2025 Yılında Ağ Trafiği Kaynağı Tanımlaması ve Tehdit Avcılığı: En Son ve En Etkili 10 İleri Teknik ve Trend

I. Yönetici Özeti

2025 dijital ortamı, bulut bilişimin yaygınlaşması, 5G'nin ve Nesnelerin İnterneti (IoT) cihazlarının çoğalması, ve yapay zekanın (YZ) siber tehditlere entegrasyonu ile benzeri görülmemiş bir ağ trafiği hacmi, hızı ve çeşitliliği ile karakterize edilmektedir. Geleneksel çevre tabanlı güvenlik modelleri, giderek artan sofistike, YZ destekli siber tehditlere ve iç tehditlere karşı yetersiz kalmaktadır. Ağ trafiği kaynaklarının – bu raporda "Yayıncı Avcılığı" olarak yorumlanan – proaktif ve ayrıntılı bir şekilde tanımlanması, güvenliği sürdürmek, performansı optimize etmek ve mevzuata uyumu sağlamak için lüks olmaktan çıkıp stratejik bir zorunluluk haline gelmiştir. Bu rapor, önümüzdeki yıl etkili ağ trafiği kaynağı tanımlamasını ve tehdit avcılığını şekillendirecek en son ve en etkili 10 ileri tekniği ve trendi derinlemesine incelemektedir.

Bu rapor, ağ görünürlüğünü artırma, anormallikleri tespit etme ve hızlı müdahaleyi sağlama konusunda her bir tekniğin temel katkısını vurgulamaktadır. Bu teknikler, gelişen siber tehditlere karşı sağlam bir savunma oluşturarak kuruluşları reaktif "yangın söndürme" yaklaşımından proaktif, akıllı güvenlik duruşlarına taşımaktadır.

II. Giriş: 2025 Yılında Ağ Görünürlüğü ve Tehdit İstihbaratının Gelişen Manzarası

Siber güvenlik ve ağ yönetimi bağlamında, "Yayıncı Avcılığı" (Publisher Hunting), bir ağ içindeki tüm veri akışlarının kökenlerini ve özelliklerini keşfetmek, izlemek, analiz etmek ve kontrol etmek için kullanılan gelişmiş metodolojileri ve teknolojileri ifade etmektedir. Bu, sadece *hangi* verilerin aktığını değil, aynı zamanda *kimin* veya *neyin* bu verileri ürettiğini (örneğin, belirli cihazlar, uygulamalar, kullanıcılar, bulut hizmetleri veya hatta kötü amaçlı süreçler) ve *neden* ürettiğini anlamayı içerir. Bu derinlebilen görünürlük, meşru etkinliği anormal veya kötü amaçlı davranışlardan ayırt etmek için kritik öneme sahiptir. Geleneksel ağ izleme genellikle trafik hacmi, bant genişliği ve temel protokol analizi gibi "ne oluyor" sorularına odaklanmıştır. Ancak, çeşitli uç noktaların (IoT, BYOD), dağıtılmış mimarilerin (bulut, uç bilgi işlem) ve sofistike saldırıların (YZ

tarafından oluşturulan kötü amaçlı yazılımlar, şifreli komuta ve kontrol kanalları) yükselişi, belirli trafik modellerini *kimin* veya *neyin* ürettiğini anlamayı kritik hale getirmektedir.[1] Örneğin, bir "yayıncı" ele geçirilmiş bir IoT cihazı veya yasa dışı bir SaaS uygulaması ise, düzeltme stratejisi basit bir ağ tıkanıklığı sorunundan önemli ölçüde farklılık gösterecektir. Bu durum, sadece trafik gözleminden ziyade akıllı kaynak tanımlamasına ve davranışsal profillemeye odaklanmayı zorunlu kılmaktadır. Bu yeniden tanımlama, güvenlik ekiplerinin becerilerini geleneksel ağ mühendisliğinden daha derinlemesine adli analiz, davranışsal analitik ve uygulama katmanı anlayışına doğru geliştirmeleri gerektiği anlamına gelmektedir. Ayrıca, araç setlerinin temel paket başlıklarının ötesinde daha zengin bağlamsal veriler sunması gerekmektedir.

