2025 Yılı İçin Gelişmiş Ağ Güvenliği Analizi: Host Tarama, Güvenlik Duvarı Tespiti, MAC Adresi Belirleme ve Güvenlik Duvarı Atlatma Teknikleri

Günümüzün hızla gelişen dijital ortamında, siber güvenlik tehditleri giderek daha karmaşık ve yaygın hale gelmektedir. Ağ güvenliği araçları, potansiyel tehditleri proaktif bir şekilde tespit etmek ve analiz süreçlerini otomatikleştirmek için hayati bir rol oynamaktadır. Bu rapor, 2025 yılı için host tarama, güvenlik duvarı tespiti, MAC adresi belirleme ve güvenlik duvarı atlatma teknikleri alanındaki en son ve en etkili on trendi derinlemesine incelemektedir. Bu tekniklerin her biri, ağ güvenliği analizlerini kolaylaştıran ve sistem güvenilirliğini değerlendiren Python tabanlı bir ağ güvenliği aracı olan ScanMatrix gibi çözümlerin gelecekteki gelişimine yön verecek önemli bilgiler sunmaktadır.

2025 Yılında Öne Çıkan Ağ Güvenliği Teknikleri ve Trendleri

1. Yapay Zeka Destekli Akıllı Keşif ve Adaptif Tarama

Yapay zeka (YZ) ve makine öğrenimi (ML), 2025 yılında siber güvenlik ortamını hem saldırganlar hem de savunmacılar için dönüştürmektedir. Saldırganlar, YZ'yi ağları taramak, güvenlik açıklarını belirlemek ve saldırıları dakikalar içinde gerçekleştirmek için kullanmaktadır.[1] YZ destekli sızma testi botları, savunmaları analiz edebilir ve hassas saldırılar başlatabilir.[2] Bu durum, geleneksel host tarama yöntemlerinin YZ güdümlü botlara karşı daha az etkili olabileceği anlamına gelmektedir, çünkü bu botlar zayıflıkları akıllıca tanımlayabilir ve savunmaları atlatmak için tarama tekniklerini dinamik olarak ayarlayabilir.[2]

Bu teknoloji, saldırganların karmaşık saldırı vektörlerini otomatikleştirmesine, güvenlik açıklarını büyük ölçekte avlamasına ve siber saldırılar sırasında mesajlaşmayı dinamik olarak uyarlamasına olanak tanımaktadır.[3] YZ destekli sıfır gün avlama araçları, daha az deneyimli saldırganlar için bile istismarları erişilebilir kılabilir, bu da genel tehdit seviyesini artırmaktadır.[3] Bu durum, savunma tarafında YZ destekli güvenlik çözümlerine yatırım yapma gerekliliğini ortaya koymaktadır. ScanMatrix gibi araçların, YZ tabanlı davranışsal analiz yeteneklerini entegre ederek normal ağ davranışının temelini oluşturması ve gizli keşif faaliyetlerini gösteren ince sapmaları işaretlemesi hayati önem taşımaktadır. Bu, güvenlik güvenilirlik derecelendirmesini daha incelikli bir tehdit değerlendirmesi sağlayarak artıracaktır.

2. Gizli ve Kaçınmacı Port Tarama Teknikleri

Gizli port tarama, hedef sistem tarafından tespit edilme olasılığını azaltırken açık

portları belirlemeye yardımcı olan kritik bir siber güvenlik tekniğidir.[4] Geleneksel TCP bağlantısının üç aşamalı el sıkışmasından kaçınan SYN taraması (-sS), bu alandaki popüler bir yöntemdir.[4] Tam bir bağlantı kurmadığı için daha az müdahalecidir ve hedef sistem tarafından fark edilme veya uyarıları tetikleme olasılığı daha düşüktür.[4] Bir diğer gelişmiş teknik olan Idle Scan (Zombie Scan olarak da bilinir), tarayıcının kimliğini başka bir hostun arkasına gizleyerek tarama yapmasına olanak tanır.[4] Bu, hedef sistemin IP ID dizisi artışını izleyerek bir portun açık olup olmadığını belirler.[4]

