitiyle kalmayıp, aynı zamanda bulunan zafiyetlere yönelik potansiyel saldırı yöntemleri ve somut savunma önlemleri hakkında pratik öneriler sunmak, bu alandaki temel hedefler arasındadır. Risk puanlaması ile genel güvenlik durumunun değerlendirilmesi ve anlaşılır raporlama, güvenlik denetimlerinin belgelendirilmesini ve paylaşılmasını kolaylaştırarak, kurumların siber saldırılara karşı daha dirençli olmalarına yardımcı olmayı amaçlamaktadır.

Bu rapor, URL ve IP adresleri aracılığıyla saldırı ve savunma analizi alanındaki en etkili 10 tekniği ve trendi derinlemesine incelemeyi amaçlamaktadır. Her bir trendin mekanizmalarını, önemini, potansiyel etkilerini ve uygulama alanlarını detaylandırarak, gelişmiş siber güvenlik programlarının geliştirilmesi için stratejik yönlendirme sağlamayı hedeflemektedir.

II. Siber Savunma ve Saldırıda Yapay Zeka Devrimi

1. YZ/Makine Öğrenimi Destekli Tehdit Tespiti ve Otomatik Yanıt

Yapay Zeka (YZ) ve Makine Öğrenimi (ML) modelleri, siber güvenlikte gelişmiş tehdit tespitinin ön saflarında yer almaktadır. Bu teknolojiler, bilinen ve potansiyel olarak bilinmeyen siber tehditleri gösteren anormal aktiviteleri ve davranışsal modelleri gerçek zamanlı olarak analiz etmek için muazzam veri kümelerini işlemektedir. Bu

yetenek, olaylara daha hızlı ve otomatik yanıtlar verilmesini sağlamaktadır.[3]

YZ, normal operasyonların bir taban çizgisini oluşturarak çalışır ve sapmaları gelişmiş izleme veya proaktif güvenlik önlemleri için işaretler. Sistem davranışını ve kod anormalliklerini analiz ederek sıfır gün zafiyetlerini tespit edebilir, geleneksel imza tabanlı tespit yöntemlerinden kaçınmak için kodunu değiştiren polimorfik kötü amaçlı yazılımları tanımlayabilir ve kötüye kullanılan kimlik bilgilerinden veya içeriden gelen tehditlerden kaynaklanan güvenlik risklerini belirleyebilir. Otomatik eylemler arasında kötü amaçlı trafiği engelleme, şüpheli kötü amaçlı yazılımları karantinaya alma ve olay yanıt süreçlerini hızlandırma yer almaktadır.[3]

Saldırganlar, daha kaçamak kötü amaçlı yazılımlar oluşturmak, ikna edici deepfake içerikler üretmek ve sofistike kimlik avı kampanyalarını otomatikleştirmek için YZ'den giderek daha fazla yararlandıkça, savunmacıların bu hıza ayak uydurmak için akıllı araçlarla yanıt vermesi zorunludur. YZ, 2025 yılında "stratejik bir güç çarpanı" haline gelerek, kuruluşların sofistike tehditlerin önünde kalmasını ve hala en önemli saldırı vektörü olan insan hatasını azaltmasını sağlamaktadır. Ayrıca, tekrarlayan görevleri otomatikleştirerek siber güvenlik tükenmişliğiyle mücadeleye yardımcı olmaktadır.[1]

2025'teki potansiyel etkileri ve uygulama alanları arasında, YZ'nin tarama araçlarına ve API ağ geçitlerine entegre edilerek gerçek zamanlı tehdit analizi ve tespit edilen kötü amaçlı IP adreslerini engelleme veya şüpheli trafiği kısıtlama gibi otomatik yanıtlar sağlaması yer almaktadır.[10] YZ destekli öngörücü güvenlik, kuruluşların potansiyel tehditleri tahmin etmelerini ve saldırganlar bunları istismar etmeden önce zafiyetleri ve saldırı vektörlerini belirlemelerini sağlayarak siber savunmayı reaktiften anticipatif bir hale dönüştürmektedir.[4] YZ destekli Güvenlik Operasyon Merkezleri (SOC'lar), olay yanıt süreçlerini otomatikleştirecek ve kötü amaçlı yazılım analizi için makine öğrenimini kullanarak yanlış pozitifleri azaltacak ve güvenlik ekiplerinin yüksek öncelikli tehditlere odaklanmasını sağlayacaktır.[4] YZ destekli tehdit istihbarat platformları, açık ve karanlık ağ dahil olmak üzere çeşitli kaynaklardan gelen büyük veri kümelerini toplayıp analiz ederek güvenlik ekipleri için gerçek zamanlı, tarafsız ve eyleme geçirilebilir bilgiler sunmaktadır.[4] Generatif YZ'nin siber güvenlik pazarında ağ güvenliği segmentinin en hızlı büyüyen alan olması beklenmektedir, bu da ağ savunması için YZ destekli çözümlere güçlü bir odaklanma olduğunu göstermektedir.[13]

YZ'nin siber güvenlikteki çift yönlü doğası, yani saldırganların YZ'yi daha kaçamak kötü amaçlı yazılımlar, deepfake'ler ve sofistike kimlik avı kampanyaları oluşturmak için kullanması, savunmacıların da YZ destekli araçlarla yanıt vermesini zorunlu kılmaktadır. Bu durum, tehditlerin YZ tarafından yönlendirilen hızlı evriminin statik güvenlik önlemlerini geride bıraktığı bir "hız farkı" yaratmaktadır.[1] Bu durum, güvenlikte dinamik

ve giderek tırmanan bir çatışmaya işaret etmektedir. Bu, programın sadece YZ'yi entegre etmekle kalmayıp, aynı zamanda sürekli öğrenme, hızlı adaptasyon ve yeni tespit ve yanıt modellerinin çevik bir şekilde dağıtılması için tasarlanması gerektiği anlamına gelmektedir. Programın YZ yetenekleri, saldırgan YZ'si kadar hızlı evrimleşebilmelidir. Ayrıca, insan liderliğindeki yanıtların YZ destekli saldırılara karşı çok yavaş kalacağı gerçeği, program içinde otomatik yanıt mekanizmalarının kritik önemini pekiştirmektedir.

YZ'nin siber güvenlikte reaktiften proaktif bir yaklaşıma geçişteki rolü de dikkat çekicidir. Proaktif bir güvenlik zihniyetinin benimsenmesi vurgulanmaktadır.[3] YZ ve makine öğrenimi kullanılarak "öngörücü güvenlik" kavramı, zafiyetleri ve saldırı vektörlerini saldırganlar bunları istismar etmeden önce belirlemeyi amaçlamaktadır.[4] YZ'nin güvenlik araçlarının "tehditleri önceden tespit etmesini" sağlaması [5], siber güvenlik stratejisinde temel bir değişime işaret etmektedir. Bu, YZ'nin sadece mevcut saldırıların daha hızlı tespit edilmesiyle ilgili olmadığı, aynı zamanda gelecekteki olayları tahmin etme ve önleme yeteneğiyle ilgili olduğu anlamına gelmektedir. Kullanıcının programı, yalnızca *mevcut* zafiyetleri belirlemeye odaklanmakla kalmamalı, aynı zamanda gözlemlenen kalıplara, geçmiş verilere ve gerçek zamanlı tehdit istihbaratına dayanarak *potansiyel* gelecekteki saldırı vektörlerini tahmin etmeye de odaklanmalıdır. Bu, belirli bir zafiyet yaygın olarak istismar edilmeden önce bile önleyici eylemler veya güçlendirme önlemleri önerebilir ve geleneksel imza tabanlı tespitin ötesine geçerek gerçekten anticipatif bir savunma sağlayabilir.

2. Ajan YZ ve Otonom Güvenlik Ajanları

"Ajan YZ", geleneksel YZ yardımcı pilotlarından önemli bir evrimi temsil eden, bağımsız kararlar alabilen ve çok adımlı görevleri sürekli insan gözetimi olmadan yürütebilen yeni nesil otonom YZ ajanlarını ifade etmektedir.[8] Bu akıllı ajanlar, sistemleri otonom olarak izleyebilir, anormallikleri tespit edebilir ve tehditlere gerçek zamanlı olarak yanıt verebilir. Tehditler ve riskler ortaya çıktıkça gerçek zamanlı bağlam oluşturmak üzere tasarlanmıştır, bu da kullanıcıların beklenmedik olayları hızla anlamalarını ve yanıt vermelerini sağlamaktadır.[8]

Ajan YZ, öngörücü güvenliği ve gerçek zamanlı tehdit yanıtını geliştirerek siber savunmayı reaktif bir duruştan anticipatif bir duruşa dönüştürmektedir. Siber Güvenlik Yöneticileri (CISO'lar), kuruluşun genel güvenlik duruşunu ve operasyonel verimliliğini önemli ölçüde artırma potansiyelleri nedeniyle bu yaklaşımları test etmeye ve dağıtmaya giderek daha istekli hale gelmektedir.[8]

2025'teki potansiyel etkileri ve uygulama alanları arasında, otonom ajanların belirli olay türleri için insan müdahalesi olmadan tehditleri içermek veya azaltmak için anında,

önceden programlanmış eylemler gerçekleştirebilmesi yer almaktadır.[8] Ajan YZ, tehdit istihbaratı için otonom olarak veri toplayabilir, işleyebilir ve gerçek zamanlı bağlam oluşturabilir, bu da gelişen tehditlere ilişkin daha derin bilgiler sağlamaktadır.[8] Ajan YZ'nin ortaya çıkışı, YZ modellerini ve karar alma süreçlerini korumak için özel güvenlik çözümleri gerektiren "YZ için Güvenlik" adlı yeni ve geniş bir kategori oluşturmaktadır.[8] URL/IP analizi üzerindeki etkisi açısından, ajan YZ, tanımlanmış URL'ler ve IP aralıkları üzerinde otonom olarak tarama, analiz yapma ve hatta önceden tanımlanmış politikalara dayanarak savunma eylemleri başlatma yeteneğine sahip olabilir, bu da manuel iş yükünü önemli ölçüde azaltır ve yanıt sürelerini hızlandırır.