2025 Ağ Ortamını Şekillendiren Temel Etkenler

2025 yılındaki ağ ortamı, bir dizi güçlü, birbirini etkileyen etken tarafından şekillendirilmektedir:

- **Dijital Dönüşüm ve Bulut Benimsenmesi:** İş yüklerinin ve verilerin çoklu bulut ve hibrit ortamlara hızla geçişi, geleneksel ağ çevrelerinin çözülmesine neden olmaktadır. Veriler ve uygulamalar son derece dağıtık hale gelmiş, bu da merkezi izlemeyi zorlaştırmıştır.[6] Kuruluşlar, karmaşık, dağıtık kaynakları yönetmeli ve farklı bulut sağlayıcıları arasında tek tip güvenlik politikaları uygulamalıdır.[7]
- **5G ve IoT Yaygınlaşması:** IoT cihazlarının ve 5G ağlarının katlanarak büyümesi, özellikle uç noktalarda ağ trafiği hacmini, karmaşıklığını ve potansiyel saldırı yüzeylerini önemli ölçüde artırmaktadır.[9] 2025 yılına kadar 75 milyar bağlı cihaz beklenmektedir.[12] Bu durum, yüksek hızlı veri iletimini yönetmek ve çeşitli uç noktaları güvence altına almak için sofistike çözümler gerektirmektedir.[9]
- **Gelişmiş YZ Destekli Siber Tehditler:** Saldırganlar, daha ikna edici kimlik avı saldırıları, polimorfik kötü amaçlı yazılımlar, deepfake sosyal mühendislik ve otomatik istismar keşfi için YZ'yi giderek daha fazla kullanmaktadır. Bu durum, saldırganlar için giriş bariyerini düşürmekte ve geleneksel kural tabanlı tespit yöntemlerini yetersiz hale getirmektedir.[7] YZ tarafından oluşturulan kimlik avı e-postaları giderek daha sofistike hale gelmekte ve meşru iletişimlerin yazım stilini ve tonunu taklit etmektedir.[17]
- **Genişleyen Saldırı Yüzeyi:** Uzaktan çalışma, Kendi Cihazını Getir (BYOD) politikaları, bulut hizmetleri ve IoT'nin birleşimi, büyük ölçüde genişlemiş ve parçalanmış bir saldırı yüzeyi oluşturarak kapsamlı görünürlüğü ve kontrolü sürdürmeyi zorlaştırmaktadır.[1]
- **Mevzuata Uyum ve Veri Gizliliği:** GDPR gibi daha katı veri koruma yasaları ve veri yerelleştirme gereksinimleri, şifreli trafik de dahil olmak üzere veri akışları üzerinde ayrıntılı görünürlük ve kontrol gerektirmektedir.[3]

Bulut ve uç bilişimin genişlemesi, 5G ve IoT büyümesi ve YZ destekli tehditlerin birleşimi, ağ güvenliği için bir "mükemmel fırtına" yaratmaktadır. Bu durum, geleneksel ağ çevrelerinin güvenilir bir savunma olmaktan çıktığı anlamına gelmektedir. Bu nedenle, kuruluşlar "ihlal varsayımı" zihniyetini benimsemek ve iç ağ görünürlüğüne odaklanmak zorunda kalmaktadır. Trafiğin muazzam hacmi ve karmaşıklığı [1], manuel analizi imkansız hale getirmekte, bu da otomasyon ve YZ'ye olan ihtiyacı artırmaktadır. Artan karmaşıklık ve trafik hacmi (bulut, 5G, IoT nedeniyle)

geleneksel güvenlik modellerinin başarısız olmasına neden olmakta, bu da YZ destekli, gerçek zamanlı ve ayrıntılı ağ görünürlüğü ve kontrolüne olan ihtiyacı artırmaktadır. Bu durum aynı zamanda, verilerin artık daha çeşitli ve daha az kontrol edilen ortamlarda akması nedeniyle mevzuata uyuma daha fazla vurgu yapılmasına yol açmaktadır.

Geleneksel Çevre Savunmasından Sürekli Doğrulama ve Derin Ağ Görünürlüğüne Geçiş

Geleneksel "kale ve hendek" güvenlik modeli, ağ çevresi içindeki her şeye güvenildiği varsayımıyla artık güncel değildir. Odak noktası, Sıfır Güven Mimarisi (ZTA) ile somutlaşan "asla güvenme, her zaman doğrula" yaklaşımına kaymıştır. Bu yaklaşım, konumdan bağımsız olarak her kullanıcı, cihaz ve uygulama için sürekli kimlik doğrulama ve katı erişim kontrolü gerektirmektedir.[1] Bu paradigma değişimi, güvenlik duruşunu sürekli olarak izlemek ve değerlendirmek için derin, gerçek zamanlı ağ görünürlüğü ve gelişmiş analitik yeteneklerini zorunlu kılmaktadır.