Bu tekniklerin önemi, saldırganların güvenlik duvarları ve Saldırı Tespit Sistemleri (IDS) gibi savunma mekanizmalarını atlatma çabalarından kaynaklanmaktadır.[5] Paketleri daha küçük parçalara bölmek (parçalama -f) veya sahte tarama trafiğini taklit IP'lerden göndermek (decoy tarama -D) gibi kaçınma teknikleri, tespit sistemlerinin gerçek aktiviteyi tespit etmesini zorlaştırmaktadır.[5] Bu durum, güvenlik sistemlerinin basit imza eşleşmelerine veya tam bağlantı kayıtlarına dayanmasının yetersiz kalmasına yol açmaktadır.[4] ScanMatrix'in, hem etik testler için bu gizli taramaları gerçekleştirebilmesi hem de kendi ağını izlerken bunları tespit edebilmesi gerekmektedir. Bu, ScanMatrix'in "gerçek zamanlı izleme ve uyarı sistemi"nin, davranışsal analiz ve makine öğrenimi modellerini kullanarak ağdaki anormallikleri ve gizli keşif girişimlerini belirlemesini gerektirmektedir.

3. Kapsamlı Saldırı Yüzeyi Yönetimi ve Sürekli Güvenlik Açığı Değerlendirmesi

2025'te siber güvenlik, periyodik güvenlik açığı taramalarından, bir kuruluşun tüm saldırı yüzeyinin sürekli ve kapsamlı yönetimine doğru bir kayma yaşamaktadır.[7] Bu kayma, bulut altyapılarının, Nesnelerin İnterneti (IoT) cihazlarının ve üçüncü taraf uygulamalarının artan kullanımıyla genişleyen saldırı yüzeyinden kaynaklanmaktadır.[3] Yanlış yapılandırmalar (örneğin, açık portlar, varsayılan kimlik bilgileri, segmentlere ayrılmamış ağlar, güncel olmayan yazılımlar ve yanlış yapılandırılmış güvenlik duvarları) "sessiz katiller" olarak tanımlanmakta ve çoğu zaman sıfır gün güvenlik açıkları olmamalarına rağmen kolayca istismar edilebilmektedir.[7]

Bu durum, geleneksel, periyodik güvenlik açığı taramalarının (yalnızca bilinen CVE'lere odaklanan) yetersiz kalmasına neden olmaktadır, çünkü bu taramalar yanlış yapılandırmaların dinamik doğasını ve yeni eklenen, yönetilmeyen varlıkları ("gölge IoT" cihazları gibi) gözden kaçırmaktadır.[9] Bu nedenle, sürekli ve bütünsel izleme ihtiyacı ortaya çıkmaktadır. Bulut Güvenlik Durumu Yönetimi (CSPM) araçları, bulut yapılandırmalarını en iyi uygulamalara ve uyumluluk standartlarına göre sürekli olarak izleyerek yanlış yapılandırmaları otomatik olarak tespit edip düzeltmektedir.[11] Benzer şekilde, IoT güvenlik denetimleri donanım, yazılım, iletişim protokolleri ve kullanıcı erişimini kapsamakta, davranışsal anomali tespiti de dahil olmak üzere kapsamlı bir

yaklaşım sunmaktadır.[9] Verizon'ın araştırmasına göre veri ihlallerinin %20'sinden fazlası yanlış yapılandırmalardan kaynaklanmaktadır ve CSPM gibi proaktif araçlar ihlalleri %60 oranında azaltabilmektedir.[11] ScanMatrix'in, mevcut port tarama ve CVE veritabanı özelliklerini sürekli varlık keşfi, bulut ve IoT için yanlış yapılandırma tespiti ve YZ destekli risk önceliklendirme ile entegre ederek bir "Saldırı Yüzeyi Yönetimi" platformuna dönüşmesi gerekmektedir. Bu, aracın güvenlik derecelendirme sisteminin, tespit edilen güvenlik açıklarına ek olarak, tüm saldırı yüzeyine dayalı daha doğru ve gerçek zamanlı bir duruş sağlamasına olanak tanıyacaktır.

