ScanMatrix 2025: Yeni Nesil Ağ Tarama ve Güvenlik Açığı Analizi için Stratejik İyileştirmeler

I. Yönetici Özeti

2025 yılı siber güvenlik ortamı, yapay zeka destekli, giderek karmaşıklaşan tehditler, bulut, konteynerler, Nesnelerin İnterneti (IoT), Operasyonel Teknoloji (OT) ve API'leri kapsayan genişleyen saldırı yüzeyleri ile karakterize edilmektedir. Bu ortamda, proaktif ve otomatikleştirilmiş savunmalara duyulan ihtiyaç kritik bir seviyeye ulaşmıştır. ScanMatrix'in, geleneksel bir ağ tarama aracından, bu karmaşık güvenlik zorluklarını etkin bir şekilde ele alabilen akıllı, entegre ve uyarlanabilir bir güvenlik açığı analizi platformuna dönüşmesi gerekmektedir.

Bu rapor, ScanMatrix'in liderliğini sürdürmesi ve 2025'in karmaşık güvenlik zorluklarını etkin bir şekilde ele alması için hayati önem taşıyan en etkili 10 dönüştürücü teknik ve eğilimi belirlemektedir. Bu iyileştirmeler, yapay zekadan yararlanmaya, modern altyapılarla uyumluluğu genişletmeye, otomatik yanıtı etkinleştirmeye ve daha derin, daha eyleme dönüştürülebilir güvenlik bilgileri sağlamaya odaklanmaktadır.

Başlıca bulgular ve öneriler şunlardır: Yapay zeka ve makine öğreniminin (örneğin MoEVD, FocusVul) güvenlik açığı tespitine entegrasyonu, doğruluğu önemli ölçüde artıracak, yanlış pozitifleri azaltacak ve yeni güvenlik açıklarını belirleyecektir. Gelişmiş gizli tarama ve kapsamlı IPv6 yetenekleri, gelişen ağ ortamlarında kapsamlı ve tespit edilemez keşif için hayati öneme sahiptir. Buluta özgü ve konteynerli ekosistemlerle sorunsuz entegrasyon, modern güvenlik duruşu yönetimi için vazgeçilmezdir. Derin SIEM ve SOAR entegrasyonları, ScanMatrix'i yalnızca bir tespit aracından, otomatikleştirilmiş olay yanıtı ve güvenlik açığı giderme iş akışlarının kritik bir bileşenine dönüştürecektir. Proaktif API güvenlik testi ve Yazılım Malzeme Listesi (SBOM) odaklı tedarik zinciri analizi, ortaya çıkan saldırı vektörlerini ve kritik uyumluluk gereksinimlerini ele alacaktır. Sürekli performans optimizasyonu ve gelişmiş otomasyon (DevSecOps entegrasyonu dahil), ScanMatrix'in verimli bir şekilde ölçeklenmesini ve

sürekli, gerçek zamanlı güvenlik bilgileri sağlamasını sağlayacaktır.

II. Giriş: 2025 Siber Güvenlik Ortamında Gezinme

2025 yılı, siber güvenlikte kritik bir dönüm noktasına işaret etmektedir. Tehdit aktörleri, giderek daha sofistike ve hedefli saldırılar başlatmak için yapay zeka da dahil olmak üzere gelişmiş tekniklerden yararlanmaktadır.[1] Bu durum, saldırı yüzeyinin geleneksel BT ağlarının ötesine geçerek, giderek dijitalleşen operasyonel teknoloji (OT) ortamlarını, Nesnelerin İnterneti (IoT) ve Tıbbi Nesnelerin İnterneti (IoMT) cihazlarını da kapsayacak şekilde dramatik bir şekilde genişlemesine yol açmıştır. Bu cihazların çoğu doğası gereği güvensizdir ve bulut bağlantılıdır.[2]

Güvenlik açıkları artık sadece geleneksel uygulamalarla sınırlı kalmamakta, API'lerde (2024'te CISA Bilinen İstismar Edilen Güvenlik Açığı (KEV) kataloğundaki güvenlik açıklarının %50'sinden fazlası API ile ilgiliydi [5]) ve yazılım tedarik zincirinde yaygın olarak bulunmaktadır.[3] Bu güvenlik açıkları, önemli finansal kayıplara ve kritik altyapılarda potansiyel fiziksel zararlara yol açma potansiyeli taşımaktadır.[2] 2024'ten 2025'e kadar ortalama cihaz riskinde %15'lik bir artış gözlemlenmiş olup, bu durum tüm sektörleri etkileyen küresel bir tehdit ortamının tırmandığını göstermektedir.[4]

Geleneksel, reaktif güvenlik önlemleri, bu hızla gelişen ve sinsi tehditlere karşı yetersiz kalmaktadır.[7] Kuruluşlar, güvenlik açıklarını erken tespit edebilen, riskleri etkin bir şekilde önceliklendirebilen ve mevcut güvenlik operasyonları ve geliştirme iş akışlarıyla sorunsuz bir şekilde entegre olabilen akıllı, otomatik ve kapsamlı çözümlere acilen ihtiyaç duymaktadır.[5] ScanMatrix, temel bir ağ tarama ve güvenlik açığı analizi aracı olarak, en son teknikleri ve eğilimleri stratejik olarak benimseyerek bu acil ihtiyaçları karşılamak için benzersiz bir konumdadır.

Siber güvenlik tehditlerinin giderek karmaşıklaşması ve saldırı yüzeylerinin genişlemesi, ScanMatrix gibi araçların geleneksel yaklaşımlarının ötesine geçerek bütünsel bir çözüm sunmasını zorunlu kılmaktadır. Geleneksel ağ tarama ve güvenlik açığı analizi araçlarının artık izole çalışamayacağı, bunun yerine birleşik bir platforma dönüşmesi gerektiği açıktır. Bu dönüşüm, basit port taramasının ötesine geçerek bağlı cihazların (IoT, IoMT), uygulamaların (API'ler) ve yazılım bileşenlerinin (SBOM'lar) bağlamını anlamayı içermektedir.[1]

III. ScanMatrix için 2025'in En İyi 10 Dönüştürücü Teknik ve Eğilimi

Bu bölüm, belirlenen en iyi 10 teknik ve eğilimi ayrıntılı olarak ele almakta, her biri için kısa bir başlık, açıklama, stratejik önem, 2025'teki potansiyel etkileri, uygulama alanları ve ilgili kaynakları sunmaktadır.