III. 2025 Yılında Ağ Trafiği Kaynağı Tanımlaması için En İyi 10 İleri Teknik ve Trend

Bu bölüm, 2025 yılında ağ trafiği kaynaklarını tanımlamak ve yönetmek için en etkili teknikleri ve trendleri detaylandırmaktadır.

Tablo 1: 2025 Yılında Ağ Trafiği Kaynağı Tanımlama Teknikleri (Özet)

Teknik Adı	Temel Prensip	Birincil Fayda	Temel Etkinleştirici	İlgili Snippet Kimlikleri
1. YZ Destekli Anomali Tespiti ve Tahmine Dayalı Tehdit Avcılığı	"Normal" ağ davranışını öğrenir ve sapmaları belirler.	Yanlış pozitifleri azaltır, gizli tehditleri gerçek zamanlı tespit eder.	YZ/Makine Öğrenimi, Davranışsal Analitik	[1]

2. Şifreli Trafik Analizi (ETA) ve İstihbaratı (ETI)	Şifreli trafiği şifre çözmeden meta veri ve davranışsal desenlerle analiz eder.	Veri gizliliğini korurken görünürlüğü sürdürür, şifreli kanallardaki tehditleri tespit eder.	YZ/Makine Öğrenimi, İstatistiksel Analiz	3
3. YZ Destekli Derin Paket İncelemesi (DPI)	Paket yüklerini YZ ile analiz ederek uygulama katmanı görünürlüğü sağlar.	Trafik yönetimi, politika uygulaması, gizli tehdit tespiti.	YZ/Makine Öğrenimi, Katman 7 Analizi	5
4. Sıfır Güven Ağ Güvenliği ve Mikro-segmentasyon	"Asla güvenme, her zaman doğrula" prensibiyle her erişimi doğrular.	Yan hareketleri sınırlar, veri korumasını artırır, iç tehditleri azaltır.	Sürekli Doğrulama, En Az Ayrıcalık	8
5. 5G Ağ Dilimleme ve Uç Güvenliği	Ağ kaynaklarını belirli kullanım durumları için izole edilmiş "dilimler" halinde tahsis eder.	Düşük gecikmeli uygulamaları destekler, yeni iş modelleri sağlar, uç saldırı yüzeyini güvence altına alır.	5G Telco Bulut, Uç Bilişim	12
6. Gelişmiş TLS Parmak İzi (JA3/JA4)	TLS el sıkışma özelliklerine göre cihazları/uygulamaları tanımlar.	Botları, kötü amaçlı kazıma faaliyetlerini ve yetkisiz uygulamaları tespit eder.	Benzersiz TLS İmzaları, WAF'lar	32
7. Kullanıcı ve Varlık Davranış Analizi (UEBA)	Kullanıcı ve cihazların tipik davranışlarını öğrenir, anormallikleri işaretler.	İç tehditleri, ele geçirilmiş hesapları ve saldırganın yan hareketlerini tespit eder.	Süpervizyonlu/ Süpervizyonsuz Makine Öğrenimi	3
8. Proaktif Ağ Adli Bilişimi ve Otomatik Olay Müdahalesi	Sürekli trafik verisi yakalama ve analiz ile tehditleri avlar ve müdahaleyi otomatikleştirir.	Tehdit avcılığını hızlandırır, güvenlik olaylarının etkisini azaltır, operasyonel dayanıklılığı artırır.	YZ/Otomasyon, Paket Analizi	1
9. Gerçek Zamanlı Akış Trafiği Sınıflandırması ve Optimizasyonu	Akış ortamı ve iletişim trafiği modellerini gerçek zamanlı olarak tanımlar ve yönetir.	Bant genişliğini optimize eder, kullanıcı deneyimini kişiselleştirir, yetkisiz akışları tespit eder.	Protokol Analizi, YZ/ Makine Öğrenimi	35
10. Gelişmiş Ağ İzleme ve Gözlemlenebilirlik	Tüm ağ ekipmanlarından telemetri toplar, performans sapmalarını ve tehditleri akıllıca analiz eder.	Hizmet güvenilirliğini artırır, operasyonel maliyetleri azaltır, güvenlik kör noktalarını ortadan kaldırır.	Otomatik Keşif, YZ Destekli Analitik	1