4. Gelişmiş MAC Adresi Tespiti ve Cihaz Parmak İzi Çıkarma

MAC adresi tespiti ve cihaz parmak izi çıkarma teknikleri, ağ gizliliğini ve keşfini anlamak için hayati öneme sahiptir, çünkü temel anonimleştirme girişimleri (MAC adresi sahtekarlığı gibi) kullanıldığında bile cihazların tanımlanmasına ve izlenmesine olanak tanır.[16] MAC adresi sahtekarlığı, bir cihazın MAC adresini ağdaki başka bir cihazınkini taklit etmek üzere değiştirmesidir.[17] Bu, ağ erişim kısıtlamalarını aşmak veya yetkisiz erişim elde etmek için kullanılabilir.[17]

Gelişmiş tespit yöntemleri, yalnızca MAC adresi karşılaştırmalarının ötesine geçerek cihaz parmak izi verilerini kullanır.[19] Bu veriler, cihazın MAC adresini ve işletim sistemi, yazılım, cihaz modeli gibi bir veya daha fazla özelliğini içerir.[19] Pasif taramalar (normal trafikten veri toplama) ve aktif taramalar (bir yanıtı tetiklemek için mesaj gönderme) birleştirilerek bu parmak izi verileri oluşturulur ve güncellenir.[19] Bu, MAC adresi sahtekarlığının doğru bir şekilde belirlenmesine ve yazılım güncellemeleri gibi meşru değişikliklerden kaynaklanan yanlış pozitiflerin azaltılmasına yardımcı olur.[19] Güven skoru ve kullanım istatistikleri (eşzamanlı kullanım veya aynı ağda kullanım gibi) da tespitin doğruluğunu artırır.[19] ScanMatrix'in MAC adresi tespiti yeteneği, OUI (Organizationally Unique Identifier) tabanlı tanımlamanın ötesine geçerek, cihazın davranışsal özelliklerini (TCP/IP yığını farklılıkları, saat kayması, paket zamanlaması, Wi-Fi prob istekleri) analiz eden gelişmiş parmak izi tekniklerini içermelidir.[16] Bu, ScanMatrix'in ağdaki cihazları daha doğru bir şekilde tanımlamasını ve MAC adresi sahtekarlığı girişimlerini tespit etmesini sağlayacaktır.

5. Yeni Nesil Güvenlik Duvarı (NGFW) ve Web Uygulama Güvenlik Duvarı (WAF) Parmak İzi Çıkarma ve Atlatma

2025 yılında, Yeni Nesil Güvenlik Duvarları (NGFW'ler) ve Web Uygulama Güvenlik Duvarları (WAF'ler), Yapay Zeka (YZ) ve Makine Öğrenimi (ML) teknolojilerini kullanarak tehditleri tespit etme ve tanımlama yeteneklerini önemli ölçüde geliştirmektedir.[21] Bu teknolojiler, sıfır gün tehditlerinin hassas bir şekilde tespit edilmesini ve engellenmesini sağlamakta, trafik analizi ve anomali tespiti gibi kritik görevleri otomatikleştirmektedir.[21]

WAF'ler, SQL enjeksiyonu, siteler arası komut çalıştırma (XSS) ve DDoS saldırıları gibi uygulama katmanı tehditlerine karşı koruma sağlarken, YZ/ML entegrasyonu ile davranışsal analizi kullanarak normal site etkileşimleri için bir temel oluşturur.[22] Anormal davranışlar (örneğin, hızlı site etkileşimleri veya otomatik form gönderimleri) tespit edildiğinde, WAF şüpheli aktiviteyi işaretleyebilir veya bir CAPTCHA gibi bir doğrulama isteği gönderebilir.[23]

Saldırganlar, güvenlik duvarlarını atlatmak için HTTP parmak izi çıkarma gibi teknikleri kullanmaktadır.[25] Bu, HTTP sunucuları ve bunlarla ilişkili programlama dilleri, çerçeveler, proxy'ler ve WAF'ler hakkında bilgi toplamayı içerir.[25] HTTP yanıt başlıkları (Server, X-Powered-By gibi) veya özel başlıklar aracılığıyla teknoloji yığını ve yazılım sürümleri hakkında ipuçları elde edilebilir.[25] Bu bilgiler, bilinen güvenlik açıklarını veya yanlış yapılandırmaları ortaya çıkararak saldırı stratejilerini daha hedefli hale getirir.[25] ScanMatrix'in, hem NGFW/WAF varlığını ve yapılandırmasını tespit etmek için gelişmiş parmak izi çıkarma yeteneklerini (derin paket denetimi ve davranışsal analiz dahil) kullanması hem de bu güvenlik duvarlarını atlatmaya yönelik potansiyel zayıflıkları belirlemesi gerekmektedir.[23] Bu, ScanMatrix'in güvenlik duvarı tespit yeteneklerini güçlendirecek ve potansiyel atlatma vektörlerini proaktif olarak belirlemesine yardımcı olacaktır.