Tablo 1: ScanMatrix 2025 İyileştirme Teknikleri/Eğilimlerine Genel Bakış

Teknik/Eğilim	Kısa Açıklama	ScanMatrix için Temel Fayda	Birincil Uygulama Alanı	İlgili Kaynak (Snippet ID'leri)
1. Yapay Zeka Destekli Bağlamsal Güvenlik Açığı Tespiti	Yapay zeka ve makine öğrenimi modelleriyle güvenlik açıklarını yüksek doğruluk ve bağlamla belirleme.	Yanlış pozitifleri azaltır, yeni ve karmaşık güvenlik açıklarını tespit eder.	Ağ cihazları, web uygulamaları, bulut yapılandırmaları, kod analizi.	11
2. Gelişmiş Gizli Ağ Taraması ve Kaçınma Teknikleri	Ağ keşfi ve güvenlik açığı tespitini hedef güvenlik sistemleri tarafından algılanmadan gerçekleştirme.	Kapsamlı ve gizli denetimler sağlar, gerçek saldırı yüzeyini ortaya çıkarır.	Sızma testleri, kırmızı takım tatbikatları, dahili ağ denetimleri.	15
3. Kapsamlı Buluta Özgü ve Konteyner Güvenliği Entegrasyonu	Bulut tabanlı uygulamalar, konteynerler ve sunucusuz işlevler için güvenlik açığı analizi yeteneklerini genişletme.	Bulut ve konteyner ortamlarında derin görünürlük ve sürekli koruma sağlar.	CI/CD boru hatları, çalışma zamanı ortamları, bulut yapılandırmaları.	17
4. Gerçek Zamanlı Tehdit İstihbaratı ile	ScanMatrix bulgularını SIEM platformlarına	ScanMatrix'i SOC için kritik bir veri	Güvenlik Operasyon Merkezleri	19

Derin SIEM Entegrasyonu	sorunsuz bir şekilde besleyerek tehdit tespiti ve olay yanıtını hızlandırma.	kaynağına dönüştürür, uyumluluk raporlamasını geliştirir.	(SOC), olay müdahale ekipleri, uyumluluk denetimleri.	
5. SOAR Entegrasyonu ile Otomatik Güvenlik Açığı Giderme	Güvenlik açıklarının tespitinden sonra otomatikleştirilm iş yanıt iş akışlarını tetiklemek için SOAR platformlarıyla entegrasyon.	Ortalama Tespit Süresini (MTTD) ve Ortalama Yanıt Süresini (MTTR) önemli ölçüde azaltır.	Güvenlik operasyonları, yama yönetimi, olay yönetimi.	10
6. Anomali Tespiti için Davranışsal Analiz (UEBA)	Kullanıcılar, cihazlar, uygulamalar ve ağlar için "normal" aktivite taban çizgileri oluşturarak anormallikleri tespit etme.	Statik kuralları atlayan tehditleri (örneğin içeriden gelen tehditler) proaktif olarak belirler.	Ağ trafiği izleme, log analizi, cihaz etkileşimleri.	7
7. Proaktif API Güvenlik Testi ve Yapay Zeka Ağ Geçidi Farkındalığı	API'leri yaygın zayıflıklara karşı test etme ve yapay zeka ajanları ile yapay zeka ağ geçitlerinin getirdiği yeni zorlukları ele alma.	API saldırı yüzeyini kapsar, yapay zeka entegrasyonların ın güvenliğini sağlar.	API geliştirme, yapay zeka entegrasyonları, bulut tabanlı hizmetler.	5
8. Tedarik Zinciri Güvenlik Açığı Yönetimi için Yazılım Malzeme Listesi (SBOM)	Yazılım ürünlerindeki bileşenlerin envanterini çıkararak tedarik zinciri güvenlik açıklarını	Yazılım bileşenlerindeki gizli güvenlik açıklarına görünürlük sağlar, uyumluluğu	Yazılım geliştirme yaşam döngüsü (SDLC), risk değerlendirmesi , olay yanıtı.	3

	yönetme.	destekler.		
9. Uyarlanabilir Tarama Metodolojileri ile Performans Optimizasyonu	Doğruluktan ödün vermeden tarama süreçlerinin verimliliğini ve hızını artırma.	Büyük ölçekli ağlarda kapsamlı taramaları hızlandırır, operasyonel etkiyi en aza indirir.	Ağ taraması, güvenlik açığı analizi, büyük veri işleme.	[8]
10. DevSecOps Entegrasyonu ile Otomatik Tarama ve Raporlama	Güvenlik testini CI/CD boru hatlarına ve DevOps iş akışlarına sorunsuz bir şekilde entegre etme.	Güvenlik açıklarının erken tespitini ve hızlı giderilmesini sağlar, güvenlik borcunu önler.	Yazılım geliştirme yaşam döngüsü (SDLC), CI/CD, DevOps, güvenlik operasyonları.	[5]

---

1. Yapay Zeka Destekli Bağlamsal Güvenlik Açığı Tespiti

Bu teknik, güvenlik açıklarını daha yüksek doğruluk ve bağlamla belirlemek için gelişmiş Yapay Zeka (AI) ve Makine Öğrenimi (ML) modellerinin kullanılmasını içerir. Mixture-of-Experts (MoEVD) gibi yaklaşımlar, uzmanlaşmış yapay zeka modellerinin, nadir olanlar da dahil olmak üzere farklı Ortak Zayıflık Numaralandırması (CWE) türlerini tespit etmesine olanak tanır ve "hepsi bir arada" yaklaşımlardan önemli ölçüde daha iyi performans gösterir.[12] FocusVul ise, dil modeli tabanlı tespiti, hassas, güvenlik açığıyla ilgili kod bağlamlarını seçmeyi öğrenerek daha da geliştirir; bu da performansı artırır ve hesaplama yükünü azaltır.[11]

ScanMatrix için bu yapay zeka yeteneklerinin entegrasyonu, aracın imza tabanlı tespitten akıllı, davranışsal analize geçmesini sağlayacak, yanlış pozitifleri önemli ölçüde azaltacak ve geleneksel yöntemlerin gözden kaçırdığı yeni veya karmaşık güvenlik açıklarını belirleyecektir.[9] Tehditlerin giderek daha sinsi ve yapay zeka destekli olduğu bir ortamda bu, aracın güncel kalması için kritik öneme sahiptir.[1]