1. YZ Destekli Anomali Tespiti ve Tahmine Dayalı Tehdit Avcılığı

Bu teknik, "normal" ağ davranışının temel çizgilerini oluşturmak ve potansiyel tehditleri, dolandırıcılığı veya sistem arızalarını işaret eden sapmaları, ince desenleri veya olağandışı etkinlikleri otomatik olarak belirlemek için gelişmiş Yapay Zeka (YZ) ve Makine Öğrenimi (MÖ) algoritmalarını kullanır. Geleneksel statik kuralların ötesine geçerek gelişen tehditlere ve ağ dinamiklerine gerçek zamanlı olarak uyum sağlar. Tahmine dayalı tehdit avcılığı, geçmiş verileri ve mevcut desenleri analiz etmek için YZ'yi kullanarak, ortaya çıkan tehditleri tam olarak ortaya çıkmadan önce tahmin eder.[1]

2025 yılında, bu yaklaşım güvenliği reaktif olmaktan proaktif hale dönüştürecektir. Analistler için yanlış pozitifleri önemli ölçüde azaltacak (bir kaynağa göre %40'a kadar) ve uyarı yorgunluğunu giderecektir.[18] YZ destekli anomali tespiti, şifreli komuta ve kontrol (C2) kanalları ve polimorfik kötü amaçlı yazılımlar gibi geleneksel sistemlerin gözden kaçırdığı sofistike, kaçamak tehditlerin gerçek zamanlı olarak belirlenmesini sağlayacaktır. YZ destekli anomali tespiti, insan analistlerin manuel olarak tespit etmesinin imkansız olduğu saniyede milyarlarca olayı işleyebilmektedir.[23] Bu, telekomünikasyonda proaktif bakım, finansal hizmetlerde dolandırıcılık tespiti ve perakendede tedarik zinciri gözetimi gibi alanlarda önemli faydalar sağlayacaktır.[23]

Bu teknik, Darktrace [24], ExtraHop Reveal(x) [24], Cisco Secure Network Analytics [3], SolarWinds Network Performance Monitor [28], Dynatrace [28] ve PRTG [28] gibi araçlar tarafından desteklenmektedir. Dünya İleri Mühendislik Teknolojisi ve Bilimleri Dergisi'nde 2025'te yayınlanan araştırmalar bu alandaki ilerlemeleri vurgulamaktadır.[23]

YZ'nin dönüştürücü gücüne rağmen, bu alandaki gelişmeler YZ'nin analistlerin yerini almadığını, aksine onları "süper kahramanlara" dönüştürdüğünü göstermektedir.[18] Bu durum, insan unsurunun alan bilgisi, bağlamsal anlayış, stratejik yönlendirme ve etik gözetim için kritik önemini koruduğunu göstermektedir.[23] YZ büyük ölçekli veri işlemeyi ve ilk tespiti üstlenirken, karmaşık soruşturmalar, politika iyileştirmeleri ve gerçekten sıfır gün tehditlerine yanıt vermek için insan uzmanlığına ihtiyaç duyulmaktadır. Bu nedenle, kuruluşların sadece YZ araçlarına yatırım yapmakla kalmayıp, aynı zamanda güvenlik ekiplerini YZ ile etkili bir şekilde çalışmak, çıktılarını yorumlamak (açıklanabilir YZ) ve uyarlanabilir uyarı sistemlerini yönetmek için eğitmesi gerekmektedir. Bu yaklaşım[18]'de belirtilen "Ekipleri Yeniden Eğitme" zorluğuna da bir çözüm sunmaktadır.

2. Şifreli Trafik Analizi (ETA) ve İstihbaratı (ETI)

İnternet trafiğinin büyük çoğunluğunun artık şifreli olmasıyla [3], geleneksel Derin Paket İncelemesi (DPI) gizlilik endişeleri, performans yükü ve TLS 1.3 ve ESNI gibi gelişmiş şifreleme protokolleri nedeniyle sınırlamalarla karşılaşmaktadır.[10] ETA ve ETI, şifreli veri akışlarını *şifre çözmeden* analiz ederek bu zorlukların üstesinden gelmektedir. Bu teknikler, kötü amaçlı faaliyetleri belirlemek için meta verilere, davranışsal desenlere, oturum özelliklerine (örneğin, olağandışı oturum uzunlukları, bağlantı desenleri) ve istatistiksel analize odaklanmaktadır. ETI özellikle, şifreli uygulamaları ve hizmetleri şifre çözmeye gerek kalmadan sınıflandırmak ve tanımlamak için YZ/MÖ algoritmalarını istatistiksel ve davranışsal analizle birleştirmektedir.[3]