Ajan YZ'nin otonom karar alma yeteneği, siber güvenlikte önemli bir gelişmeyi temsil etmektedir.[8] Bu, YZ'nin sadece insan operatörlere yardımcı olmaktan, bağımsız eylemler gerçekleştirmeye doğru ilerlediğini göstermektedir. Bu durum, tehdit yanıtında benzeri görülmemiş bir hız ve ölçeklenebilirlik vaat ederken [4], aynı zamanda yeni ve karmaşık güvenlik risklerini de beraberinde getirmektedir. Ajanın yanlış bir karar vermesi veya ele geçirilmesi durumunda ne olacağı gibi sorular ortaya çıkmaktadır. Ajan YZ'nin ortaya çıkışıyla "YZ için Güvenlik"in yeni bir kategori haline geldiği belirtilmektedir.[8] Bu durum, YZ sistemlerinin kendilerini, karar alma mantıklarını ve veri bütünlüklerini güvence altına almanın kritik önemini vurgulamaktadır. Kullanıcının programı, otomatik yanıtlar için ajan YZ'yi (örneğin, kötü amaçlı IP'leri engelleme, URL'lerde şüpheli trafiği kısıtlama) içeriyorsa, sağlam "YZ için Güvenlik" ilkelerini yerleştirmelidir. Bu, YZ modellerinin düşmanca saldırılara karşı dirençli olmasını, karar alma süreçlerinin denetlenebilir olmasını ve kritik eylemler için hata korumaları veya insan gözetimi mekanizmalarının bulunmasını gerektirmektedir. Programın analizi, hedef URL'ler/IP'lerin ötesine geçerek dağıttığı YZ ajanlarının güvenlik duruşunu ve güvenilirliğini de içermelidir.

Ajan YZ'nin sistemleri otonom olarak izleme ve anormallikleri tespit etme yeteneği [8], Saldırı Yüzeyi Yönetimi (ASM)'nin sürekli izleme ve otomatik keşif yönleriyle doğrudan uyumludur.[15] Ajanlar, varlıkları (URL'ler ve IP'ler dahil) sürekli olarak keşfeder, haritalar ve değerlendirirse, ASM girişimlerinin hızını ve kapsamlılığını önemli ölçüde artırabilir. Bu durum, kullanıcının programının URL ve IP aralıklarında sürekli, otonom keşif ve zafiyet tespiti yapmak için ajan YZ'den stratejik olarak yararlanabileceği anlamına gelmektedir. Bu yetenek, kuruluşun saldırı yüzeyi haritasına gerçek zamanlı güncellemeler sağlayarak, yeni potansiyel giriş noktalarını veya mevcut olanlardaki değişiklikleri geleneksel yöntemlerden çok daha hızlı bir şekilde belirleyecektir. Bu, programı anlık bir tarayıcıdan dinamik bir saldırı yüzeyi istihbarat platformuna yükseltecektir.

III. Gelişen Zafiyet Yönetimi ve Sızma Testi Paradigmları

3. YZ Destekli Önceliklendirme ile Sürekli Zafiyet Yönetimi (CVM)

Sürekli Zafiyet Yönetimi (CVM), periyodik zafiyet taramasından kuruluşun sistemleri, ağları ve uygulamalarının sürekli, gerçek zamanlı izlemesine temel bir geçişi temsil etmektedir. Bu, tespit edilen zafiyetleri yalnızca genel ciddiyet puanlarına göre değil, aynı zamanda gerçek dünya istismar edilebilirliği, iş operasyonları için kritikliği ve potansiyel iş etkisi temelinde önceliklendirmek için YZ ve makine öğrenimini kritik bir şekilde kullanmaktadır.[2]

CVM araçları, yeni zafiyetleri sürekli olarak tarayarak güvenlik sorunlarının ortaya çıktıkça tespit edilmesini ve anında ele alınmasını sağlamaktadır. Bu araçlar, Güvenlik Bilgileri ve Olay Yönetimi (SIEM) platformları ve biletleme sistemleri gibi mevcut BT ekosistemleriyle sorunsuz bir şekilde entegre olacak şekilde tasarlanmıştır. YZ algoritmaları, en yüksek gerçek riski oluşturan zafiyetleri belirlemek için büyük miktarda tehdit istihbaratı ve bağlamsal veriyi analiz ederek eyleme geçirilebilir ve kolaylaştırılmış düzeltme adımları sağlamaktadır.[2]

Siber tehditlerin giderek sofistike ve sık hale gelmesi ve veri ihlallerinin %80'inden fazlasının giderilmemiş zafiyetlerden kaynaklanması nedeniyle CVM vazgeçilmezdir. Kuruluşların gelişen tehdit ortamının önünde kalmasına, güvenlik ekiplerini bunaltabilecek yanlış pozitifleri önemli ölçüde azaltmasına ve en çok istismar edilebilir ve etkili risklere odaklanarak giderek daha katı düzenleyici uyumluluk gereksinimlerini karşılamasına yardımcı olmaktadır.[2]

2025'teki potansiyel etkileri ve uygulama alanları arasında, YZ'nin gerçek dünya etkisi ve istismar edilebilirliğine dayalı olarak zafiyetlerin daha doğru ve otomatik önceliklendirilmesini sağlaması, böylece uyarı yorgunluğunu önemli ölçüde azaltması ve güvenlik ekiplerinin kritik sorunlara odaklanmasına olanak tanıması yer almaktadır.[2] Sürekli izleme, tehditlerin anında tespit edilmesini ve azaltılmasını sağlayarak, kuruluşun dijital varlıkları genelinde güvenlik duruşunun dinamik, anlık bir görünümünü sunmaktadır.[2] CVM, "sol kaydırma" güvenliğini ve kod geliştirilirken ve dağıtılırken zafiyetlerin hızlı bir şekilde düzeltilmesini sağlayarak yazılım geliştirme süreçlerine derinlemesine entegre olacaktır.[2] CVM, sürekli ağ envanteri ve izlemesi için etkili olup, tespit edilen zafiyetleri ve önerilen düzeltme iş akışlarını detaylandıran kapsamlı raporlama yetenekleri sunmaktadır.[2] Kullanıcının Nmap ve Nikto gibi araçları kullanarak otomatik tarama yapan programı, CVM ilkeleriyle doğrudan uyumludur. YZ destekli önceliklendirmenin entegrasyonu, risk puanlamasını ve raporlama özelliklerini önemli ölçüde geliştirerek, gerçek istismar edilebilirliğe ve iş etkisine dayalı olarak en kritik

URL/IP ile ilgili zafiyetleri vurgulamasına olanak tanıyacaktır.

[2]'a göre, kuruluşlar "veriye aç değil, veriye boğulmuş durumdalar." [1]'de "önceliklendirme olmadan hacim gürültüdür" uyarısı bulunmaktadır. Bu durum, siber güvenlik endüstrisinin sadece çok sayıda zafiyet bulmaktan, iş için en önemli, eyleme geçirilebilir riski oluşturanları akıllıca belirlemeye doğru ilerlediğini göstermektedir. Kullanıcının halihazırda zafiyet tespiti ve risk puanlaması içeren programı, risk puanlama mekanizmasını son derece sofistike ve bağlama duyarlı hale getirmelidir. Yalnızca genel ciddiyet puanlarının (örneğin, CVSS) ötesine geçerek, zafiyetin internete açık olup olmadığı, üretim ortamında bulunup bulunmadığı, yüksek ayrıcalıklı kimliklerle ilişkili olup olmadığı veya bilinen bir istismar kanıtına sahip olup olmadığı gibi bağlamsal faktörleri [22] entegre etmelidir. Bu gelişmiş bağlamsallaştırma, programın "risk puanlaması" özelliğini hem teknik hem de teknik olmayan kullanıcılar için gerçekten değerli ve eyleme geçirilebilir hale getirecek ve düzeltme çabalarını en önemli noktalara odaklamalarını sağlayacaktır.

[14]'te "Siber Dirençlilik—siber tehditleri öngörme, bunlara dayanma ve bunlardan kurtulma yeteneği" vurgulanmaktadır. CVM, sürekli izleme, zafiyetlerin gerçek zamanlı tespiti ve öncelikli düzeltme yetenekleriyle [2] bu direncin oluşturulmasına doğrudan katkıda bulunmaktadır. Saldırı yüzeyini sürekli olarak azaltarak ve kritik kusurları proaktif bir şekilde ele alarak, kuruluşlar doğal olarak daha sağlam hale gelmekte ve siber saldırılara karşı daha iyi dayanma ve kurtarma yeteneği kazanmaktadır. Programın "savunma önerileri" sadece bireysel zafiyetleri düzeltmekle kalmamalı, aynı zamanda tespit edilen sorunların kuruluşun genel siber direncine nasıl katkıda bulunduğuna veya onu nasıl olumsuz etkilediğine dair rehberlik sağlamalıdır. Bu, daha geniş, bütünsel bir direnç stratejisiyle uyumlu mimari değişiklikler, politika uygulamaları veya diğer güvenlik araçlarıyla [17] entegrasyonlar önermeyi içerebilir ve böylece kullanıcıya daha stratejik bir değer sunabilir.

Tablo 1: 2025 Yılında Siber Güvenlikteki En Önemli 10 Trend (Özet)

Bu tablo, tespit edilen en önemli 10 trende ilişkin kısa ve üst düzey bir genel bakış sunarak, özellikle raporun kapsamını hızlıca anlamak isteyen okuyucular için hızlı bir referans noktası görevi görmektedir.