6. Tünelleme ve Protokol Manipülasyonu ile Güvenlik Duvarı Atlatma

Güvenlik duvarı atlatma teknikleri, saldırganların güvenlik duvarlarının ağ protokollerini uç nokta sistemlerinden farklı yorumlama ve işleme şekillerini istismar etmesini içermektedir.[27] Bu, güvenlik duvarlarının tam olarak incelemediği veya anlamadığı daha yüksek seviyeli protokollerden faydalanmayı, kötü niyetli içeriği meşru trafikte gizlemek için şifreleme ve gizleme yöntemlerini kullanmayı veya yasaklanmış trafiği izin verilen protokoller içinde kapsüllemeyi (tünelleme) içerebilir.[27]

HTTP/HTTPS tünelleme, verileri özel HTTP başlıklarında gizleyerek, URI parametrelerini kodlayarak veya POST gövdelerine tam protokol akışlarını kapsülleyerek yaygın olarak kullanılmaktadır.[27] Saldırganlar, meşru web trafiği desenlerini taklit ederek, geçerli kullanıcı aracıları kullanarak ve istekleri normal insan tarama davranışlarına uyacak şekilde zamanlayarak tespit edilmekten kaçınmaya çalışırlar.[27] ICMP tünelleme de bir başka etkili yöntemdir, çünkü ICMP yankı paketleri rastgele veriler içerebilir ve birçok güvenlik duvarı ICMP paket içeriklerini derinlemesine incelemez.[27] Bu teknikler, güvenlik duvarı kurallarının optimizasyonunu ve protokol uyumluluk kurallarının sıkı bir şekilde uygulanmasını gerektirmektedir.[27] ScanMatrix'in, bu tür tünelleme ve protokol manipülasyon tekniklerini tespit etme yeteneğini geliştirmesi gerekmektedir. Bu, derin paket denetimi, anormal trafik desenlerini belirlemek için YZ/ML kullanımı ve potansiyel

gizli kanalları ortaya çıkarmak için davranışsal analiz içermelidir.

7. Nesnelerin İnterneti (IoT) Cihaz Güvenlik Tarama ve Kimlik Doğrulama

2025 yılına kadar 30 milyardan fazla IoT cihazının ağlara bağlanması beklenirken, bu cihazlar geniş bir saldırı yüzeyi sunmaktadır.[9] IoT cihazları genellikle sınırlı kaynaklarla tasarlanır ve yerel güvenlik özelliklerinden yoksundur, bu da onları siber saldırılar için cazip hedefler haline getirir.[10] IoT kötü amaçlı yazılım saldırıları 2023'ten 2024'e %45 artış göstermiştir.[28] Etkili bir IoT güvenlik denetimi, donanım, yazılım, iletişim protokolleri, kullanıcı erişimi ve bulut bağlantılarını kapsayan kapsamlı bir taramayı içerir.[9]

Bu denetimler, açık portlar, zayıf veya varsayılan parolalar, güncel olmayan bellenim ve bilinen CVE'ler için otomatik tarama yapmayı içerir.[9] Ayrıca, cihazların en iyi güvenlik uygulamalarını (güçlü parolalar, şifreli iletişim, sınırlı erişim ayrıcalıkları) kullanıp kullanmadığını kontrol eden yapılandırma incelemelerini de içerir.[9] Görünürlük, IoT güvenliğinin temelidir; pasif keşifler (ağ trafiği analizi, DHCP/DNS/ARP günlükleri) ve makine öğrenimi tabanlı davranış imzaları kullanılarak dinamik varlık haritaları oluşturulur.[10] ScanMatrix'in, IoT cihazlarına yönelik özel güvenlik açığı tarama yeteneklerini (bellenim analizi, YZ destekli anomali tespiti, kimlik doğrulama kontrolleri) entegre etmesi gerekmektedir.[9] Bu, ScanMatrix'in IoT ekosistemindeki zayıflıkları proaktif olarak belirlemesini ve ağ güvenilirliğini artırmasını sağlayacaktır.