2025 yılında bu yetenek, veri gizliliğinden veya mevzuata uyumdan ödün vermeden giderek artan şifreli ortamda ağ görünürlüğünü ve tehdit tespitini sürdürmek için kritik öneme sahiptir.[3] Şifreli akışlarda gizlenmiş C2 faaliyetleri ve veri sızması gibi tehditlerin tespitini sağlamaktadır.[3] Uygulama alanları arasında kötü amaçlı yazılım iletişiminin tespiti, veri sızmasının belirlenmesi, kripto uyumluluğunun sağlanması ve trafiğin şifreli olduğu durumlarda bile uygulama kullanımına (örneğin, yetkisiz akış) ilişkin içgörüler elde edilmesi yer almaktadır.[3]

Cisco Secure Network Analytics [3] ve ExtraHop Reveal(x), Corelight Open NDR, Darktrace gibi Ağ Tespit ve Müdahale (NDR) çözümleri [3] bu alandaki temel araçlardır. OpenPR.com kaynakları bu gelişmeleri desteklemektedir.[10]

Şifrelemenin (TLS 1.3, ESNI) yükselişi gizlilik ve güvenlik ihtiyaçlarından kaynaklanmaktadır.[10] Ancak bu durum, geleneksel güvenlik araçları için bir "kör nokta" yaratmaktadır.[3] ETA/ETI, şifre çözmeye gerek kalmadan tehdit tespitine izin vererek bu paradoksu çözmeye çalışmaktadır, böylece gizliliği korumaktadır. Bu, özellikle katı veri gizliliği düzenlemeleri göz önüne alındığında, 2025 yılında kuruluşlar için kritik bir denge unsurudur.[7] Kuruluşlar, uyum sorunlarını önlemek ve sağlam bir güvenlik duruşunu sürdürmek için ETA/ETI yetenekleri sunan çözümlere öncelik vermelidir. Bu aynı zamanda, yasal ve etik sınırların aşılmamasını sağlamak için şifreli trafik analizine ilişkin net iç politikaların gerekliliğini de ima etmektedir.

3. YZ Destekli Derin Paket İncelemesi (DPI)

DPI, ağ trafiği hakkında ayrıntılı içgörüler elde etmek için veri paketlerinin tüm içeriğini (yükünü) Katman 7'de (uygulama katmanı) incelemeyi içerir; bu, yalnızca başlıkları inceleyen geleneksel yöntemlerden farklıdır.[5] 2025 yılında DPI, YZ ve Makine Öğrenimi ile önemli ölçüde geliştirilmekte, daha doğru tehdit tespiti, iyileştirilmiş performans ve gerçek zamanlı uyum sağlamaktadır.[9] YZ destekli DPI, şifreli trafiği (meta veri analizi yoluyla) çözebilir, standart dışı protokol kullanımı gibi anormallikleri tespit edebilir ve kural setlerini dinamik olarak güncelleyebilir.[18]

2025 yılında bu teknik, ağ verileri üzerinde eşsiz bir görünürlük ve kontrol sağlayarak hassas trafik yönetimi, politika uygulaması ve güvenlik geliştirmesi sağlamaktadır.[5] Standart bağlantı noktalarını veya şifrelemeyi kullansalar bile belirli uygulamaları (örneğin, akış platformları) tanımlayabilir.[5] YZ entegrasyonu, yanlış pozitifleri azaltmakta ve DPI'yı tehditleri tahmin eden tahmine dayalı bir kalkan haline getirmektedir.[18] Uygulama alanları arasında saldırı önleme, anomali tespiti (örneğin, şifreli trafikte olağandışı bir artış), trafik şekillendirme (VoIP veya akış gibi kritik uygulamalara öncelik verme), Hizmet Kalitesi (QoS) uygulaması ve içerik filtreleme yer almaktadır.[5]

Cisco, Intel, IBM ve Palo Alto Networks gibi büyük pazar oyuncuları DPI alanında yenilikler yapmaktadır.[9] YZ destekli Suricata [18] ve NDR çözümleri [3] bu alandaki önemli araçlardır. OpenPR.com [10], Hackzone Cyber Security Blog [18] ve Fidelis Security [5] bu teknik için güvenilir referanslardır.