Trend Başlığı	Kısa Açıklama	Temel Etki/Neden Önemli	Rapordaki İlgili Bölüm
YZ/ML Destekli Tehdit Tespiti ve Otomatik	YZ ve ML, tehditleri gerçek zamanlı tespit	Saldırgan YZ'sine karşı savunma hızını	Bölüm II.1

Yanıt	etmek ve otomatik yanıtlar sağlamak için büyük veri kümelerini analiz eder.	artırır, insan hatasını azaltır ve proaktif savunma sağlar.	
Ajan YZ ve Otonom Güvenlik Ajanları	Bağımsız karar alabilen ve çok adımlı görevleri yürütebilen otonom YZ varlıkları.	Gerçek zamanlı tehdit yanıtını hızlandırır, öngörücü güvenliği geliştirir ve saldırı yüzeyi yönetimini güçlendirir.	Bölüm II.2
YZ Destekli Önceliklendirme ile Sürekli Zafiyet Yönetimi (CVM)	Zafiyetleri gerçek zamanlı izler ve YZ kullanarak iş etkisine göre önceliklendirir.	Yanlış pozitifleri azaltır, düzeltme çabalarını optimize eder ve siber direnci artırır.	Bölüm III.3
Gelişmiş Sızma Testi: YZ Destekli ve Sürekli Entegrasyon	Sızma testini YZ ile otomatikleştirir ve CI/CD süreçlerine entegre ederek sürekli hale getirir.	Tehdit evrimine ayak uydurur, API'ler gibi kritik varlıkları daha etkin test eder ve DevSecOps olgunluğunu artırır.	Bölüm III.4
Saldırı Yüzeyi Yönetimi (ASM) ve Maruz Kalma Yönetimi	Kuruluşun tüm dijital varlıklarını sürekli olarak haritalar, değerlendirir ve izler.	Gizli riskleri ortaya çıkarır, güvenlik araçlarının silo etkisini azaltır ve ZTA'nın temelini oluşturur.	Bölüm IV.5
URL/IP Erişimi ve Ötesi İçin Sıfır Güven Mimarisi (ZTA)	Hiçbir kullanıcı, cihaz veya uygulamanın varsayılan olarak güvenilmediği ve sürekli doğrulandığı bir güvenlik modeli.	Veri ihlallerinin olasılığını ve etkisini azaltır, kimlik tabanlı saldırılara karşı koruma sağlar ve ayrıcalıklı erişimi sınırlar.	Bölüm IV.6
YZ Destekli Tehdit Tespiti ile Gelişmiş API Güvenliği	API'leri birincil saldırı vektörü olarak ele alır, YZ tabanlı anomali tespiti ve güvenlik kodunu entegre eder.	API trafiğindeki artışla birlikte ortaya çıkan zafiyetleri (BOLA, enjeksiyon) proaktif olarak ele alır.	Bölüm IV.7

Kuantum Dirençli Kriptografi Hazırlığı	Gelecekteki kuantum bilgisayarların mevcut şifrelemeyi kırma potansiyeline karşı yeni algoritmalar geliştirme ve bunlara geçiş.	Uzun vadeli veri gizliliğini korur ve "şimdi topla, sonra şifresini çöz" tehdidine karşı savunma sağlar.	Bölüm V.8
YZ Destekli Sosyal Mühendislik Savunması	YZ ve ML'yi kullanarak deepfake'ler ve gelişmiş kimlik avı gibi sofistike sosyal mühendislik saldırılarını tespit etme.	İnsan hatasını azaltır, YZ destekli aldatmacalara karşı çalışanları korur ve farkındalığı artırır.	Bölüm V.9
Bulut Güvenlik Duruşu Yönetimi (CSPM) ve Buluta Özgü Güvenlik	Bulut altyapısını korumak, yanlış yapılandırmaları belirlemek ve uyumluluğu sağlamak için otomatik görünürlük ve sürekli izleme.	Bulut ortamlarındaki yaygın yanlış yapılandırma tabanlı ihlalleri önler ve kuruluşların sorumluluklarını netleştirir.	Bölüm V.10

4. Gelişmiş Sızma Testi: YZ Destekli ve Sürekli Entegrasyon

Sızma testi (pentesting), geleneksel, periyodik ve genellikle manuel değerlendirmelerden, yazılım geliştirme yaşam döngüsüne (CI/CD boru hatları) derinlemesine entegre edilmiş daha sürekli, dinamik ve YZ destekli bir sürece doğru evrilmektedir.[1] YZ, zafiyet taraması, bulguların önceliklendirilmesi ve detaylı rapor oluşturma gibi rutin ve tekrarlayan pentesting görevlerini otomatikleştirmektedir. YZ, belirli zafiyetleri belirlemede ve otomatik olarak istismar etmede bile yardımcı olabilir. Ancak, otomasyonun hala zorlandığı karmaşık zincirleme istismarları ortaya çıkarmak, derinlemesine API testi yapmak ve nüanslı bulut yanlış yapılandırmalarını belirlemek için insan uzmanlığı vazgeçilmez olmaya devam etmektedir.[1] Sürekli sızma testi, geliştiricilere gerçek zamanlı geri bildirim sağlamak için güvenlik testlerini ve analizlerini doğrudan CI/CD boru hatlarına yerleştirmeyi içermektedir.[1]

Hızla gelişen, YZ destekli tehditler ile geleneksel, statik test döngüleri arasındaki "hız farkı", daha hızlı, daha sık ve daha akıllı testleri zorunlu kılmaktadır. Özellikle API'ler, yeterince test edilmedikleri ve aşırı güvenildikleri için hızla en riskli varlıklar haline

gelmektedir. Sürekli sızma testi, maruz kalma sürelerini önemli ölçüde azaltır ve maliyetli ihlalleri önleyerek güvenlik yatırımları için açık, ölçülebilir bir Yatırım Getirisi (ROI) sağlar.[1]

2025'teki potansiyel etkileri ve uygulama alanları arasında, Açık Kaynak İstihbaratı (OSINT) kaynaklarından akıllı veri analizi için YZ'den yararlanarak daha verimli ve hedefe yönelik bilgi toplama yer almaktadır.[19] YZ, zafiyetleri otomatik olarak belirleyebilir ve istismar edebilir, hedeflere erişim sağlayarak test çabalarına büyük ölçüde yardımcı olabilir.[19] URL/IP'ye açık uygulamalar için güvenlik testlerini geliştirme iş akışlarına erken ve sürekli olarak yerleştirerek güvenliğin baştan itibaren yerleşik olmasını sağlamak, "sol kaydırma" güvenliğini mümkün kılmaktadır.[1] Gelişmiş sızma testi, bulut sızma testine (örneğin, Kimlik ve Erişim Yönetimi (IAM) politikalarındaki yanlış yapılandırmalar, sunucusuz mimariler, konteynerleştirilmiş ortamlar) ve Nesnelerin İnterneti (IoT) sızma testine (örneğin, aygıt yazılımı analizi, kablosuz protokol analizi) odaklanmaktadır.[19] Kullanıcının Nmap, Nikto, Gobuster, WPScan, SSLScan, ARP-scan, Whois gibi popüler araçlar için otomatik tarama yapan programı, bu trendden doğrudan yararlanmaktadır. Program, bu taramaların YZ destekli otomasyonunu hedeflemeli, web/API uç noktalarının sürekli analizi için CI/CD ile entegre olmalı ve potansiyel olarak URL/IP aracılığıyla erişilebilen bulut ve IoT'ye özgü zafiyetler için modüller içermelidir.

YZ'nin sızma testindeki rolünü vurgulayan [1] ve [19]'ye rağmen, [1] kritik bir karşıt görüş sunmaktadır: "YZ'nin insan yargısının yerini aldığı efsanesi"nin çürütüldüğünü belirtmekte ve "otomasyonun hala zorlandığı alanlarda, özellikle API'ler, bulut yapılandırmaları ve karmaşık zincirleme istismarlarda manuel olarak keşfedilen zafiyetlerde neredeyse %2000'lik bir artış" olduğunu belirtmektedir. Bu durum, kritik bir nüansı ortaya koymaktadır: YZ, hacmi ölçeklendirmede ve bilinen kalıpları belirlemede mükemmel olsa da, derin bağlamsal anlayış, mantık hatalarını belirleme ve sofistike, çok aşamalı istismarlar oluşturma gibi konularda insan uzmanlığı vazgeçilmez olmaya devam etmektedir. Kullanıcının programı, insan sızma test uzmanlarını tamamen değiştirmek yerine yeteneklerini artırmak üzere tasarlanmalıdır. Otomatik tarama ve YZ destekli analiz özellikleri, tekrarlayan, yüksek hacimli görevleri üstlenerek insan uzmanlarının YZ'nin şu anda üstesinden gelemediği daha karmaşık, yüksek değerli ve nüanslı güvenlik testi yönlerine odaklanmasını sağlamalıdır. Programın raporlama ve düzeltme önerileri, bu karmaşık bulgular için verimli insan incelemesini ve karar almayı kolaylaştıracak şekilde yapılandırılmalıdır.

[1]'de "2025'te, CI/CD boru hatlarıyla uyumlu sürekli sızma testine geçişin sessizce yeni standart haline geldiği" belirtilmektedir. Bu, "yazılım tedarik zincirinizde koruyucu önlemler dağıtın" ve "SDLC'nizi güvence altına alın" konularını tartışan [22] tarafından

doğrudan desteklenmektedir. Bu durum, güçlü bir nedensel ilişki kurmaktadır: sürekli güvenlik doğrulama (sızma testi aracılığıyla) ihtiyacı, kuruluşları daha olgun bir DevSecOps modeline doğru iten birincil etkenlerden biridir; burada güvenlik, dağıtım sonrası bir denetim olmaktan ziyade, geliştirme boru hattının her aşamasına "sol kaydırma" yaklaşımıyla entegre edilmektedir. URL'leri ve IP'leri analiz eden bir program için bu trend, API öncelikli ilkeler ve sağlam entegrasyon yetenekleriyle tasarlanması gerektiği anlamına gelmektedir. Web uygulamalarına ve API'lere yapılan yeni dağıtımları veya değişiklikleri otomatik olarak taramak için CI/CD boru hatlarına kolayca dahil edilebilecek modüler bileşenler veya API'ler sunmalı ve geliştiricilere anında güvenlik geri bildirimi sağlamalıdır. Bu stratejik entegrasyon, programı bağımsız bir tarama aracından, kuruluşun güvenli yazılım geliştirme yaşam döngüsünün ayrılmaz bir parçasına dönüştürecektir.

Tablo 2: Siber Güvenlikte Temel YZ/ML Uygulamaları (Detaylı)

Bu tablo, Yapay Zeka (YZ) ve Makine Öğreniminin (ML) çeşitli siber güvenlik alanlarında nasıl özel olarak uygulandığına dair kapsamlı ve detaylı bir genel bakış sunmaktadır. YZ'nin faydalarını somut örneklerle açıklayarak, kullanıcının program geliştirmesi için eyleme geçirilebilir bilgiler sağlamayı amaçlamaktadır.