8. API Güvenlik Taraması ve Gölge API Keşfi

Mikro hizmetlerin ve web tabanlı arayüzlerin yaygınlaşmasıyla birlikte, API'ler (Uygulama Programlama Arayüzleri) sofistike saldırılar için birincil hedef haline gelmiştir.[24] API'ler, modern dijital hizmetlerin omurgasını oluşturmasına rağmen, genellikle kötü bir şekilde güvence altına alınmıştır ve SQL enjeksiyonu, XSS ve bozuk kimlik doğrulama gibi saldırılara karşı savunmasızdır.[24] Bulut dağıtımlarında bilinen bir güvenlik açığıdır.[3]

API güvenlik taraması, API uç noktalarını güvenlik açıkları için proaktif olarak test etmeyi içerirken, "gölge API keşfi", saldırganlar için arka kapı görevi görebilecek belgelenmemiş veya unutulmuş API'leri belirlemeye odaklanır.[29] Pynt ve Salt Security gibi özel API güvenlik çözümleri, gerçek dünya saldırı senaryolarını simüle etmek için YZ destekli, bağlama duyarlı Dinamik Uygulama Güvenlik Testi (DAST) kullanmaktadır.[29] Bu araçlar, manuel testlerin yerini alarak sürekli, CI/CD entegre taramalar sunar.[29] Ayrıca, tüm API'leri (gölge ve belgelenmemiş olanlar dahil) bulut ortamlarında otomatik olarak keşfeder ve sınıflandırır.[29] API'lerin birbirine bağlılığı nedeniyle, bir API'deki bir ihlal domino etkisi yaratabilir.[30] ScanMatrix'in, API keşfi, YZ destekli API güvenlik açığı

taraması ve API'ye özgü tehdit istihbaratı yeteneklerini genişletmesi gerekmektedir. Bu, ScanMatrix'in uygulama katmanındaki potansiyel saldırı vektörlerini belirlemesini ve ağın genel güvenlik duruşunu güçlendirmesini sağlayacaktır.

9. Tedarik Zinciri Güvenlik Açıkları ve Etkileri

2025 yılında, tedarik zinciri saldırıları, kuruluşlar için en yıkıcı tehditlerden biri olarak öne çıkmaktadır.[31] Siber suçlular, iyi savunulan hedeflere doğrudan saldırmak yerine, güvenilir üçüncü tarafların (yazılım satıcıları, BT sağlayıcıları veya donanım üreticileri gibi) daha zayıf güvenliklerini istismar ederek bir kuruluşa sızmaktadır.[31] Bu saldırılar, açık kaynak platformlara, üçüncü taraf satıcılara ve API'lere artan bağımlılık ile tedarik zincirindeki zayıf güvenlik uygulamaları nedeniyle artmaktadır.[32]

Tedarik zinciri saldırıları, tek bir tehlikeye atılmış satıcının yüzlerce veya binlerce aşağı akış müşterisini etkileyebilecek geniş kapsamlı sonuçlara yol açabilir.[31] 2025'te yürürlüğe giren yeni düzenlemeler, kuruluşları üçüncü taraf ihlallerinden doğrudan sorumlu tutmakta, bu da tedarik zincirinin güvence altına alınmamasının maliyetli para cezalarına ve itibar kaybına yol açabileceği anlamına gelmektedir.[31] Savunma stratejileri, tüm üçüncü taraf satıcıların ve yazılım bağımlılıklarının haritalandırılmasını, katı satıcı değerlendirmelerini, en az ayrıcalık erişimini ve sürekli izlemeyi içerir.[31] ScanMatrix'in, tedarik zinciri riskini değerlendirmek için dışarıdan taramalar, anketler ve doğrudan kanıtlar gibi çeşitli kaynaklardan gelen verileri birleştirmesi gerekmektedir.[3] Bu, ScanMatrix'in ağdaki üçüncü taraf bileşenlerinden kaynaklanan potansiyel güvenlik açıklarını belirlemesini ve sistem güvenilirliği değerlendirmesine tedarik zinciri riskini dahil etmesini sağlayacaktır.

10. Sıfır Gün (Zero-Day) İstismarları ve Gelişmiş Kalıcı Tehditler (APT'ler)

Sıfır gün istismarları, daha önce bilinmeyen güvenlik açıklarını hedef alan saldırılar olup, 2025'te ciddi aksaklıklar yaratmaya devam edecektir.[3] YZ'nin artan yetenekleri, tehdit aktörlerinin karmaşık saldırı vektörlerini otomatikleştirmesine ve güvenlik açıklarını büyük ölçekte avlamasına olanak tanımaktadır.[3] Üretken YZ (GenAI), sağlam arama yetenekleri sayesinde saldırganlar tarafından yeni sıfır günler ve yamalanmamış CVE'leri keşfetmek için kullanılacaktır.[3] Ulus devletler, hacktivistler ve Gelişmiş Kalıcı Tehdit (APT) grupları, kendi saldırıları için sıfır günleri kullanmaya veya istismarları karaborsada satmaya devam edecektir.[3]