Geleneksel DPI, imzalar ve bilinen kalıplara dayalı olarak büyük ölçüde kural tabanlıydı.[23] Ancak, gelişen tehditler ve şifreli trafikle birlikte bu yaklaşım yetersiz kalmaktadır. YZ/MÖ entegrasyonu, DPI'nın davranışsal analize doğru ilerlemesini sağlamakta, "standart dışı protokol kullanımı" ve "anormallikler" tespit etmesini sağlamaktadır.[5] Bu, DPI'nın önceden açık bilgiye ihtiyaç duymadan yeni tehditleri tespit edebileceği anlamına gelmektedir. Geleneksel DPI'nın modern, gizli tehditlere karşı sınırlamaları, YZ/MÖ entegrasyonunu zorunlu kılmakta, bu da davranışsal ve tahmine dayalı analize geçişi mümkün kılmakta ve daha sağlam ve uyarlanabilir ağ güvenliğine yol açmaktadır.

4. Sıfır Güven Ağ Güvenliği ve Mikro-segmentasyon

Sıfır Güven (ZT), "asla güvenme, her zaman doğrula" prensibiyle çalışmaktadır.[20] Kuruluşun ağının içinde veya dışında olsun, hiçbir kullanıcı, cihaz veya uygulamanın varsayılan olarak güvenilmemesi gerektiğini varsaymaktadır.[8] Bu çerçeve, kimlik, bağlam ve güvenlik duruşuna dayalı olarak her erişim isteğinin sürekli doğrulamasını gerektirmektedir.[8] Mikro-segmentasyon, hassas verileri ve kritik sistemleri daha küçük, bağımsız segmentlere ayırarak saldırganlar için yan hareketleri sınırlayan önemli bir bileşendir.[8]

2025 yılında, dağıtık kaynaklar ve genişlemiş saldırı yüzeyleri nedeniyle bulut güvenliği için kritik öneme sahiptir.[8] Saldırganların yan hareketlerini sınırlar [8], ayrıntılı erişim kontrolleri ve sürekli izleme yoluyla veri korumasını artırır [8] ve katı uyum gereksinimleriyle uyumludur.[8] En az ayrıcalıklı erişim prensibini uygulayarak iç tehditleri ve tedarik zinciri saldırılarını hafifletir.[17] Uygulama alanları arasında hibrit ve çoklu bulut ortamlarının güvenliğini sağlama, hassas verileri (örneğin, savunma ile ilgili veriler) koruma, üçüncü taraf satıcı erişimini yönetme ve geleneksel VPN'lere güvenmeden güvenli uzaktan çalışmayı etkinleştirme yer almaktadır.[8]

SentinelOne, Palo Alto Networks Zero Trust, Zscaler, Okta, Cisco Zero Trust, Microsoft Azure Conditional Access ve Google BeyondCorp [21] bu alandaki önde gelen çözümlerdir. Gold Comet [20], Dev.to [8], SentinelOne [21] ve DataStealth.io [22] güvenilir referanslardır.

Bulut ve uzaktan çalışma ortamlarında geleneksel çevre savunmalarının etkisizliği sürekli olarak vurgulanmaktadır.[8] Sıfır Güven, odağı kullanıcıya ve cihaza kaydırarak, her isteği doğrulayarak bu sorunu doğrudan ele almaktadır. Bu sadece bir teknoloji değil, "kapsamlı bir siber güvenlik stratejisidir".[21] Prensipleri (asla güvenme, her zaman doğrula; en az ayrıcalık; ihlal varsayımı; sürekli izleme) 2025 ağlarının dağıtık, dinamik doğası için açıkça tasarlanmıştır. Bu, kuruluşların Sıfır Güven'i benimsemedikleri takdirde, ağ çevreleri aşınmaya devam ettikçe artan güvenlik açıklarına maruz kalacakları anlamına gelmektedir. Bu, sadece yeni araçların dağıtılması değil, temel bir kültürel ve mimari değişimi gerektirmektedir. [20]'da bahsedilen "Karmaşıklık ve Entegrasyon" zorluğu, aşamalı bir uygulama stratejisinin gerekli olduğunu göstermektedir.