Uygulama Alanı	YZ/ML Nasıl Kullanılır?	Spesifik Faydalar	İlgili Kaynak Kimlikleri
Tehdit Tespiti ve Analizi	Büyük veri kümelerini (ağ trafiği, loglar) gerçek zamanlı analiz ederek anormallikleri ve davranışsal kalıpları belirler.	Sıfır gün zafiyetlerini, polimorfik kötü amaçlı yazılımları ve içeriden gelen tehditleri hızla tespit eder.	[3]
Zafiyet Önceliklendirme	Tehdit istihbaratını, bağlamsal veriyi ve iş etkisini analiz ederek kritik zafiyetleri belirler.	Yanlış pozitifleri azaltır, düzeltme çabalarını optimize eder ve güvenlik ekiplerinin en önemli risklere odaklanmasını sağlar.	[2]
Olay Yanıtı ve Otomasyon	Tehditleri tespit ettikten sonra otomatik eylemler	Dwell süresini azaltır, insan hatasını en aza indirir ve güvenlik	[3]

	(engelleme, karantinaya alma) gerçekleştirir ve olay yanıt iş akışlarını hızlandırır.	operasyonlarını ölçeklendirir (SOAR).	
Saldırı Yüzeyi Yönetimi (ASM)	Varlıkları (URL'ler, IP'ler, bulut hizmetleri) sürekli olarak keşfeder, haritalar ve izler.	Gizli varlıkları ve yanlış yapılandırmaları otomatik olarak belirler, saldırı yüzeyinin gerçek zamanlı görünümünü sağlar.	15
API Güvenliği	API davranışındaki anormallikleri (BOLA, enjeksiyon denemeleri) gerçek zamanlı tespit eder ve şüpheli trafiği kısıtlar.	API'ler aracılığıyla yapılan saldırıları (örneğin, veri sızdırma, yetkilendirme ihlalleri) önler.	10
Sosyal Mühendislik Savunması	Deepfake'lerdeki tutarsızlıkları (ses, video, piksel kalıpları) ve kimlik avı e-postalarındaki yazım stillerini analiz eder.	YZ tarafından oluşturulan aldatmacaları (deepfake, spear-phishing) tespit eder ve insan hatası riskini azaltır.	3
Kötü Amaçlı Yazılım Analizi	Yeni ve gelişen kötü amaçlı yazılım türlerini (polimorfik, dosyasız) analiz eder ve sınıflandırır.	Geleneksel imza tabanlı sistemlerin kaçırdığı tehditleri belirler ve tehdit istihbaratını geliştirir.	4
Öngörücü Güvenlik	Geçmiş olayları ve saldırı vektörlerini analiz ederek gelecekteki tehditleri tahmin eder.	Proaktif savunma önlemleri almayı sağlar, zafiyetleri istismar edilmeden önce belirler.	4
Bulut Güvenlik Duruşu Yönetimi	Bulut yapılandırmalarını	Yanlış yapılandırma tabanlı ihlalleri önler,	5

(CSPM)	sürekli olarak izler ve yanlış yapılandırmaları otomatik olarak tespit eder.	uyumluluğu sağlar ve bulut güvenlik duruşunu güçlendirir.	
Kimlik ve Erişim Yönetimi (IAM)	Kullanıcı ve makine kimliklerindeki anormal davranışları (olağandışı oturum açma, erişim kalıpları) tespit eder.	Kimlik tabanlı ihlalleri önler, ayrıcalıklı erişimi yönetir ve Sıfır Güven ilkelerini destekler.	[5]

IV. Bütünsel Güvenlik Duruşu ve Temel Değişimler

5. Saldırı Yüzeyi Yönetimi (ASM) ve Maruz Kalma Yönetimi

Saldırı Yüzeyi Yönetimi (ASM), bir kuruluşun tüm dijital ayak izini (web siteleri, bulut hizmetleri ve genel API'ler gibi harici varlıklar ile veritabanları ve bağlı cihazlar gibi dahili varlıklar dahil) tanımlamaya, değerlendirmeye ve izlemeye odaklanan sürekli bir süreçtir. Bu süreç, potansiyel siber tehditlere karşı koruma sağlamayı amaçlamaktadır. Maruz Kalma Yönetimi ise ASM'yi temel alarak, tanımlanan zafiyetlerden hangilerinin tehdit aktörleri tarafından gerçekten istismar edilebilir olduğunu belirler ve böylece teorik risklerin ötesine geçerek gerçek saldırı maruziyetini değerlendirir.[15]

ASM, tüm BT ortamını (bulut, şirket içi ve SaaS genelinde) haritalayarak varlıkların kapsamlı bir envanterini oluşturmayı, ilişkili riskleri sınıflandırmayı ve düzeltme çabalarını önceliklendirmeyi içerir. Dijital (örneğin, kusurlar, yanlış yapılandırmalar, API'ler, kod tabanları, YZ kaynakları), fiziksel (örneğin, uç noktalar, IoT cihazları) ve sosyal mühendislik unsurlarını kapsar. Bilinen ve bilinmeyen varlıkların sürekli izlenmesi ve otomatik keşfi, temel operasyonel yönlerdir.[15]

Günümüzün karmaşık, hibrit ortamlarında, varlıkların çoğalması, silolanmış güvenlik araçları ve artan saldırı vektörleri nedeniyle saldırı yüzeyini yönetmek hem kritik hem de zordur. ASM, potansiyel giriş noktalarına birleşik bir görünüm sağlayarak genel risk maruziyetini önemli ölçüde azaltır ve gerçekten istismar edilebilir zayıflıkları belirleyerek kuruluşların güvenlik çabalarını en önemli noktalara odaklamasına yardımcı olur.[15]

2025'teki potansiyel etkileri ve uygulama alanları arasında, farklı güvenlik araçlarından gelen bulguları birleştirerek tüm BT ortamındaki kör noktaları ortadan kaldırmak ve riskleri ilişkilendirmek yer almaktadır.[15] Proaktif risk azaltma stratejileri arasında gölge

BT'yi ortaya çıkarma, gereksiz varlıkları temizleme, güvenlik politikalarını güçlendirme, yayılmayı azaltmak için araçları birleştirme, üçüncü taraf ve tedarik zinciri risklerini ele alma ve kullanım ömrü sonuna gelmiş donanımı güvenli bir şekilde hizmetten çıkarma yer almaktadır.[15] ASM, sürekli keşif, doğrulama ve önceliklendirmeyi birleştirerek sürekli gelişen saldırı yüzeyine uyum sağlayan Sürekli Tehdit Maruz Kalma Yönetimi (CTEM) için temel oluşturmaktadır.[15] Kullanıcının URL'leri ve IP'leri tarama yeteneğine sahip programı, dijital saldırı yüzeyini haritalamaya doğrudan katkıda bulunmaktadır. Tespit edilen zafiyetler ve potansiyel saldırı yöntemleri hakkındaki bulguları, daha geniş bir ASM çerçevesine entegre edilmeli ve belirli URL/IP ile ilgili risklerin kuruluşun genel saldırı yüzeyine ve gerçek maruziyetine nasıl katkıda bulunduğuna dair kritik bağlam sağlamalıdır.

[15] ve [16], Saldırı Yüzeyi Yönetimi (ASM)'ni "otomatik keşif" ve "sürekli izleme"ye büyük ölçüde dayanan sürekli bir süreç olarak tanımlamaktadır. Aynı zamanda, [8] ve [14], sistemleri sürekli olarak izleyebilen ve anormallikleri tespit edebilen otonom ajanlar olan "ajan YZ"yi tanıtırken, [3] ve [4], YZ'nin gerçek zamanlı analiz ve tehdit istihbaratındaki rolünü vurgulamaktadır. Bu bilgilerin birleşimi, güçlü bir nedensel ilişkiyi işaret etmektedir: 2025'te etkili ve ölçeklenebilir ASM, dijital varlıkların ve bunlarla ilişkili zafiyetlerin hacmini, dinamik doğasını ve karmaşıklığını yönetmek için YZ ve otomasyonun yaygın uygulamasına kritik bir şekilde bağımlı olacaktır. Kullanıcının programı, yalnızca izole taramalar yapmakla kalmamalı, aynı zamanda özellikle internete açık URL'ler ve IP aralıkları için sürekli varlık keşfi ve haritalama yeteneklerini entegre etmeli veya sunmalıdır. Bu, keşif sürecini otomatikleştirmek ve değişiklikleri sürekli izlemek için YZ'den yararlanmalı, bu bilgileri bir ASM platformuna aktararak kuruluşun gelişen saldırı yüzeyinin dinamik, gerçek zamanlı ve kapsamlı bir görünümünü sağlamalıdır.

[15], "en az ayrıcalık ve tam zamanında erişim gibi sıfır güven ilkeleri"nin "tüm güvenlik duruşunuzu güçlendirme ve saldırı vektörlerinin sayısını azaltma" yolları olarak bahsetmektedir. [5] ve [14] da Sıfır Güven Mimarisi (ZTA)'nın artan benimsenmesini vurgulamaktadır. ZTA'nın temel bir ilkesi, bilmediğiniz şeye güvenemeyeceğinizdir. Bu nedenle, ZTA'yı etkili bir şekilde uygulamak için bir kuruluşun öncelikle ortamında *hangi* varlıkların (URL'ler/IP'ler, kullanıcılar, cihazlar ve insan dışı kimlikler dahil) bulunduğunu ve *nasıl* birbirine bağlı olduklarını kapsamlı bir şekilde anlaması gerekir. Bu temel anlayış ve varlık haritalaması, tam olarak ASM'nin sağladığı şeydir. Programın URL'ler ve IP'ler üzerindeki bulguları ve ilişkili zafiyetleri, Sıfır Güven politikalarını bilgilendirmek ve uygulamak için kritik girdilerdir. Örneğin, program kritik bir zafiyete sahip genel bir URL veya IP tespit ederse, Sıfır Güven ilkeleri, zafiyet giderilene kadar bu varlık etrafında anında, daha katı erişim kontrolleri veya ağ segmentasyonu gerektirecektir.