Bu durum, daha az deneyimli saldırganlar için bile bu istismarları erişilebilir hale getirebilir ve genel tehdit seviyesini artırabilir.[3] Örneğin, 2025'in ilk çeyreğinde Ivanti Endpoint Manager Mobile (EPMM) gibi ürünlerde kimlik doğrulama atlatma ve kod enjeksiyonu güvenlik açıkları aktif olarak istismar edilmiştir.[33] Bu tür güvenlik açıkları,

uzaktan kimlik doğrulaması yapılmamış saldırganların cihazda rastgele kod çalıştırmasına olanak tanıyabilir.[34] Kuruluşların, tehdit aktörü faaliyetlerinin ve Taktik, Teknik ve Prosedürlerinin (TTP'ler) gerçek zamanlı izlenmesini uygulayarak ve güvenlik açığı ciddiyetine, yaşına, istismar edilebilirliğine ve iş etkisine göre risk senaryolarını önceliklendirerek proaktif savunma stratejileri geliştirmesi gerekmektedir.[3] ScanMatrix'in, YZ destekli güvenlik açığı avlama yeteneklerini entegre etmesi ve bilinen istismar edilen güvenlik açıkları kataloğunu (CISA'nınki gibi) sürekli olarak taraması gerekmektedir.[33] Bu, ScanMatrix'in potansiyel sıfır gün tehditlerini belirlemesine ve sistem güvenilirliği derecelendirmesine bu tür tehditlerin riskini dahil etmesine yardımcı olacaktır.

Sonuçlar ve Öneriler

2025 yılı için ağ güvenliği ortamı, YZ'nin hem saldırgan hem de savunma tarafında artan kullanımıyla birlikte dinamik ve karmaşık bir yapı sergilemektedir. Host tarama, güvenlik duvarı tespiti, MAC adresi belirleme ve güvenlik duvarı atlatma teknikleri alanındaki gelişmeler, ağ güvenliği araçlarının sürekli adaptasyonunu ve gelişimini zorunlu kılmaktadır.

ScanMatrix gibi bir ağ güvenliği aracı için bu trendlerden çıkarılabilecek temel sonuçlar ve öneriler şunlardır:

1. **Yapay Zeka Entegrasyonunun Derinleştirilmesi:** ScanMatrix, mevcut yeteneklerini YZ ve ML ile güçlendirmelidir. Bu, sadece açık port tarama ve sistem bilgisi toplama gibi mevcut özelliklerin etkinliğini artırmakla kalmayacak, aynı zamanda YZ destekli davranışsal analiz ile ağ trafiğindeki anormallikleri ve gizli keşif girişimlerini çok daha hassas bir şekilde tespit etmesini sağlayacaktır. YZ destekli güvenlik açığı avlama ve risk önceliklendirme, aracın proaktif tehdit tespit yeteneklerini önemli ölçüde geliştirecektir.
2. **Kapsamlı Saldırı Yüzeyi Yönetimine Geçiş:** ScanMatrix, geleneksel ağ taramasının ötesine geçerek kapsamlı bir saldırı yüzeyi yönetim platformuna dönüşmelidir. Bu, bulut ortamlarındaki yanlış yapılandırmaların (CSPM entegrasyonu), IoT cihazlarının güvenlik açıklarının ve gölge API'lerin sürekli keşfi ve değerlendirilmesini içermelidir. Aracın "düşük, orta, yüksek, kritik" güvenlik güvenilirliği derecelendirmesi, bu genişletilmiş saldırı yüzeyi değerlendirmesini yansıtacak şekilde geliştirilmelidir.
3. **Gelişmiş Tespit ve Kaçınma Mekanizmalarının Geliştirilmesi:** Güvenlik duvarı atlatma ve gizli tarama tekniklerinin evrimi göz önüne alındığında, ScanMatrix'in derin paket denetimi, protokol manipülasyonu tespiti ve davranışsal analiz yeteneklerini geliştirmesi kritik öneme sahiptir. Aynı zamanda, etik hackleme

senaryoları için gizli tarama tekniklerini (SYN, Idle, parçalama, decoy taramaları) simüle etme yeteneği, aracın test ve değerlendirme kabiliyetini artıracaktır.