2025 yılında ScanMatrix, farklı varlık türleri (örneğin, web uygulamaları, ağ cihazları, bulut yapılandırmaları) veya güvenlik açığı kategorileri için güvenlik açığı tespit motorunu uzmanlaştırmak amacıyla MoEVD'yi uygulayabilir, böylece genel F1 puanını

ve geri çağırmayı iyileştirebilir.[12] FocusVul, özellikle ağ taramaları sırasında keşfedilen uygulama bileşenlerindeki güvenlik açıklarını belirlemek için ScanMatrix'in yetenekleri dahilindeki kod analizine uygulanabilir.[13] Bu, daha hassas ve eyleme dönüştürülebilir güvenlik açığı raporlarına yol açacak ve giderme çabalarını hızlandıracaktır.[9] Yapay zekanın güvenlik açığı tespitindeki rolü, yalnızca mevcut yetenekleri artırmaktan ziyade, tespitin temel zekası haline gelmektedir. Bu, mevcut modellerin temel sınırlamalarının (uzun kod, çeşitli CWE'ler) üstesinden gelmek ve önemli performans artışları elde etmek için tasarlanmış belirli yapay zeka mimarileri aracılığıyla gerçekleşmektedir. Bu, mevcut tespiti hızlandırmaktan öte, daha önce zor veya imkansız olan güvenlik açıklarının (nadir CWE'ler, ince kod hataları) tespitini sağlamak ve yüksek düzeyde bağlamsal sonuçlar sunmak anlamına gelmektedir.

2. Gelişmiş Gizli Ağ Taraması ve Kaçınma Teknikleri

Bu eğilim, hedef güvenlik sistemleri tarafından algılanmayı en aza indirirken ağ keşfi ve güvenlik açığı tespiti yapmaya odaklanan teknikleri kapsar. Temel yöntemler arasında SYN gizli taramaları (tam el sıkışmayı önlemek için SYN ve RST gönderme [15]), Boşta Tarama (tarayıcının IP'sini maskelemek için bir "zombi" ana bilgisayar kullanma [15]), paket parçalama, MTU manipülasyonu, yem taraması (birden fazla kaynak IP'yi taklit etme), MAC adresi sahtekarlığı ve kaynak port manipülasyonu yer almaktadır.[16]

2025 yılında, sofistike saldırganlar gelişmiş kaçınma teknikleri kullanmakta, bu da geleneksel taramaları kolayca tespit edilebilir hale getirmektedir. ScanMatrix, uyarıları tetiklemeden kapsamlı denetimler gerçekleştirmek için sağlam gizli yetenekler sunmalı, böylece bir kuruluşun gerçek saldırı yüzeyinin ve potansiyel kör noktalarının daha doğru bir değerlendirmesini sağlamalıdır.[15]

ScanMatrix, bu gelişmiş Nmap esinli teknikleri bünyesine katarak güvenlik profesyonellerinin daha gizli ve kapsamlı sızma testleri yapmasına olanak tanıyabilir. Bu, özellikle kırmızı takım tatbikatları, mavi takımlar tarafından tespitin bir test hedefi olduğu dahili ağ denetimleri ve saldırı tespit sistemlerinin etkinliğini değerlendirmek için değerlidir. ScanMatrix, farklı operasyonel ihtiyaçlar için yapılandırılabilir gizli profiller sunabilir. Gizli tarama, artık yalnızca saldırganların kullandığı bir teknik olmaktan çıkıp, savunma stratejilerinin ayrılmaz bir parçası haline gelmiştir. Bir savunma aracı olan ScanMatrix için bu yetenekleri sunmak, kuruluşların "bir saldırgan gibi düşünmesini" ve açık taramalarla gözden kaçırılabilecek güvenlik açıklarını belirlemesini sağlar. Bu, kuruluşun kendi tespit sistemlerinin etkinliğini test etmek ve

gizli varlıkları veya yanlış yapılandırmaları ortaya çıkarmakla ilgilidir.

3. Kapsamlı Buluta Özgü ve Konteyner Güvenliği Entegrasyonu

Bu eğilim, buluta özgü uygulamaların, konteynerlerin (Docker, Kubernetes) ve sunucusuz işlevlerin dinamik ve geçici doğasına yönelik güvenlik açığı analizi yeteneklerinin genişletilmesini içerir. Bu, CI/CD boru hattı boyunca sürekli görüntü taraması, çalışma zamanı güvenlik izlemesi, yanlış yapılandırmaların tespiti (CSPM), gizli tarama ve DevOps araç zincirleriyle entegrasyonu kapsar.[17] Araçlar, uç nokta, bulut iş yükü ve tehdit istihbaratı için birleşik platformlara doğru ilerlemektedir.[17]

Kuruluşlar bulut ve konteynerli mimarileri hızla benimsedikçe, saldırı yüzeyi değişmektedir. ScanMatrix, koddan buluta kadar güvenlik açıklarını, Kubernetes kümeleri ve konteyner görüntüleri de dahil olmak üzere bu ortamlar arasında derin görünürlük ve sürekli koruma sağlamalıdır.[17] Aksi takdirde, ScanMatrix bir kuruluşun dijital varlıklarının önemli ve büyüyen bir kısmını gözden kaçıracaktır.

2025 yılında ScanMatrix, otomatik görüntü taraması gerçekleştirmek ve yalnızca güvenli konteynerlerin dağıtılmasını sağlamak için doğrudan CI/CD boru hatlarına (örneğin Jenkins, GitLab) entegre olabilir.[18] Canlı konteyner davranışını kötü amaçlı faaliyetler için izleyerek çalışma zamanı koruması sunabilir.[17] Ayrıca, bulut yanlış yapılandırmalarını tespit edebilir ve buluta özgü dağıtımlar için uyumluluk doğrulaması sağlayarak hibrit ve çoklu bulut ortamlarında birleşik bir güvenlik duruşu sunabilir.[17] Bulut güvenliğindeki "sola kaydırma" yaklaşımı, yalnızca kod analiziyle sınırlı kalmayıp, altyapıyı kod olarak (IaC) ve çalışma zamanı güvenliğini de kapsamaktadır. Bu, "sola kaydırma"nın geleneksel olarak kodda güvenlik açıklarını erken bulmak anlamına gelirken, buluta özgü ortamlar için dağıtımdan

önce Altyapı olarak Kod (IaC) şablonlarını ve çalışma zamanı *sırasında* sürekli izlemeyi de içerdiği anlamına gelir. "Kabul Denetleyicisi" konsepti [18], güvensiz dağıtımları önleyen bir "sağa kaydırma" uygulama mekanizmasıdır.