Program, tarama sonuçlarına dayanarak ZTA politika ayarlamaları için önerilerde bulunabilir ve böylece ZTA uygulaması için eyleme geçirilebilir istihbarat sağlayabilir.

6. URL/IP Erişimi ve Ötesi İçin Sıfır Güven Mimarisi (ZTA)

Sıfır Güven Mimarisi (ZTA), "asla güvenme, her zaman doğrula" ilkesine dayanan bir siber güvenlik modelidir. Bu, ağ çevresinin içinde veya dışında konumundan bağımsız olarak hiçbir kullanıcı, cihaz veya uygulamanın doğal olarak güvenilir olmadığı anlamına gelir. Belirli URL'lerden veya IP'lerden kaynaklanan veya bunları hedefleyenler de dahil olmak üzere tüm erişim girişimleri sürekli kimlik doğrulama ve yetkilendirme gerektirir.[3]

ZTA, kullanıcı kimliklerini (genellikle Çok Faktörlü Kimlik Doğrulama - MFA aracılığıyla), cihaz duruşunu ve erişim izni vermeden önce uygulama yetkilendirmesini sürekli olarak doğrulayarak saldırı yüzeyini sınırlar. Temel bileşenleri arasında mikro segmentasyon, en az ayrıcalık ilkesinin uygulanması ve yalnızca kimlik bilgilerinin ötesinde ek bilgileri dikkate alan bağlama duyarlı yetkilendirmenin uygulanması yer almaktadır.[3]

İşletmeler dijital dönüşümden geçip dağıtılmış bulut ortamlarına geçtikçe, geleneksel çevre tabanlı güvenlik modelleri yetersiz kalmaktadır. ZTA, bir hesabın ele geçirilmesi durumunda bile, saldırganın yeniden doğrulama gerektirmeden önce yalnızca sınırlı erişim elde etmesini sağlayarak veri ihlallerinin olasılığını ve etkisini önemli ölçüde azaltır ve böylece potansiyel hasarı sınırlar.[5]

2025'teki potansiyel etkileri ve uygulama alanları arasında, ZTA'nın 2025'te önemli gelişmeler gösteren MFA ve gelişmiş Kimlik ve Erişim Yönetimi (IAM) araçları gibi daha güçlü kimlik doğrulama yöntemlerini zorunlu kılması yer almaktadır.[5] Bulut ortamlarında makineler, IoT cihazları ve ajan YZ gibi insan dışı kimliklerin güvenliğinin sağlanmasına artan bir odaklanma vardır, çünkü bu insan dışı varlıklar da ZTA altında sürekli doğrulama gerektirmektedir.[9] Biyometrik kimlik doğrulama ve gerçek zamanlı risk faktörlerine göre erişim düzeylerini dinamik olarak ayarlayan bağlama duyarlı erişim, önemli ölçüde popülerlik kazanacaktır.[5] URL/IP analizi açısından, program, Sıfır Güven ilkelerini ihlal eden URL/IP erişimli hizmetlerdeki yanlış yapılandırmaları veya zafiyetleri (örneğin, zayıf kimlik doğrulama mekanizmaları, aşırı izinler, MFA eksikliği) belirleyebilir. Daha sonra, web uygulamaları için MFA'yı zorunlu kılma veya dahili IP tabanlı hizmetler için daha sıkı erişim kontrolleri uygulama gibi belirli ZTA uygulamalarını önererek kuruluşun güvenlik duruşunu geliştirebilir.

[15], Saldırı Yüzeyi Yönetimi (ASM)'nin hibrit ortamlardaki genişleyen saldırı yüzeyini yönetmek için çok önemli olduğunu belirtmektedir. Aynı zamanda, [14] ve [5], Sıfır Güven Mimarisi (ZTA)'nın artan benimsenmesini vurgulamaktadır. [14]'ün "veri ihlallerinin yaklaşık %80'ini kimlik tabanlı saldırıların oluşturduğunu" belirtmesi ve [8]'ün "Kimlik"i

"henüz çözülmemiş en büyük güvenlik sorunu" olarak tanımlamasıyla kritik bir bağlantı kurulmaktadır. Bu, güçlü bir nedensel ilişkiyi açıkça göstermektedir: dijital kimliklerin (hem insan hem de insan dışı) çoğalması ve kimlik tabanlı ihlallerin endişe verici yaygınlığı, kuruluşları Sıfır Güven'i temel, yaygın bir güvenlik ilkesi olarak benimsemeye zorlayan birincil etkenlerdir. Kullanıcının programı, taranan URL'leri ve IP'leriyle ilgili kimlik ve erişim yönetimi zafiyetleri için kapsamlı kontrolleri açıkça dahil etmelidir. Bu, yalnızca açık bağlantı noktalarını veya genel web uygulaması kusurlarını belirlemenin ötesine geçerek, kimlik doğrulama mekanizmalarının sağlamlığını (örneğin, MFA varlığı ve gücü, zayıf kimlik bilgilerine veya varsayılan parolalara karşı hassasiyet), yetkilendirme kusurlarını (örneğin, API'ler için Kırık Nesne Seviyesi Yetkilendirme (BOLA) veya Kırık Fonksiyon Seviyesi Yetkilendirme (BFLA) - [21]'ye göre) ve potansiyel ayrıcalık yükseltme yollarını değerlendirmeyi içermektedir. Programın raporları, bu bulguların bir kuruluşun Sıfır Güven duruşunu nasıl doğrudan etkilediğini belirgin bir şekilde vurgulamalı ve düzeltme için eyleme geçirilebilir öneriler sunmalıdır.

[14] ve [9], 2025'te kimlik güvenliğinin kritik yönleri olarak "insan dışı kimlikler (NHI'ler)" ve "makine kimliklerini yönetme"den açıkça bahsetmektedir. [8] ayrıca "ajan YZ ve makineden makineye iletişim gibi insan dışı kimlikler" hakkında ayrıntılı bilgi vermektedir. Bu, ZTA uygulaması için daha derin bir karmaşıklık katmanını ortaya koymaktadır: artık sadece insan kullanıcıları güvence altına almakla kalmayıp, aynı zamanda kuruluş kaynaklarına erişen ve onlarla etkileşim kuran çok sayıda otomatik süreç, IoT cihazı, bulut iş yükü ve YZ ajanını da yönetmeyi içermektedir. Programın, URL'ler/IP'ler aracılığıyla etkileşime girebilecek veya maruz kalabilecek İnsan Dışı Kimliklerin (NHI'ler) güvenliğini nasıl analiz edeceğini ve raporlayacağını değerlendirmesi gerekmektedir. Bu, yönetilmeyen veya güvensiz API anahtarlarını, güvensiz makineden makineye iletişim kanallarını veya URL/IP erişimli arayüzlere sahip yanlış yapılandırılmış bulut hizmeti hesaplarını belirlemeyi içerebilir. Programın "savunma önerileri", saldırı yüzeyindeki artan rolleri göz önünde bulundurarak bu NHI'leri Sıfır Güven ilkeleri altında güvence altına almak için özel rehberlik sağlamayı içermelidir.

7. YZ Destekli Tehdit Tespiti ile Gelişmiş API Güvenliği

Uygulama Programlama Arayüzleri (API'ler), siber suçlular için hızla birincil saldırı vektörü haline geldiğinden, API'lerin güvenliğine özel ve giderek kritikleşen bir odaklanma söz konusudur. Bu trend, sağlam kimlik doğrulama, ayrıntılı yetkilendirme, sıkı giriş doğrulaması ve gerçek zamanlı anomali tespiti ve otomatik yanıtlar için YZ'den yararlanmayı içermektedir.[1]

API güvenliği, "API'ler için Sıfır Güven"i (sürekli doğrulama ve en az ayrıcalıklı erişim

gerektiren), davranışsal anormallikleri (örneğin, Kırık Nesne Seviyesi Yetkilendirme (BOLA), enjeksiyon denemeleri, aşırı veri maruziyeti) tespit etmek için YZ/ML'yi ve güvenlik kontrollerini doğrudan DevOps boru hatlarına yerleştiren "Kod Olarak API Güvenliği"ni entegre etmektedir. Ayrıca, kimlik doğrulama için OAuth 2.0 ve OpenID Connect, jeton tabanlı kimlik doğrulama için JWT, ayrıntılı yetkilendirme için RBAC/ABAC, hız sınırlama ve şema doğrulama gibi modern savunma mekanizmalarına dayanmaktadır.[10]

API trafiği, 2025'te ilk kez web trafiğini geride bırakarak API'leri siber saldırılar için en sık giriş noktası haline getirmiştir. Kritik rollerine rağmen, API'ler genellikle yeterince test edilmemekte ve aşırı güvenilmekte, bu da önemli kör noktalara ve Kırık Nesne Seviyesi Yetkilendirme (BOLA), Kırık Fonksiyon Seviyesi Yetkilendirme (BFLA), Toplu Atama ve klasik enjeksiyon saldırıları gibi yaygın zafiyetlere yol açmaktadır.[1]

2025'teki potansiyel etkileri ve uygulama alanları arasında, güvenlik araçlarının genel web uygulaması taramalarının ötesine geçerek API'ye özgü kusurları ve yanlış yapılandırmaları belirlemeye giderek daha fazla odaklanması yer almaktadır.[1] API ağ geçitlerine entegre YZ, gerçek zamanlı davranışsal analize dayanarak kötü amaçlı IP adreslerini engelleme veya şüpheli trafiği kısıtlama gibi otomatik yanıtlar sağlayarak gerçek zamanlı API tehdit analizi sunacaktır.[10] Güvenlik kontrollerinin ve testlerinin doğrudan API geliştirme ve dağıtım boru hatlarına yerleştirilmesi, zafiyetlerin erken tespit edilmesini ve düzeltilmesini sağlayarak "sol kaydırma" API güvenliğini mümkün kılmaktadır.[1] API keşfi, testi, izlemesi ve tehdit tespitini entegre platformlarda birleştirme eğilimi, API yayılmasını yönetmek ve uyumluluğu sürdürmek için önemlidir.[14] Kullanıcının URL'leri tarayan programı, API tarama yeteneklerini açıkça geliştirmelidir. Bu, temel web uygulaması taramalarının ötesine geçerek API uç noktalarını, kimlik doğrulama/yetkilendirme mekanizmalarını ve yaygın API'ye özgü zafiyetleri anlamayı gerektirmektedir. Program, URL/IP analizi aracılığıyla belirlenen API trafik modelleri üzerinde davranışsal anomali tespiti için YZ'den yararlanmalıdır.