4. **MAC Adresi Tespiti ve Parmak İzi Çıkarma Doğruluğunun Artırılması:** MAC adresi tespiti, yalnızca OUI tabanlı tanımlamanın ötesine geçerek cihaz parmak izi verilerini (TCP/IP yığını farklılıkları, saat kayması, Wi-Fi prob istekleri) ve MAC adresi kullanım istatistiklerini birleştirmelidir. Bu, MAC adresi sahtekarlığı gibi saldırıları daha doğru bir şekilde tespit etmeye ve yanlış pozitifleri azaltmaya yardımcı olacaktır.
5. **Gerçek Zamanlı İzleme ve Uyarı Sisteminin İyileştirilmesi:** ScanMatrix'in gerçek zamanlı izleme ve uyarı sistemi, YZ ve ML'den elde edilen derinlemesine analizlerle beslenmelidir. Bu, ağ trafiğindeki ince anormallikleri ve potansiyel tehditleri daha hızlı ve daha doğru bir şekilde belirlemesini sağlayacak, böylece kuruluşların proaktif bir şekilde yanıt vermesine olanak tanıyacaktır.

Bu trendlerin entegrasyonu ve sürekli geliştirilmesi, ScanMatrix'i 2025 ve sonrasında ağ güvenliği analizi için vazgeçilmez bir araç haline getirecektir.

Alıntılanan çalışmalar

1. Preparing For The AI-Generated Cyber Threats Of 2025, erişim tarihi Haziran 5, 2025, https://www.cyberdefensemagazine.com/preparing-for-the-ai-generated-cyber-threats-of-2025/
2. AI-Powered Cyber Threats in 2025: How Attackers Use Machine ..., erişim tarihi Haziran 5, 2025, https://abusix.com/blog/the-rise-of-ai-powered-cyber-threats-in-2025-how-attackers-are-weaponizing-machine-learning/
3. Most Likely and Damaging Cyber Threats and Vulnerabilities in ..., erişim tarihi Haziran 5, 2025, https://safe.security/resources/blog/most-likely-damaging-cyber-threats-vulnerabilities-2025/
4. Perform Stealth Network Scanning with Nmap - LabEx, erişim tarihi Haziran 5, 2025, https://labex.io/tutorials/nmap-perform-stealth-network-scanning-with-nmap-415933
5. Recon #4: Port scanning and revealing hidden services - YesWeHack, erişim tarihi Haziran 5, 2025, https://www.yeswehack.com/learn-bug-bounty/recon-port-scanning-attack-vectors
6. Advanced NMAP Scanning Techniques: Technical Deep-Dive for Security Professionals, erişim tarihi Haziran 5, 2025, https://securedebug.com/advanced-nmap-scanning-techiques-network-scan/
7. Widespread Network Misconfigurations in 2025 Highlight Urgent Need for