4. Gerçek Zamanlı Tehdit İstihbaratı ile Derin SIEM Entegrasyonu

Bu, ScanMatrix'in güvenlik açığı ve tarama verilerini, çeşitli kaynaklardan gelen

günlükleri toplayan, normalleştiren ve depolayan Güvenlik Bilgileri ve Olay Yönetimi (SIEM) platformlarına sorunsuz bir şekilde aktarmasını içerir.[19] Tehdit İstihbaratı Platformları (TIP'ler) ile birleştirildiğinde, SIEM'ler kural tabanlı korelasyon, davranışsal analiz ve güncel tehdit beslemelerini kullanarak potansiyel güvenlik tehditlerini belirler ve olay yanıtını hızlandırır.[19]

ScanMatrix için derin SIEM entegrasyonu, bulgularının izole kalmaması, aksine bütünsel bir güvenlik resminin parçası haline gelmesi anlamına gelir. Bu, ScanMatrix'i bağımsız bir araçtan, bir kuruluşun Güvenlik Operasyon Merkezi (SOC) için kritik bir veri kaynağına yükseltir; daha hızlı tehdit tespiti, bağlamsal olay soruşturması ve uyumluluk raporlaması sağlar.[19]

2025 yılında ScanMatrix, popüler SIEM çözümleri (örneğin Splunk, IBM QRadar, Microsoft Sentinel, Elastic Stack) için sağlam API'ler ve bağlayıcılar geliştirebilir.[22] SIEM'lerin diğer olay günlükleriyle ilişkilendirebileceği normalleştirilmiş, yüksek doğrulukta güvenlik açığı verileri sağlamalıdır.[19] TIP'lerle entegrasyon, ScanMatrix'in aktif istismarlara ve gerçek zamanlı tehdit ortamlarına göre güvenlik açıklarını önceliklendirmesine olanak tanıyarak çıktısını güvenlik ekipleri için daha eyleme dönüştürülebilir hale getirecektir.[20] SIEM entegrasyonu, güvenlik açığı verilerinin operasyonel hale getirilmesi için kritik bir kapı görevi görmektedir. ScanMatrix'in ham tarama çıktısı değerli olsa da, gerçek gücü bu verilerin daha geniş bir güvenlik ekosistemi içinde alınması, ilişkilendirilmesi ve üzerinde hareket edilmesiyle ortaya çıkar. SIEM, bunun için merkezi sinir sistemi görevi görür ve ham güvenlik açığı verilerini eyleme dönüştürülebilir güvenlik istihbaratına dönüştürür.

5. SOAR Entegrasyonu ile Otomatik Güvenlik Açığı Giderme

Güvenlik Orkestrasyonu, Otomasyon ve Yanıt (SOAR) platformları, çeşitli kaynaklardan (SIEM'ler dahil) gelen uyarıları alarak ve olayları insan müdahalesi olmadan araştırmak, önceliklendirmek ve genellikle çözmek için "oyun kitaplarını" tetikleyerek güvenlik iş akışlarını otomatikleştirir.[10] Bu, CVE'leri önceliklendirme, yamaları gönderme ve bilet oluşturma gibi güvenlik açığı giderme görevlerinin otomatikleştirilmesini içerir.[10]

Güvenlik uyarısı ve güvenlik açığı hacmi, insan ekipleri için bunaltıcıdır.[10] SOAR ile entegre olarak, ScanMatrix yalnızca güvenlik açıklarını belirlemenin ötesine geçerek, bunların giderilmesini aktif olarak başlatabilir, Ortalama Tespit Süresini (MTTD) ve Ortalama Yanıt Süresini (MTTR) önemli ölçüde azaltabilir.[10] Bu, ScanMatrix'i yalnızca bir

tespit aracından ziyade proaktif bir savunma mekanizmasına dönüştürür.

2025 yılında ScanMatrix, tespit edilen güvenlik açıklarını ve kritikliklerini doğrudan bir SOAR platformuna besleyebilir. Oyun kitapları daha sonra BT hizmet yönetimi sistemlerinde giderme biletleri oluşturma, tespit edilen sistemler için yama dağıtımlarını başlatma veya tehlikeye atılmış varlıkları izole etme gibi eylemleri otomatik olarak tetikleyecek şekilde yapılandırılabilir.[10] Bu otomasyon, güvenlik analistlerinin daha karmaşık, stratejik tehditlere odaklanmasını sağlayacaktır. Otomasyon, güvenlik açığı tespiti ile giderilmesi arasındaki boşluğu kapatmanın anahtarıdır. ScanMatrix'in temel işlevi olan güvenlik açıklarını belirlemek, savaşın sadece yarısıdır. Gerçek değer, bunları hızlı bir şekilde düzeltmekten gelir. SOAR, bu eksik bağlantıyı sağlayarak tespiti otomatik eyleme dönüştürür; bu da modern tehditlerin ölçeği ve hızı göz önüne alındığında kritik öneme sahiptir.

6. Anomali Tespiti için Davranışsal Analiz (UEBA)

Kullanıcı ve Varlık Davranış Analizi (UEBA), kullanıcılar, cihazlar, uygulamalar ve ağlar için "normal" aktivite taban çizgileri oluşturmak amacıyla makine öğrenimini kullanır. Daha sonra bu taban çizgilerinden sapmaları sürekli olarak izleyerek, içeriden gelen tehditler, ele geçirilmiş hesaplar, kaba kuvvet saldırıları, veri sızdırma veya gelişmiş kalıcı tehditler (APT'ler) gibi anormallikleri işaretler.[7]

ScanMatrix geleneksel olarak ağ ve sistem güvenlik açıklarına odaklanırken, UEBA'nın entegrasyonu, bilinen güvenlik açıklarını içermeyen, ancak ağdaki anormal davranışları içeren tehditleri tespit etmesine olanak tanır. Bu, özellikle içeriden gelen tehditleri veya statik kuralları atlayan sinsi kimlik bilgisi kötüye kullanımlarını belirlemek için proaktif, bağlam açısından zengin bir güvenlik katmanı sağlar.[7]

2025 yılında ScanMatrix, taramalar sırasında toplanan ağ trafiğini, günlük verilerini ve cihaz etkileşimlerini analiz ederek UEBA yeteneklerini bünyesine katabilir. Ağ cihazları, hizmetler ve hatta taranan sistemlerde gözlemlenen belirli kullanıcı etkinlikleri için davranışsal profiller oluşturabilir. Tespit edilen anormallikler (örneğin, olağandışı port erişimi, bir cihazdan beklenmeyen veri transferleri veya anormal davranan bir hizmet), ScanMatrix'in raporlamasında yüksek öncelikli uyarıları tetikleyebilir veya daha fazla eylem için SIEM/SOAR'a beslenebilir.[7] Bu yaklaşım, yalnızca güvenlik açıklarını tespit etmekle kalmayıp, aynı zamanda bu açıklıkların istismar edilmekte olup olmadığını davranışsal analiz yoluyla belirlemeyi sağlamaktadır. ScanMatrix gibi bir araç, UEBA'yı

entegre ederek, bir sistemin yalnızca savunmasız olup olmadığını değil, aynı zamanda bilinen bir CVE olmasa bile şu anda istismar edilip edilmediğini veya kötü amaçlı faaliyetin meydana gelip gelmediğini de tespit edebilir. Bu, statik risk değerlendirmesinden dinamik tehdit tespitine doğru kritik bir kaymadır.