[21], çarpıcı bir iddiada bulunmaktadır: "API trafiği, 2025'te ilk kez web trafiğini geride bırakarak API'leri siber saldırılar için en sık giriş noktası haline getirdi." [1] ise API'leri "hala yumuşak hedef" ve "verilerinize açılan arka kapı" olarak nitelendirerek bu durumu daha da vurgulamaktadır. Bu fenomen, mikro hizmetlerin, sunucusuz mimarilerin ve bulut ortamlarının [5] yaygın bir şekilde benimsenmesinin doğrudan bir sonucudur, çünkü bunlar doğal olarak kapsamlı API iletişimine dayanmaktadır. Bu mimari değişim, API saldırı yüzeyini dramatik bir şekilde genişleterek, saldırganlar için yeni, birincil bir hedef oluşturmuştur. Kullanıcının programı, URL taraması için tasarlanmış olsa da, derinlemesine ve kapsamlı API güvenlik testine öncelik vermelidir. "Zafiyet tespiti" modülü, API'ye özgü kusurlar (örneğin, Kırık Nesne Seviyesi Yetkilendirme (BOLA), Kırık

Fonksiyon Seviyesi Yetkilendirme (BFLA), aşırı veri maruziyeti, API parametrelerinde enjeksiyon zafiyetleri ve uygun hız sınırlamasının olmaması gibi [21]'de detaylandırılanlar) için yüksek derecede uzmanlaşmış olmalıdır. Program tarafından üretilen "saldırı yöntemleri" ve "savunma önerileri", geleneksel web uygulaması zafiyetlerinin ötesine geçerek, API güvenliği için özel olarak hazırlanmış ayrıntılı, eyleme geçirilebilir rehberlik içermelidir.

[21], temel API güvenlik trendleri olarak "API'ler için Sıfır Güven," "YZ Destekli Tehdit Tespiti" ve "Kod Olarak API Güvenliği"ni listelemektedir. Bu trendler izole değildir, aksine Sıfır Güven Mimarisi [5], yaygın YZ destekli güvenlik [3] ve DevSecOps'un "Sol Kaydırma" yaklaşımı [1] gibi daha geniş, genel siber güvenlik trendlerini doğrudan yansıtmaktadır. Bu güçlü tematik uyum, API güvenliğinin izole bir alan olmadığını, aksine daha geniş siber güvenlik ortamında meydana gelen en önemli gelişmelerin ve zorlukların ayrılmaz bir parçası ve yansıması olduğunu göstermektedir. Programın mimari tasarımı bu yakınlaşmayı yansıtmalıdır. API tarama modülü, bağımsız bir özellik olmaktan ziyade, anomali tespiti için YZ/ML yetenekleriyle ve Sıfır Güven uyumluluğunu değerlendirmek için raporlama mekanizmalarıyla sıkı bir şekilde entegre olmalıdır. Program ayrıca "Kod Olarak API Güvenliği" şablonları sağlayabilir veya geliştiricilerin API geliştirme yaşam döngüsünün erken aşamalarında güvenlik kontrollerini ve en iyi uygulamaları yerleştirmelerine yardımcı olmak için CI/CD boru hatlarıyla doğrudan entegrasyonlar sunabilir.

V. Gelişen Tehditler ve Proaktif Savunma Stratejileri

8. Kuantum Dirençli Kriptografi Hazırlığı

Bu trend, siber güvenlik topluluğu içinde, gelecekteki kuantum bilgisayarların saldırılarına dayanacak şekilde tasarlanmış yeni kriptografik algoritmalar geliştirmeye ve bunlara geçiş yapmaya yönelik proaktif, ileriye dönük bir çabayı temsil etmektedir. Bu kuantum bilgisayarlar, tam olarak hayata geçirildiklerinde, RSA ve ECC gibi şu anda yaygın olarak kullanılan birçok şifreleme yöntemini kırma teorik yeteneğine sahiptir.[7]

Hazırlık, hem klasik hem de kuantum saldırılarına karşı güvenli olduğuna inanılan matematiksel yapılar olan kuantum sonrası kriptografik (PQC) algoritmalarını tanımayı ve aktif olarak uygulamayı içermektedir. Örnekler arasında kafes tabanlı kriptografi, hash tabanlı imzalar ve kod tabanlı kriptografi yer almaktadır. CISA gibi devlet kurumları, mevcut şifrelemeyi kırabilecek pratik, büyük ölçekli kuantum bilgisayarların hala yıllar uzakta olmasına rağmen, kritik altyapı sektörlerini bu kaçınılmaz değişime hazırlanmaya çağırmaktadır.[8]

Büyük ölçekli kuantum şifre çözme tehdidi 2025'te hemen gerçekleşmeyebilirken,

"şimdi topla, sonra şifresini çöz" kavramı önemli bir uzun vadeli risk oluşturmaktadır. Bu, sofistike saldırganların bugün şifrelenmiş hassas verilerin büyük miktarlarını topluyor olabileceği ve kuantum bilişim yetenekleri kullanılabilir hale geldiğinde bunları yıllar sonra çözmeyi amaçladığı anlamına gelmektedir. Bu nedenle, hassas bilgilerin uzun vadeli gizliliğini ve bütünlüğünü korumak için proaktif hazırlık çok önemlidir.[7]

2025'teki potansiyel etkileri ve uygulama alanları arasında, PQC'ye geçişin VPN'ler, TLS/SSL (URL'ler için HTTPS trafiğini güvence altına alan) ve güvenli kabuk (SSH) dahil olmak üzere IP ağları üzerinden kullanılan tüm güvenli iletişim protokollerini temelden etkilemesi yer almaktadır. Hassas verilerin hem depoda (örneğin, veritabanlarında, bulut depolamada) hem de aktarımda (örneğin, finansal işlemler, kişisel sağlık bilgileri) uzun süreli gizliliğinin sağlanması gerekmektedir. Kuruluşların, yeni kuantum dirençli standartlar ortaya çıktıkça ve doğrulandıkça kriptografik algoritmaları kolayca değiştirmeye olanak tanıyan stratejiler ve mimariler geliştirmeleri gerekecektir. URL/IP analizi açısından, program öncelikle anlık zafiyetleri analiz etse de, URL erişimli hizmetlerin kriptografik gücünü raporlayarak (örneğin, mevcut SSLScan yeteneğini kullanarak) katkıda bulunabilir. Bu trend, programın kuantum sonrası kriptografi hazırlığını değerlendirmek üzere evrilmesi gerektiğini, örneğin gelecekte kuantum saldırılarına karşı savunmasız olduğu bilinen algoritmaların kullanımını işaretleyerek veya PQC benimsenmesi için öneriler sunarak bunu yapabileceğini göstermektedir.

[8], "şimdi topla, sonra şifresini çöz" kavramından açıkça bahsetmektedir. Bu, kritik bir nüanstır: kuantum bilgisayarlar 2025'te tam olarak çalışır durumda olmasa bile, saldırganlar *bugün* şifrelenmiş verileri *yıllar sonra* şifresini çözme niyetiyle topluyor olabilirler. Bu durum, gelecekteki teorik bir tehdidi, uzun ömürlü hassas veriler için mevcut bir riske dönüştürmektedir. Kullanıcının programı için, doğrudan kuantum şifre çözme analizi mümkün olmasa da, hassas verilerin kriptografik protokoller kullanılarak nerede iletildiğini veya depolandığını belirleyerek katkıda bulunabilir. Programın "savunma önerileri", kuruluşları kritik veriler için "kuantum hazırlıklarını" değerlendirmeye, özellikle URL'ler/IP'ler aracılığıyla maruz kalan uzun vadeli hassas bilgiler için, ve kuantum sonrası kriptografi benimsenmesi için plan yapmaya başlamaya teşvik etmeyi içerebilir. Bu, risk değerlendirmesine ileriye dönük bir boyut katmaktadır.

9. YZ Destekli Sosyal Mühendislik Savunması

Bu trend, deepfake'ler, YZ tarafından oluşturulan hedefli kimlik avı e-postaları ve vishing gibi giderek sofistike hale gelen sosyal mühendislik saldırılarını tespit etmek ve bunlara karşı koymak için YZ ve makine öğreniminden yararlanmayı içermektedir.[3] YZ modelleri, deepfake'ler için piksel kalıplarını, ses modülasyonunu, dudak

senkronizasyonunu ve kimlik avı için yazım stillerini analiz etmektedir. Tutarsızlıkları belirleyebilir ve davranışsal doğrulama sağlayabilirler. Kuruluşlar, çalışan eğitimine ve YZ destekli sosyal mühendislik için yeni tespit kontrollerine öncelik vermelidir.[3]

Siber suçlular, kimlik avı kampanyalarını otomatikleştirmek ve ikna edici deepfake içerikler üretmek için YZ kullanmaktadır, bu da yazım stillerini taklit etmelerini ve bireyleri benzeri görülmemiş bir hassasiyetle hedeflemelerini sağlamaktadır. İnsan hatası, en önemli saldırı vektörü olmaya devam etmektedir.[3]

2025'teki potansiyel etkileri ve uygulama alanları arasında, YZ tarafından oluşturulan hedefli kimlik avı e-postalarının yazım stillerini taklit edebilmesi yer almaktadır.[3] YZ modelleri, kimlik taktikleri için deepfake ses/videodaki tutarsızlıkları tespit edebilir.[4] YZ destekli sosyal mühendislik için çalışan eğitimine ve yeni tespit kontrollerine öncelik verilmelidir.[4] Programın URL analizi, YZ tarafından oluşturulan kimlik avı kampanyalarında kullanılan kötü amaçlı URL'lerin özelliklerini (örneğin, alan adı istismarı, yazım hatası istismarı, yeni kaydedilen alan adları veya bilinen deepfake dağıtımıyla ilişkili olanlar) tespit etmek için modüller içerebilir. Ayrıca, bir savunma önlemi olarak çalışan eğitimini de önerebilir.