Network VAPT, erişim tarihi Haziran 5, 2025, https://northeast.newschannelnebraska.com/story/52823555/widespread-network-misconfigurations-in-2025-highlight-urgent-need-for-network-vapt
8. The Rising Tide of Supply Chain Cybersecurity Risks in 2025 - Blog - Daily Security Review, erişim tarihi Haziran 5, 2025, https://dailysecurityreview.com/blog/the-rising-tide-of-supply-chain-cybersecurity-risks-in-2025/
9. Complete Guide to Performing an IoT Security Audit in 2025 - Qualysec, erişim tarihi Haziran 5, 2025, https://qualysec.com/complete-guide-to-performing-an-iot-security-audit/
10. Best Practices to Secure IoT Devices in 2025 - Sattrix, erişim tarihi Haziran 5, 2025, https://www.sattrix.com/blog/iot-security-best-practices-2025/
11. Cloud Security Posture Management: 7 Powerful Steps 2025, erişim tarihi Haziran 5, 2025, https://kraftbusiness.com/blog/cloud-security-posture-management/
12. The Best Tools for Cloud Security Posture Management (CSPM) in 2025: Enhance Compliance, Visibility, and Risk Mitigation - CloudNuro.ai, erişim tarihi Haziran 5, 2025, https://www.cloudnuro.ai/blog/the-best-tools-for-cloud-security-posture-management-cspm-in-2025-enhance-compliance-visibility-and-risk-mitigation
13. 9 Best CSPM Tools in 2025 - Wiz, erişim tarihi Haziran 5, 2025, https://www.wiz.io/academy/cspm-solutions-landscape
14. Top 5 CSPM Tools To Strengthen Cloud Security In 2025 - AccuKnox, erişim tarihi Haziran 5, 2025, https://accuknox.com/blog/cspm-tools
15. 9 Open source cloud security tools for 2025 - Sysdig, erişim tarihi Haziran 5, 2025, https://sysdig.com/blog/9-open-source-cloud-security-tools/
16. Mastering Network Privacy: Change Your MAC Address to Stay ..., erişim tarihi Haziran 5, 2025, https://www.examcollection.com/blog/mastering-network-privacy-change-your-mac-address-to-stay-anonymous/
17. MAC Spoofing Is A Silent Threat: How To Detect & Prevent Now - VPN.com, erişim tarihi Haziran 5, 2025, https://www.vpn.com/guide/mac-spoofing/
18. MAC Spoofing Explained: How It Works, Risks, and Prevention Techniques - OnionLinux, erişim tarihi Haziran 5, 2025, https://onionlinux.com/mac-spoofing-explained-how-it-works-risks-and-prevention-techniques/
19. US20250112952A1 - Detection of mac spoofing - Google Patents, erişim tarihi Haziran 5, 2025, https://patents.google.com/patent/US20250112952A1/en
20. DevPF: Device identification through passive fingerprints in IoT - ResearchGate, erişim tarihi Haziran 5, 2025, https://www.researchgate.net/publication/381425458_DevPF_Device_identification_through_passive_fingerprints_in_IoT
21. Top 5 NGFW solutions for 2025 | Nomios Group, erişim tarihi Haziran 5, 2025, https://www.nomios.com/news-blog/top-5-solutions-ngfw-2025/
22. Best 12 Web Application Firewall Software In 2025 - IO River, erişim tarihi Haziran 5, 2025, https://www.ioriver.io/blog/best-web-application-firewall-software

23. NGFW vs. WAF: How They Can Work Together - Check Point Software, erişim tarihi Haziran 5, 2025, https://www.checkpoint.com/cyber-hub/cloud-security/what-is-web-application-firewall/ngfw-vs-waf/
24. What Is a Web Application Firewall (WAF) and Why You Need One in 2025 - Atrity, erişim tarihi Haziran 5, 2025, https://www.atrity.com/what-is-a-web-application-firewall-waf-and-why-you-need-one-in-2025/
25. Recon series #3: HTTP fingerprinting – sleuthing for a web application's hidden vulnerabilities - YesWeHack, erişim tarihi Haziran 5, 2025, https://www.yeswehack.com/learn-bug-bounty/recon-series-http-fingerprinting
26. Enterprise Network Detection and Response Best Practices | Fidelis Security, erişim tarihi Haziran 5, 2025, https://fidelissecurity.com/threatgeek/network-security/enterprise-network-detection-and-response-best-practices/
27. Firewall Bypass Techniques and Mitigation Strategies: Technical Deep-Dive - Secure Debug, erişim tarihi Haziran 5, 2025, https://securedebug.com/firewall-bypass-techniques-secure-debug-limited/
28. Defend Your IoT with Device Hardening Tactics for a Secure 2025 - Asimily, erişim tarihi Haziran 5, 2025, https://asimily.com/blog/defend-your-iot-with-device-hardening-tactics-for-a-secure-2025/
29. 10 Vulnerability Scanning Tools to Know in 2025 - Pynt, erişim tarihi Haziran 5, 2025, https://www.pynt.io/learning-hub/application-security/10-vulnerability-scanning-tools-to-know-in-2025
30. Top 10 API Security Tools in 2025 - Jit.io, erişim tarihi Haziran 5, 2025, https://www.jit.io/resources/appsec-tools/top-10-api-security-tools
31. The Surge of Supply Chain Attacks - AgileBlue, erişim tarihi Haziran 5, 2025, https://agileblue.com/the-surge-of-supply-chain-attacks/
32. 10 common cybersecurity threats and attacks: 2025 update ..., erişim tarihi Haziran 5, 2025, https://www.connectwise.com/blog/common-threats-and-attacks
33. CISA Adds Six Known Exploited Vulnerabilities to Catalog, erişim tarihi Haziran 5, 2025, https://www.cisa.gov/news-events/alerts/2025/05/19/cisa-adds-six-known-exploited-vulnerabilities-catalog
34. Vulnerability Summary for the Week of May 5, 2025 | CISA, erişim tarihi Haziran 5, 2025, https://www.cisa.gov/news-events/bulletins/sb25-132