5. 5G Ağ Dilimleme ve Uç Güvenliği için Trafik Yönetimi

5G telco bulut, 5G bağlantısını bulut tabanlı altyapı ile birleştirerek ağ işlevlerinin sanallaştırılmasına ve dinamik olarak dağıtılmasına olanak tanır.[14] 5G'nin temel bir yeteneği olan ağ dilimleme, sağlayıcıların belirli kullanım durumları için, her biri özel QoS, gecikme ve bant genişliğine sahip izole edilmiş, optimize edilmiş "dilimler" oluşturmasına olanak tanır.[11] Uç bilişim, verileri kaynağa daha yakın işleyerek gecikmeyi azaltır ve gerçek zamanlı uygulamaları destekler; Gartner, 2025 yılına kadar kurumsal verilerin %75'inin uçta işleneceğini tahmin etmektedir.[12]

2025 yılında bu teknik, gecikmeyi azaltarak ve bağlantıyı iyileştirerek uç bilişimin benimsenmesini hızlandırmaktadır.[12] Özelleştirilmiş hizmet teklifleri aracılığıyla yeni iş modelleri ve gelir fırsatları yaratmaktadır.[11] Uzaktan cerrahi, otonom araçlar ve akıllı fabrikalar gibi düşük gecikmeli uygulamalar için kritik öneme sahiptir.[12] Ayrıca, uçta yeni saldırı yüzeyleri ortaya çıkarmakta ve sağlam güvenlik önlemlerini zorunlu kılmaktadır.[12] Uygulama alanları arasında ultra düşük gecikmeli uygulamalar (örneğin, AR/VR, uzaktan cerrahi), yüksek tanımlı video akışı, büyük

IoT dağıtımları, akıllı şehirler ve gerçek zamanlı endüstriyel otomasyon yer almaktadır.[11]

5G bağımsız çekirdek ağlar [11], ağ optimizasyonu ve tahmine dayalı bakım için YZ/MÖ [14] ve uç güvenliği için OTAVA'nın S.E.C.U.R.E.™ Çerçevesi [12] bu alandaki temel teknolojiler ve araçlardır. InterDigital [11], Suse.com [14], ResearchAndMarkets.com [15] ve Otava.com [12] güvenilir referanslardır.

Veri işlemenin uca kayması (2025'e kadar %75) [12] ve 5G ağ dilimlemenin modülerliği [14], güvenliğin artık merkezi bir boğulma noktası olamayacağı anlamına gelmektedir. Her dilim ve uç düğümü, potansiyel bir trafik "yayıncısı" ve potansiyel bir saldırı vektörü haline gelmektedir. Bu durum, dağıtık güvenlik önlemlerini, uçta YZ destekli tehdit tespitini [12] ve değişen ağ dilimlerine uyum sağlayabilen dinamik, bağlam farkındalıklı trafik analizini zorunlu kılmaktadır.[14] Güvenlik ekipleri, geleneksel veri merkezi güvenlik modellerinin ötesine geçerek stratejilerini son derece dağıtık bir ortama uyarlamalıdır. Bu, güvenlik çözümlerinin bulut tabanlı, ölçeklenebilir ve 5G ve uç altyapısıyla entegre olabilen çözümler olması gerektiği anlamına gelmektedir. Ayrıca, yeni uzmanlık gerektirdiğinden "Beceri Açığı" zorluğunu da vurgulamaktadır.[6]

6. Gelişmiş TLS Parmak İzi (JA3/JA4) ile Uygulama ve Bot Tanımlaması

TLS parmak izi, bir cihazı veya uygulamayı TLS el sıkışmasının benzersiz özelliklerine göre tanımlayan bir yöntemdir.[32] Bir istemci güvenli bir bağlantı başlattığında, TLS sürümü, şifreleme paketleri, desteklenen uzantılar ve eliptik eğriler gibi ayrıntıları içeren bir ClientHello mesajı gönderir.[32] JA3 (ve halefi JA4), bu ayrıntılardan benzersiz bir karma (parmak izi) oluşturur. Bu, sunucuların ve Web Uygulama Güvenlik Duvarlarının (WAF'lar) yazılım yığınını, işletim sistemini tanımlamasına ve hatta meşru tarayıcıları otomatik süreçlerden veya botlardan ayırt etmesine olanak tanır.[32]