[3]'de "İnsan hatası, en önemli saldırı vektörü olmaya devam ediyor" ifadesi yer almaktadır. [7]'de ise "insan unsuru en büyük" savunmasız saldırı yüzeylerinden biri olarak belirtilmektedir. [4], "Deepfake ve Sosyal Mühendislik Savunması"nı en önemli YZ trendlerinden biri olarak vurgulamaktadır. Bu durum, teknolojik gelişmelere rağmen insan faktörünün kritik bir zayıf nokta olmaya devam ettiğini ve YZ'nin bu zayıflığı daha etkili bir şekilde istismar etmek için silahlandırıldığını göstermektedir. Program, URL'lerin/IP'lerin teknik zafiyetlerine odaklanırken, "savunma önerileri" insan odaklı güvenliği de kapsamalıdır. Program, sosyal mühendislik taktikleriyle (örneğin, kimlik avı alan adları) yaygın olarak ilişkilendirilen URL'leri/IP'leri işaretleyebilir ve çalışanlar için YZ tarafından oluşturulan içerik risklerini vurgulayan sağlam güvenlik farkındalığı eğitimi önerebilir. Program ayrıca, insan direncini test etmek için simüle edilmiş kimlik avı saldırıları araçlarıyla entegre olabilir veya bu tür araçları önerebilir.

10. Bulut Güvenlik Duruşu Yönetimi (CSPM) ve Buluta Özgü Güvenlik

Bulut Güvenlik Duruşu Yönetimi (CSPM), bulut altyapısını korumak, yanlış yapılandırmaları belirlemek ve uyumluluğu sağlamak için otomatik görünürlük ve sürekli izleme kullanan bir metodolojidir. Buluta özgü uygulamaları ve hizmetleri güvence altına almak için çok önemlidir.[5] CSPM araçları, bulut yapılandırmalarını en iyi uygulamalara ve düzenlemelere karşı sürekli olarak değerlendirerek, yanlış yapılandırmaları (örneğin, yanlış atanmış izinler, konteynerlere genel erişim, MFA eksikliği) tespit eder. Risk görselleştirmesi sunar ve uyumluluğun otomasyonuna

yardımcı olurlar. YZ ayrıca uyumluluğu otomatikleştirmede ve yanlış yapılandırmaları tespit etmede CSPM'ye yardımcı olmaktadır.[5]

Bulut ortamları karmaşık ve dinamiktir, bu da yanlış yapılandırmaları veri ihlallerinin yaygın bir nedeni haline getirmektedir. Bulut zafiyetleri 1.8 kat artmıştır ve genellikle IAM yanlış adımları, anahtar sızıntıları veya zayıf varsayılan ayarlardan kaynaklanmaktadır. CSPM, bulut iş akışlarını güvence altına almak için yerel bulut sağlayıcılarından daha verimli araçlar sağlamaktadır.[1]

2025'teki potansiyel etkileri ve uygulama alanları arasında, bulut hizmetlerindeki güvenlik açıklarının otomatik olarak tespit edilmesi ve düzeltilmesi yer almaktadır.[5] GDPR, PCI DSS ve SEC yönergeleri gibi düzenlemelere uyumluluğun sürekli olarak sağlanması.[5] Sunucusuz mimarileri, konteynerleştirilmiş ortamları ve çoklu bulut dağıtımlarını güvence altına alarak buluta özgü uygulama güvenliğinin sağlanması.[15] Birçok URL ve IP, bulut tabanlı hizmetlere çözümlenmektedir. Program, URL'ler/IP'ler aracılığıyla erişilebilen bulutla ilgili yanlış yapılandırmaları (örneğin, herkese açık S3 kovaları, güvensiz konteyner kayıt defterleri, yanlış yapılandırılmış IAM politikaları) özel olarak belirlemelidir. Risk puanlaması, yaygınlıkları ve etkileri nedeniyle bu bulut yanlış yapılandırmalarını ağır bir şekilde değerlendirmelidir.

[1], "Bulut ortamlarındaki ihlallerin çoğu sıfır gün açıklarından kaynaklanmıyor. Bunlar yanlış yapılandırmalar, zayıf erişim kontrolü ve dikkatsiz IAM'den kaynaklanıyor" demektedir. [5], "Yanlış Yapılandırma Tespiti"ni temel bir CSPM yeteneği olarak listeleyerek bunu pekiştirmekte ve "yanlış atanmış izinler, konteynerlere genel erişim, MFA eksikliği veya aşırı izinli ağ bağlantısı" gibi durumları vurgulamaktadır. Bu durum, en yaygın ve etkili bulut zafiyetlerinin sofistike istismarlar değil, temel yapılandırma hataları olduğunu göstermektedir. Kullanıcının programı, bulut kaynaklarına işaret eden URL'leri ve IP'leri tararken, yaygın bulut yanlış yapılandırmalarının tespitine öncelik vermelidir. Bu, geleneksel ağ/web uygulaması zafiyetlerinin ötesine geçerek, bulut hizmeti yapılandırmaları, IAM politikaları [19] ve depolama kovası izinleri için özel kontroller gerektirmektedir. Programın "savunma önerileri", bu yanlış yapılandırmaları düzeltmek için açık, eyleme geçirilebilir adımlar sağlamalıdır.

[1], paylaşılan sorumluluk modellerine rağmen, "suçun genellikle yanlış bir şekilde sağlayıcılara yüklendiğini" belirtmektedir. Ayrıca, "bulut uygulamalarını güvence altına almak, yığının kendi kısmına sahip olmak anlamına gelir" vurgusu yapmaktadır. Bu, kritik bir zorluğu ortaya koymaktadır: kuruluşlar genellikle bulut güvenliğindeki rollerini yanlış anlamakta ve bulut sağlayıcılarının her şeyi hallettiğini varsaymaktadır. CSPM, kuruluşlara bulut içindeki güvenlik duruşlarını yönetmeleri için araçlar sağlayarak bu durumu doğrudan ele almaktadır. Programın raporları, kullanıcılara paylaşılan

sorumluluk modeli içindeki sorumluluklarını öğretmelidir. URL/IP analizi aracılığıyla bir bulut yanlış yapılandırması tespit edildiğinde, rapor zafiyeti açıkça kuruluşun yapılandırma seçimlerine atfetmeli, bulut sağlayıcısının platformuna değil, ve bu bağlamda nasıl düzeltileceğine dair özel rehberlik sağlamalıdır. Bu, bir sahiplenme kültürünün geliştirilmesine yardımcı olmaktadır.

Tablo 3: Örnek Zafiyet Yönetimi ve Sızma Testi Araçları Manzarası

Bu tablo, kullanıcının programının yetenekleriyle uyumlu mevcut ve gelişmekte olan araçlar hakkında bağlam sağlamayı amaçlamaktadır. Programın daha geniş ekosisteme nasıl uyduğunu göstermekte ve kullanıcının programının birleştirdiği ve otomatikleştirdiği araç türlerini vurgulamaktadır.

Araç Adı	Kategori	Temel Özellikler/Güçlü Yönler	URL/IP Analizi/Program Hedefine Uygunluk	Kaynak Kimlikleri
Nmap	Ağ Keşfi ve Güvenlik Denetimi	Ağ envanteri ve izleme için etkili; özelleştirilebilir taramalar ve güçlü betik yetenekleri.	Programın temel ağ tarama yeteneğiyle uyumlu, IP adresleri üzerinde keşif ve ilk zafiyet tespiti için kritik.	2
OpenVAS (Greenbone)	Altyapı Zafiyet Değerlendirme Platformu	Kapsamlı zafiyet veritabanı, geniş eklenti yelpazesi, düzenli güncellemeler, açık kaynaklı ve ücretsiz.	Otomatik zafiyet tarama ve değerlendirme yeteneklerini genişletir, programın zafiyet tespitini zenginleştirir.	2
Qualys VMDR	Sürekli Zafiyet Yönetimi Platformu	Kapsamlı zafiyet kapsamı, sürekli izleme, entegre yama yönetimi, ölçeklenebilirlik, detaylı	Programın risk puanlaması ve raporlama özelliklerini geliştirmek için CVM ilkelerini	17

		raporlama.	entegre eder.	
Rapid7 InsightVM	Gerçek Zamanlı Zafiyet Yönetimi	Gerçek zamanlı analiz, zafiyet önceliklendirme, düzeltme çabalarını izleme, SIEM entegrasyonu.	Programın gerçek zamanlı zafiyet tespiti ve risk önceliklendirme yeteneklerini güçlendirir.	17
Ridge Security RidgeBot	YZ Destekli Otomatik Sızma Testi	Zafiyet taramalarını sızma testiyle birleştirir, YZ destekli otomatik testler, kendini öğrenme yeteneği.	Programın otomatik saldırı simülasyonu ve zafiyet istismarı yetenekleri için bir model sunar.	23
Invicti (eski Netsparker)	Otomatik Web Zafiyet Tarayıcı	Enjeksiyon, XSS gibi web tabanlı zafiyetleri otomatik olarak tanımlar, doğru ve kanıtlanmış istismarlar sağlar.	Programın URL tabanlı web uygulaması zafiyet analizi ve raporlama yeteneklerini destekler.	23
Burp Suite	Web Uygulaması Güvenlik Testi	Kapsamlı web zafiyet taraması, geniş otomasyon ve manuel yetenekler, güçlü proxy özellikleri.	Programın web uygulaması zafiyet tespiti ve manuel test yeteneklerini tamamlar.	18
SentinelOne Singularity™ Platformu	Gelişmiş Saldırı Yüzeyi Yönetimi	YZ destekli tehdit tespiti, otonom yanıtlar, XDR, kimlik ve bulut güvenliği, kapsamlı görünürlük.	Programın URL/IP tabanlı ASM yeteneklerini daha geniş bir kurumsal güvenlik duruşuna	12

			entegre etme potansiyelini gösterir.	
Recorded Future Intelligence Cloud	Tehdit İstihbarat Platformu	Açık ve karanlık web dahil interneti indeksler, gerçek zamanlı, eyleme geçirilebilir tehdit istihbaratı sağlar.	Programın YZ destekli tehdit istihbaratı entegrasyonu ve proaktif analiz yetenekleri için bir referans noktasıdır.	[11]
Cyble Vision	Siber Tehdit İstihbarat Platformu	YZ destekli çözümler, Saldırı Yüzeyi Yönetimi, Marka İstihbaratı, Karanlık Web İzleme, Zafiyet Yönetimi.	Programın kapsamını tehdit istihbaratı ve saldırı yüzeyi yönetimi alanlarına genişletmek için bir model sunar.	[11]

VI. Sonuç: 2025 İçin Dirençli Siber Savunmalar Oluşturmak

2025 yılı siber güvenlik ortamı, YZ'nin hem saldırganlar hem de savunmacılar tarafından yaygın olarak kullanılmasıyla karakterize edilen dinamik ve hızla gelişen bir alandır. Bu "hız farkı" ortamında, kuruluşların siber saldırılara karşı dirençli olmaları için proaktif, akıllı ve uyarlanabilir güvenlik duruşları benimsemeleri zorunludur. Bu rapor, URL ve IP adresleri aracılığıyla saldırı ve savunma analizi yapan programların geliştirilmesi için en kritik on trendi vurgulamıştır.