7. Proaktif API Güvenlik Testi ve Yapay Zeka Ağ Geçidi Farkındalığı

API güvenliği, API ile ilgili güvenlik açıklarının dramatik bir şekilde artmasıyla kritik bir endişe kaynağıdır.[5] Bu eğilim, "bozuk yetkilendirme" (OWASP API Güvenliği İlk 10) gibi yaygın zayıflıklara karşı API'lerin proaktif test edilmesini ve yapay zeka ajanları ile yapay zeka ağ geçitlerinin ortaya çıkardığı yeni zorlukların ele alınmasını vurgulamaktadır.[11] Yapay zeka ajanları, doğal dil komutları aracılığıyla API'leri kullanabilen yazılımlardır; yapay zeka ağ geçitleri ise trafiği Büyük Dil Modellerine (LLM'ler) yönlendirir ve istem enjeksiyonu koruması gibi güvenlik özelliklerini uygular.[11]

API'ler modern uygulamaların ve yapay zeka entegrasyonlarının omurgası haline geldikçe, önemli bir saldırı yüzeyini temsil etmektedirler. ScanMatrix, kapsamlı kapsama sağlamak için API'leri derinlemesine tarama ve analiz etme, benzersiz güvenlik açıklarını ve yapay zeka ajanlarının onlarla nasıl etkileşime girebileceğini anlama yeteneklerini genişletmelidir.[5]

2025 yılında ScanMatrix, OWASP API Güvenliği İlk 10 güvenlik açıkları için otomatik kontroller de dahil olmak üzere API keşfi ve testi için özel modüller geliştirebilir.[11] Yapay zeka sistemlerine maruz kalan API'lerde potansiyel kötüye kullanım veya istem enjeksiyonu güvenlik açıklarını belirlemek için yapay zeka ajanı etkileşimlerini simüle edebilir.[11] ScanMatrix ayrıca, ağ içindeki yapay zeka ağ geçitlerinin güvenlik duruşu hakkında bilgi sunarak, LLM entegrasyonlarını korumak için doğru şekilde yapılandırıldıklarından emin olabilir. API güvenliği, artık sadece web uygulamalarıyla ilgili olmaktan çıkıp, yapay zeka odaklı dijital ekonominin temel bir bileşeni haline gelmiştir. Geleneksel "web uygulaması istismarları"na odaklanma [5] genişlemektedir. API'ler, yapay zeka sistemleri için arayüz haline gelmekte ve istem enjeksiyonu gibi yeni saldırı vektörlerini ve "insan dışı kimlikleri" kontrol etme ihtiyacını ortaya çıkarmaktadır.[1]

8. Tedarik Zinciri Güvenlik Açığı Yönetimi için Yazılım Malzeme Listesi (SBOM)

Bir SBOM, bir yazılım ürünündeki bileşenlerin (ticari, açık kaynak, tescilli) resmi, makine tarafından okunabilir bir envanteridir.[6] 2025'te SBOM'lar, şeffaflığı artırmak ve yazılım tedarik zincirindeki güvenlik açıklarını azaltmak için hükümetler (örneğin, ABD Yürütme Emri 14028, AB CRA) tarafından zorunlu kılınan stratejik varlıklara dönüşmektedir.[3] Gömülü bileşenlere ve bilinen güvenlik açıklarına görünürlük sağlayarak risk değerlendirmesi, olay yanıtı ve yazılım varlık yönetimini etkinleştirirler.[6]

Yazılım tedarik zinciri saldırıları, açık kaynak, ticari yazılımları ve derleme boru hatlarını hedef alan büyüyen ve sofistike bir tehdittir.[3] ScanMatrix, SBOM analizini entegre ederek, taranan sistemlerde çalışan yazılım bileşenlerine görünürlük sağlayabilir, geleneksel ağ taramalarının gözden kaçırabileceği üçüncü taraf kitaplıklarında veya bağımlılıklarında gizlenmiş güvenlik açıklarını belirleyebilir.

2025 yılında ScanMatrix, geliştirme ekipleri veya üçüncü taraf araçlar tarafından oluşturulan SBOM'ları alabilir.[6] Daha sonra taranan cihazlardaki tanımlanmış yazılım sürümlerini genel veri tabanlarındaki (CVE'ler) bilinen güvenlik açıklarıyla ilişkilendirerek güvenlik açığı raporlarını tedarik zinciri bağlamıyla zenginleştirebilir.[3] Bu, kuruluşların mevcut bileşenlere ve bunlarla ilişkili risklere göre yamalamayı önceliklendirmesine olanak tanıyarak, ağ düzeyindeki güvenlik açıklarının ötesine geçerek daha derin yazılım bileşimi analizine geçişi sağlar. SBOM'lar, güvenlik açığı yönetimini reaktif bir süreçten proaktif ve daha ayrıntılı bir yaklaşıma dönüştürmektedir. Geleneksel güvenlik açığı taraması genellikle uygulama veya işletim sistemi düzeyinde güvenlik açıklarını belirler. SBOM'lar, bir güvenlik açığının

neden var olduğuna dair ayrıntılı bir görünüm (örneğin, belirli bir savunmasız kitaplık) sağlar ve dağıtımdan önce veya halihazırda kullanımda olan bir bileşende yeni bir güvenlik açığı keşfedilirse bile risklerin proaktif olarak belirlenmesine olanak tanır. Bu, yalnızca bir güvenlik açığını tespit etmekten öte, kökenini ve bir kuruluşun yazılım varlıkları üzerindeki daha geniş etkisini anlamaya odaklanmayı sağlar.