Bu trendlerin her biri, kullanıcının programının yeteneklerini önemli ölçüde artırma potansiyeli taşımaktadır. YZ/ML destekli tehdit tespiti ve otomatik yanıt, programın yalnızca mevcut zafiyetleri belirlemesini değil, aynı zamanda gelecekteki saldırı vektörlerini tahmin etmesini ve otomatik savunma eylemleri gerçekleştirmesini sağlayacaktır. Ajan YZ'nin entegrasyonu, programın otonom keşif ve yanıt yeteneklerini geliştirerek saldırı yüzeyi yönetimini gerçek zamanlı hale getirecektir.

Sürekli Zafiyet Yönetimi (CVM) ve YZ destekli önceliklendirme, programın risk puanlamasını iyileştirerek, tespit edilen zafiyetlerin gerçek iş etkisine göre önceliklendirilmesini sağlayacaktır. Gelişmiş sızma testi teknikleri, programın otomatik tarama yeteneklerini CI/CD boru hatlarına entegre etmesini ve API'ler gibi modern

saldırı yüzeylerinde daha derinlemesine analizler yapmasını gerektirmektedir. Bu, programın insan sızma test uzmanlarını tamamlayıcı bir araç olarak konumlandırılmasına olanak tanıyacaktır.

Saldırı Yüzeyi Yönetimi (ASM) ve Maruz Kalma Yönetimi, programın bulgularını daha geniş bir güvenlik bağlamına yerleştirmek için kritik öneme sahiptir. Program, URL ve IP tarama sonuçlarını bir ASM çerçevesine entegre ederek, kuruluşun tüm dijital ayak izine ilişkin birleşik bir görünüm sunmalıdır. Sıfır Güven Mimarisi (ZTA) ilkeleri, programın kimlik ve erişim yönetimi zafiyetlerini (insan dışı kimlikler dahil) değerlendirme yeteneğini güçlendirmeli ve bu bulgulara dayanarak ZTA uygulamaları için öneriler sunmalıdır. Gelişmiş API güvenliği, programın URL tarama yeteneklerinin API'ye özgü zafiyetlere derinlemesine odaklanmasını sağlamalı ve YZ destekli anomali tespiti ile API trafiğini izlemelidir.

Gelişen tehditler açısından, Kuantum Dirençli Kriptografi hazırlığı, programın uzun vadeli veri gizliliği risklerini değerlendirmesine olanak tanıyacak ve YZ Destekli Sosyal Mühendislik Savunması, programın kimlik avı URL'lerini tespit etme ve insan odaklı güvenlik önerileri sunma yeteneğini artıracaktır. Son olarak, Bulut Güvenlik Duruşu Yönetimi (CSPM), programın bulut tabanlı URL'ler ve IP'ler aracılığıyla ortaya çıkan yanlış yapılandırmaları belirlemesine ve düzeltme için net, sahiplenme odaklı öneriler sunmasına olanak tanıyacaktır.

Özetle, kullanıcının programı, yalnızca mevcut güvenlik araçlarını konsolide etmekle kalmayıp, aynı zamanda YZ'nin dönüştürücü gücünü, sürekli izleme paradigmalarını ve bütünsel güvenlik yaklaşımlarını entegre ederek 2025 ve sonrası için siber güvenlikte öncü bir çözüm haline gelmelidir. Bu entegrasyon, proaktif zafiyet tespiti, eyleme geçirilebilir savunma önerileri ve hem teknik hem de teknik olmayan kullanıcılar için anlaşılır raporlama sağlayarak, kuruluşların giderek daha karmaşık hale gelen siber tehditlere karşı dirençlerini önemli ölçüde artıracaktır.

Alıntılanan çalışmalar

1. Penetration Testing Trends 2025: Insights & Predictions, erişim tarihi Haziran 5, 2025, https://www.getastra.com/blog/security-audit/penetration-testing-trends/
2. Top 10 Vulnerability Scanning Tools – You Need to Know in 2025 - Qualysec Technologies, erişim tarihi Haziran 5, 2025, https://qualysec.com/vulnerability-scanning-tools/
3. Business growth through superior technology - BytePlus, erişim tarihi Haziran 5, 2025, https://www.byteplus.com/en/topic/514517
4. Emerging AI Trends in Cybersecurity: A Guide for 2025, erişim tarihi Haziran 5, 2025, https://overturepartners.com/it-staffing-resources/emerging-ai-trends-in-cybers

ecurity
5. Top Cloud Security Trends in 2025 - Check Point Software, erişim tarihi Haziran 5, 2025, https://www.checkpoint.com/cyber-hub/cloud-security/what-is-code-security/top-cloud-security-trends-in-2025/
6. The Cyber Risk Tides Are Turning: RSAC '25 And Beyond - Forrester, erişim tarihi Haziran 5, 2025, https://www.forrester.com/blogs/the-cyber-risk-tides-are-turning-rsac-25-and-beyond/
7. Which cybersecurity threats will dominate 2025? - Silicon Republic, erişim tarihi Haziran 5, 2025, https://www.siliconrepublic.com/enterprise/cybersecurity-threats-predictions-tech-trends-2025-data-breaches-hacking-cyberattacks
8. 7 Trends to Watch from RSA 2025 - NightDragon | Securing our ..., erişim tarihi Haziran 5, 2025, https://www.nightdragon.com/insights/7-trends-to-watch-from-rsa-2025/
9. Gartner's Top Cybersecurity Trends for 2025—Are You Securing AI?, erişim tarihi Haziran 5, 2025, https://www.forcepoint.com/blog/insights/gartner-top-cybersecurity-trends-2025-secure-ai
10. api7.ai, erişim tarihi Haziran 5, 2025, https://api7.ai/blog/2025-top-8-api-management-trends#:~:text=Security%20Enhancements&text=By%202025%2C%20AI%20will%20be,addresses%20or%20throttling%20suspicious%20traffic.
11. Best Security Threat Intelligence Products and Services Reviews 2025 | Gartner Peer Insights, erişim tarihi Haziran 5, 2025, https://www.gartner.com/reviews/market/security-threat-intelligence-products-and-services
12. Top 7 Threat Intelligence Solutions for 2025 - SentinelOne, erişim tarihi Haziran 5, 2025, https://www.sentinelone.com/cybersecurity-101/threat-intelligence/threat-intelligence-solutions/
13. Generative AI in Cyber Security Research Report 2025: Market Opportunities and Strategies to 2034 - Remote Work and Data Breach Costs Fuel Growth Amid High Implementation Challenges - GlobeNewswire, erişim tarihi Haziran 5, 2025, https://www.globenewswire.com/news-release/2025/05/12/3079051/28124/en/Generative-AI-in-Cyber-Security-Research-Report-2025-Market-Opportunities-and-Strategies-to-2034-Remote-Work-and-Data-Breach-Costs-Fuel-Growth-Amid-High-Implementation-Challenges.html
14. RSA Conference 2025: 5 Big Trends Shaping the Future of Cybersecurity - SafeBase, erişim tarihi Haziran 5, 2025, https://safebase.io/blog/5-trends-rsa-2025
15. What Is Attack Surface Management in 2025? | Wiz, erişim tarihi Haziran 5, 2025, https://www.wiz.io/academy/attack-surface-management
16. Top 11 Attack Surface Management Tools For 2025 - SentinelOne, erişim tarihi Haziran 5, 2025,

https://www.sentinelone.com/cybersecurity-101/cybersecurity/attack-surface-management-tools/
17. Top 9 Vulnerability Management Tools for 2025: Features & Comparisons | Balbix, erişim tarihi Haziran 5, 2025, https://www.balbix.com/insights/best-vulnerability-management-tools-for-2025-a-comprehensive-comparison/
18. Top 10 Continuous Vulnerability Management Tools for 2025, erişim tarihi Haziran 5, 2025, https://firecompass.com/top-10-continuous-vulnerability-management-tools-2025/
19. Top 5 Penetration Testing Strategies in 2025 - Teceze, erişim tarihi Haziran 5, 2025, https://teceze.com/penetration-testing-strategies-2025
20. Secure Your Fortress: Building Robust and Resilient Defenses for ..., erişim tarihi Haziran 5, 2025, https://www.sans.org/webcasts/secure-your-fortress-building-robust-resilient-defenses-2025/
21. The State of API Security in 2025: Emerging Threats and Best Practices - SecureMyOrg, erişim tarihi Haziran 5, 2025, https://securemyorg.com/2025/04/05/the-state-of-api-security-in-2025/
22. Key learnings from the 2025 State of DevSecOps study - Datadog, erişim tarihi Haziran 5, 2025, https://www.datadoghq.com/blog/devsecops-2025-study-learnings/
23. Essential Vulnerability Scanning Tools in 2025 - Cyphere, erişim tarihi Haziran 5, 2025, https://thecyphere.com/blog/vulnerability-scanning-tools-2025/