9. Uyarlanabilir Tarama Metodolojileri ile Performans Optimizasyonu

Bu eğilim, doğruluktan ödün vermeden tarama süreçlerinin verimliliğini ve hızını artırmaya odaklanmaktadır. Ağ taramaları için uyarlanabilir zamanlama şablonlarını, hız sınırlamasını ve akıllı paket oluşturmayı [16], ayrıca güvenlik açığı tespitinde FLOP'ları

azaltma [13] ve kaynakları korumak için görevleri otomatikleştirme [24] gibi yapay zeka/makine öğrenimi odaklı optimizasyonları içerir. Amaç, operasyonel istikrarı tehlikeye atmadan büyük ölçekli ağları ve karmaşık veri hacimlerini yönetmektir.[16]

Modern ağlar geniş ve dinamiktir, genellikle bulut ortamlarını ve binlerce cihazı içerir. ScanMatrix, kabul edilebilir zaman dilimlerinde kapsamlı taramalar yapmak, ağ etkisini en aza indirmek ve gerçek zamanlı bilgiler sağlamak için yüksek performanslı olmalıdır.[16] Sürekli izleme ve hızlı yanıt için verimlilik kritik öneme sahiptir.

2025 yılında ScanMatrix, ağ koşullarına veya hedef hassasiyetine göre tarama yoğunluğunu dinamik olarak ayarlayan uyarlanabilir tarama profilleri uygulayabilir.[16] Daha hızlı sonuçlar için tarama hedeflerini önceliklendirmek ve paket iletimini optimize etmek için yapay zekadan yararlanabilir.[13] Güvenlik açığı analizi için, performans optimize edilmiş yapay zeka modellerinin (FocusVul gibi) entegrasyonu, ScanMatrix'in büyük kod tabanlarını veya yapılandırma dosyalarını daha verimli bir şekilde işlemesine olanak tanıyacak, tarama sürelerini ve kaynak tüketimini azaltacaktır.[13] Bu, ScanMatrix'in kurumsal ortamlar için ölçeklenebilir kalmasını sağlar. Performans, artık sadece tarama hızıyla ilgili olmayıp, sürdürülebilir ve ölçeklenebilir bir güvenlik duruşu sağlamakla ilgilidir. 2025'teki performans, tek bir taramanın ne kadar hızlı çalıştığıyla değil, güvenlik sürecinin genel verimliliğiyle ilgilidir. Bu, hesaplama maliyetini, ağ etkisini ve insan kaynakları tahsisini içerir. Veri hacimleri büyüdükçe ölçeklenebilirlik çok önemlidir.

10. DevSecOps Entegrasyonu ile Otomatik Tarama ve Raporlama

Bu eğilim, güvenlik testini Sürekli Entegrasyon/Sürekli Teslimat (CI/CD) boru hattına ve DevOps iş akışlarına sorunsuz bir şekilde entegre etmeyi, güvenliği "sola" (geliştirmenin erken aşamaları) ve "sağa" (üretimde sürekli izleme) kaydırmayı vurgular.[5] Otomatik güvenlik açığı taramasını, geliştiricilere gerçek zamanlı geri bildirimi ve eyleme dönüştürülebilir, özelleştirilebilir raporlar oluşturmayı içerir.[5]

Manuel güvenlik testi, çevik geliştirme döngülerine ayak uyduramaz.[9] ScanMatrix, tarama süreçlerini otomatikleştirmeli ve geliştirici iş akışlarına doğrudan entegre olmalı, hızlı geri bildirim sağlamalı, Ortalama Giderme Süresini (MTTR) azaltmalı ve güvenlik borcunun birikmesini önlemelidir.[5] Bu, "tasarımla güvenlik" kültürünü teşvik eder.

2025 yılında ScanMatrix, kod taahhütleri veya derleme tamamlamaları üzerine otomatik taramaları tetiklemek için popüler CI/CD araçlarıyla (örneğin Jenkins, GitLab, Azure DevOps) önceden oluşturulmuş entegrasyonlar sunabilir.[18] Geliştiricilere Entegre Geliştirme Ortamlarında (IDE'ler) veya pull request iş akışlarında gerçek zamanlı, bağlamsal geri bildirim sağlayabilir.[5] Otomatik, özelleştirilebilir raporlama özellikleri, ekiplerin gelişmiş panolar ve görselleştirmelerle güvenlik açıklarını, uyumluluğu ve güvenlik duruşunu zaman içinde izlemesine olanak tanıyacaktır.[9] Bu aynı zamanda, bu otomatik süreçleri şeffaf ve yönetilebilir kılan gelişmiş GUI özelliklerinin potansiyelini de içerir. Güvenlik, artık tek bir kontrol noktası değil, sürekli bir süreçtir. Geleneksel güvenlik modelinin, ayrı, geç aşama bir kapı olarak işlev görmesi artık geçerliliğini yitirmiştir. Güvenlik, ilk kod taahhüdünden üretim izlemesine kadar tüm yazılım geliştirme ve dağıtım yaşam döngüsü boyunca yerleşik olmalıdır. Otomasyon, bu sürekli geri bildirim döngüsünün etkinleştiricisidir.

IV. ScanMatrix Ürün Yol Haritası için Stratejik Öneriler

Belirlenen eğilimlerin ScanMatrix'in geliştirilmesine entegrasyonu için eyleme dönüştürülebilir öneriler, ScanMatrix'in pazardaki konumunu güçlendirmek için kritik öneme sahiptir.

- **Yapay Zeka Odaklı Geliştirmeye Öncelik Verin:** MoEVD ve FocusVul gibi yapay zeka/makine öğrenimi modelleri için Ar-Ge'ye yoğun yatırım yapılmalıdır. Bu, OWASP'ın 2025 veri toplama planından yararlanarak eğitim verilerine [26] ve model açıklanabilirliğine odaklanmayı içerir.
- **Altyapı Bağımsızlığını Genişletin:** ScanMatrix'in yeteneklerinin şirket içi, IPv6 ağları ve tüm büyük bulut sağlayıcıları (AWS, Azure, GCP) arasında eşit derecede sağlam olduğundan, konteyner ve sunucusuz ortamlar için özel modüllerle birlikte emin olunmalıdır.
- **Ekosistem Entegrasyonunu Benimseyin:** Önde gelen SIEM, SOAR ve DevSecOps platformlarıyla sorunsuz entegrasyon için sağlam, iyi belgelenmiş API'ler geliştirilmelidir. Veri alışverişi için endüstri standartlarına (örneğin, SIEM için IDMEF [19]) katılım sağlanmalıdır.
- **Gizli ve Kaçınma Karşı Önlemlerini Geliştirin:** Gelişmiş gizli tarama teknikleri uygulanmalı ve sürekli güncellenmeli, kullanıcıların sofistike saldırgan keşiflerini simüle etmesine olanak tanınmalıdır.
- **Eyleme Dönüştürülebilir İstihbarata Odaklanın:** Raporlama, ham güvenlik açığı

listelerinden, potansiyel etki, giderme adımları ve otomatik giderme iş akışlarıyla entegrasyon dahil olmak üzere önceliklendirilmiş, bağlam açısından zengin bilgilere kaydırılmalıdır.

Kullanılabilirlik ve otomatik, akıllı raporlama için GUI iyileştirmelerine özel önem verilmelidir. Yeniden tasarlanmış, gelişmiş bir GUI, tüm taranan ortamlarda (ağ, bulut, konteynerler, API'ler) güvenlik duruşuna ilişkin net, eyleme dönüştürülebilir bilgiler sağlamalı, eğilim analizi ve risk önceliklendirmesi için görselleştirmelerden yararlanmalıdır.[9] Kullanıcıların farklı paydaşlara (teknik ekipler, yönetim, uyumluluk görevlileri) özel olarak uyarlanmış otomatik raporlar oluşturmasına izin verilmelidir; bu raporlar temel metrikleri, uyumluluk durumunu ve giderme ilerlemesini vurgulamalıdır.[8] Gerçek zamanlı uyarılar ve geri bildirim, geliştirici ve operasyon iş akışlarına doğrudan entegre edilerek, güvenlik açıklarının tespit edildiği anda anlaşılmasını ve üzerinde hareket edilmesini kolaylaştırmalıdır.[5] Gelişmiş bir grafik kullanıcı arayüzü (GUI), karmaşık veriler ile eyleme dönüştürülebilir güvenlik arasındaki köprüyü oluşturmaktadır. Güçlü bir arka uç (yapay zeka, entegrasyonlar) etkili bir ön uç olmadan kullanışsızdır. ScanMatrix için gelişmiş bir GUI, sadece estetikle ilgili değildir; karmaşık teknik verileri çeşitli kullanıcılar (geliştiriciler, SOC analistleri, yönetim) için açık, eyleme dönüştürülebilir istihbarata dönüştürmekle ilgilidir. Verimli önceliklendirme ve yanıtı etkinleştirir.

Sürekli bir inovasyon döngüsünü teşvik etmeye yönelik bir tartışma da gereklidir. ScanMatrix'in geliştirme yol haritası, ortaya çıkan tehditlere ve teknolojilere karşı çevik ve duyarlı olmalıdır. Bu, yeni saldırı vektörlerine (örneğin, yapay zeka deepfake'leri [1]) sürekli araştırma, siber güvenlik topluluklarına (örneğin, OWASP [26]) katılım ve hızlı özellik yinelemeye bağlılık gerektirir.

Tablo 2: ScanMatrix Özellik Entegrasyonu ve Etki Matrisi

ScanMatrix Fonksiyonel Alanı	Önerilen İyileştirme (Özel Özellik/Yetenek)	Uyumlu Eğilim (İlk 10'dan)	Beklenen Stratejik Etki	Geliştirme Önceliği
Ağ Taraması	IPv6 için Gelişmiş Paket Oluşturma ve Dinamik Zamanlama	2. Gelişmiş Gizli Ağ Taraması & Evasion Teknikleri; 9. Performans Optimizasyonu	Kapsamlı IPv6 kapsama, ağ etkisinin azaltılması, daha hızlı keşif.	Yüksek

Güvenlik Açığı Tespiti	MoEVD ve FocusVul Tabanlı AI Motoru	1. Yapay Zeka Destekli Bağlamsal Güvenlik Açığı Tespiti	Yanlış pozitiflerde önemli azalma, nadir CWE'lerin tespiti, daha derin kod analizi.	Yüksek
Bulut Güvenliği	Konteyner Görüntüsü ve Çalışma Zamanı Taraması, CSPM	3. Kapsamlı Buluta Özgü & Konteyner Güvenliği Entegrasyonu	Bulut iş yüklerinde uçtan uca koruma, yanlış yapılandırma tespiti, DevSecOps entegrasyonu.	Yüksek
Raporlama ve Analiz	SIEM/SOAR ile Otomatik Veri Besleme ve Önceliklendirme	4. Derin SIEM Entegrasyonu; 5. Otomatik Güvenlik Açığı Giderme	Merkezi güvenlik görünürlüğü, otomatik olay yanıtı başlatma, MTTR azaltma.	Yüksek
Tehdit Tespiti	UEBA Tabanlı Anomali Algılama Modülleri	6. Davranışsal Analiz (UEBA)	Gelişmiş içeriden gelen tehdit tespiti, sıfır gün istismarlarının davranışsal tespiti.	Orta
API Güvenliği	OWASP API Top 10 ve Yapay Zeka Ajanı Etkileşim Testi	7. Proaktif API Güvenlik Testi & Yapay Zeka Ağ Geçidi Farkındalığı	API saldırı yüzeyinin kapsamlı kapsamı, yapay zeka entegrasyonların ın güvenliği.	Orta
Tedarik Zinciri Güvenliği	SBOM Alımı ve Güvenlik Açığı Korelasyonu	8. Tedarik Zinciri Güvenlik Açığı Yönetimi için SBOM	Yazılım bileşenlerine derinlemesine görünürlük, proaktif risk değerlendirmesi , uyumluluk.	Orta
Otomasyon ve İş	CI/CD Boru Hattı	10. DevSecOps	Geliştirme	Yüksek

Akışı	Entegrasyonu ve Geliştirici Geri Bildirimi	Entegrasyonu ile Otomatik Tarama ve Raporlama	yaşam döngüsüne güvenlik entegrasyonu, hızlı geri bildirim, güvenlik borcunun önlenmesi.	
Kullanıcı Deneyimi	Sezgisel Panolar ve Özelleştirilebilir Akıllı Raporlama	10. Otomatik Tarama ve Raporlama; Genel GUI İyileştirmeleri	Gelişmiş kullanılabilirlik, hızlı karar verme, paydaşlara özel bilgiler.	Yüksek

V. Sonuç: ScanMatrix'i Gelecekteki Siber Güvenlik Liderliği için Konumlandırma

Yapay zeka destekli tespit, kapsamlı buluta özgü ve konteyner güvenliği, gelişmiş gizli yetenekler, derin SIEM/SOAR entegrasyonu, davranışsal analiz, proaktif API güvenliği, SBOM tabanlı tedarik zinciri yönetimi ve sürekli performans optimizasyonunu stratejik olarak bünyesine katarak ScanMatrix, mevcut yeteneklerinin ötesine geçebilir. Bu dönüşüm, ScanMatrix'i 2025'in karmaşık tehdit ortamında vazgeçilmez, bütünsel, akıllı ve otomatik bir platform haline getirecektir.

Siber güvenlik alanı sürekli evrimle karakterize edilmektedir. ScanMatrix'in devam eden başarısı, yalnızca mevcut eğilimleri benimseme yeteneğine değil, aynı zamanda gelecekteki zorlukları tahmin etme, kötü niyetli aktörlerin bir adım önünde olmak için sürekli inovasyon ve adaptasyon kültürünü teşvik etme yeteneğine de bağlıdır. Bu stratejik vizyon, ScanMatrix'i 2025 ve sonrasında siber güvenlik pazarında lider bir çözüm olarak konumlandıracaktır.

Alıntılanan çalışmalar

1. RSAC 2025: 4 Cybersecurity Trends Shaping Tomorrow's Threatscape | PCMag, erişim tarihi Haziran 17, 2025, https://www.pcmag.com/news/rsac-2025-4-cybersecurity-trends-shaping-tomorrows-threatscape
2. Trends and expectations for OT security in 2025 | Nomios Group, erişim tarihi

Haziran 17, 2025, https://www.nomios.com/news-blog/trends-ot-security-2025/
3. The 2025 Software Supply Chain Security Report - ReversingLabs, erişim tarihi Haziran 17, 2025, https://www.reversinglabs.com/sscs-report
4. Forescout's 2025 report reveals surge in device vulnerabilities across IT, IoT, OT, and IoMT, erişim tarihi Haziran 17, 2025, https://industrialcyber.co/reports/forescouts-2025-report-reveals-surge-in-device-vulnerabilities-across-it-iot-ot-and-iomt/
5. Contrast Secures AI Applications and Modern Software | Forrester 2025 SAST Report, erişim tarihi Haziran 17, 2025, https://www.contrastsecurity.com/security-influencers/contrast-secures-ai-applications-and-modern-software-forrester-2025-sast-report-contrast-security
6. SBOM Guide 2025 - How to Turn Compliance into a Security Asset - OPSWAT, erişim tarihi Haziran 17, 2025, https://www.opswat.com/resources/whitepapers/sbom-in-2025-a-strategic-asset-not-just-a-list
7. Microsoft Sentinel UEBA: 2025 Guide to Behavior Analytics, erişim tarihi Haziran 17, 2025, https://secureazcloud.com/microsoft-security/f/microsoftsentinelueba2025guidetobehavioranalytics
8. Top 10 Dynamic Application Security Testing (DAST) Tools for 2025, erişim tarihi Haziran 17, 2025, https://www.acunetix.com/blog/web-security-zone/10-best-dast-tools/
9. Growth Roadmap for Application Security Testing Market 2025-2033, erişim tarihi Haziran 17, 2025, https://www.datainsightsmarket.com/reports/application-security-testing-1368773
10. SOAR in Action: Automating Security Response and Redefining Cyber Defense, erişim tarihi Haziran 17, 2025, https://openretail.io/soar-in-action-automating-security-response-and-redefining-cyber-defense/
11. 2025's Most Important API Security Trends | Curity, erişim tarihi Haziran 17, 2025, https://curity.io/blog/2025-top-api-security-trends/
12. One-for-All Does Not Work! Enhancing Vulnerability ... - arXiv, erişim tarihi Haziran 17, 2025, https://arxiv.org/pdf/2501.16454
13. Learning to Focus: Context Extraction for Efficient Code Vulnerability ..., erişim tarihi Haziran 17, 2025, https://www.arxiv.org/pdf/2505.17460
14. The top 5 software testing trends for 2025 - Xray Blog, erişim tarihi Haziran 17, 2025, https://www.getxray.app/blog/top-2025-software-testing-trends
15. Perform Stealth Network Scanning with Nmap | LabEx, erişim tarihi Haziran 17, 2025, https://labex.io/tutorials/nmap-perform-stealth-network-scanning-with-nmap-415933
16. Advanced NMAP Scanning: Complete Technical Guide, erişim tarihi Haziran 17, 2025, https://securedebug.com/advanced-nmap-scanning-techiques-network-scan/

17. Top 10 Container Security Scanning Tools for 2025 - SentinelOne, erişim tarihi Haziran 17, 2025, https://www.sentinelone.com/cybersecurity-101/cloud-security/container-security-scanning-tools/
18. CrowdStrike Falcon® Cloud Security: Secure Kubernetes and ..., erişim tarihi Haziran 17, 2025, https://www.crowdstrike.com/en-us/platform/cloud-security/container-kubernetes/
19. The top free and open source SIEM tools for 2025 | Red Canary, erişim tarihi Haziran 17, 2025, https://redcanary.com/cybersecurity-101/security-operations/top-free-siem-tools/
20. Best Insider Threat Management Software: Top 9 Solutions in 2025, erişim tarihi Haziran 17, 2025, https://www.exabeam.com/explainers/cyber-threat-intelligence/best-threat-intelligence-platforms-top-10-solutions-in-2025/
21. 7 SIEM Providers to Enhance Threat Detection in 2025 - SentinelOne, erişim tarihi Haziran 17, 2025, https://www.sentinelone.com/cybersecurity-101/data-and-ai/siem-providers/
22. Tenable Vulnerability Scan Monitoring - Panther | A Cloud SIEM Platform for Modern Security Teams, erişim tarihi Haziran 17, 2025, https://panther.com/integrations/tenable
23. Best SIEM Tools for 2025: Top Security Information and Event Management Solutions, erişim tarihi Haziran 17, 2025, https://www.cloudnuro.ai/blog/best-siem-tools-for-2025-top-security-information-and-event-management-solutions
24. 9 Vulnerability Remediation Tools in 2025 - SentinelOne, erişim tarihi Haziran 17, 2025, https://www.sentinelone.com/cybersecurity-101/cybersecurity/vulnerability-remediation-tools/
25. The 2025 Guide to User & Entity Behavior Analytics (UEBA) - Teramind, erişim tarihi Haziran 17, 2025, https://www.teramind.co/blog/user-and-entity-behavior-analytics-guide/
26. OWASP Top Ten, erişim tarihi Haziran 17, 2025, https://owasp.org/www-project-top-ten/