2025 yılında bu teknik, otomatik süreçleri, botları ve kötü amaçlı kazıma faaliyetlerini tanımlamak ve engellemek için web güvenliği için giderek daha önemli hale gelecektir.[32] Veri isteklerine izin vermeden önce istemcileri tanımlayarak güvenliği artırır ve geleneksel IP itibarı veya başlık analizini tamamlar.[32] Akış platformlarını ve e-ticaret sitelerini yetkisiz erişim ve veri sızmasına karşı korumak için kritik öneme sahiptir.[32] Uygulama alanları arasında bot tespiti ve hafifletme, web kazıma önleme, yetkisiz uygulama kullanımının belirlenmesi, WAF yeteneklerinin geliştirilmesi ve API'lerin güvenliğini sağlama yer almaktadır.[32]

TLS kütüphaneleri, WAF'lar ve gerçek JA3 parmak izlerini taklit edebilen tls-client ve curl-impersonate gibi özel HTTP istemcileri [32] bu alandaki

temel teknolojiler ve araçlardır. Rayobyte.com [32] ve CensoredPlanet.org [33] güvenilir referanslardır.

[32]'da açıkça belirtildiği gibi, bot tespiti ile bot kaçırma arasındaki etkileşim bir "kedi fare oyunu"dur. TLS parmak izi giderek daha sofistike hale geldikçe, bu parmak izlerini taklit etme yöntemleri de gelişmektedir. Bu durum, uygulama katmanı güvenliğinde sürekli bir silahlanma yarışı olduğunu ve kuruluşların en son parmak izi ve kaçırma teknikleri hakkında güncel kalması gerektiğini göstermektedir. "TLS İçindeki TLS El Sıkışmaları" zorluğu [33] tespiti daha da karmaşık hale getirmektedir. Bu teknik, çok katmanlı güvenlik yaklaşımlarının gerekliliğini vurgulamaktadır. Yalnızca TLS parmak izine güvenmek yetersizdir; etkinliği sürdürmek için diğer davranışsal analitikler, IP itibarı ve potansiyel olarak YZ destekli analizlerle birleştirilmelidir. Kuruluşların yeni kaçırma taktiklerine sürekli uyum sağlayan güvenlik çözümlerine yatırım yapması gerekmektedir.

7. Kullanıcı ve Varlık Davranış Analizi (UEBA)

UEBA araçları, bir ağdaki kullanıcıların ve cihazların (varlıkların) tipik davranışları için temel çizgiler oluşturmak üzere süpervizyonlu ve süpervizyonsuz makine öğrenimini kullanır.[24] BT erişimi, kullanım modelleri ve ağ iletişimi gibi faaliyetleri sürekli olarak izleyerek, UEBA, ele geçirilmiş bir kullanıcıyı, iç tehdidi (kötü niyetli veya ihmalkar) veya gelişmiş kalıcı tehdidi (APT) işaret edebilecek anormal faaliyetleri belirler.[3]

2025 yılında bu teknik, belirlenmiş temel çizgilerden sapmalara odaklanarak uyarı önceliklendirmesini, olay soruşturmasını ve tehdit avcılığını hızlandırmaktadır.[3] Yetkili erişimi olan içeriden gelenler de dahil olmak üzere saldırıların ve riskli davranışların tespitini otomatikleştirir.[6] Normal ağ modellerini anlamak ve güvenlik sorunlarını işaret edebilecek sapmaları tespit etmek için ağ faaliyetlerine derinlebilen görünürlük sağlar.[3] Uygulama alanları arasında iç tehditlerin tespiti (veri sızması, yetkisiz erişim), ele geçirilmiş hesapların belirlenmesi, saldırganların yan hareketlerinin tespiti ve sadece imzalar yerine davranışsal anormalliklere odaklanarak genel ağ güvenliğinin artırılması yer almaktadır.[2]

Aruba IntroSpect [24], Darktrace [24], ExtraHop Reveal(x) [24] ve Cisco Secure Network Analytics [24] bu alandaki temel araçlardır. PeerSpot [24], CrowdStrike [2], Exabeam [3] ve ThreatIntelligence.com [17] güvenilir referanslardır.

Geleneksel ağ çevrelerinin çözülmesiyle birlikte, insan kullanıcı (ve ilişkili cihazları) fiilen yeni çevre haline gelmektedir. İç tehditler [6] ve ele geçirilmiş kimlik bilgileri önemli saldırı vektörleridir. UEBA, bu "yayıncıların" (kullanıcılar ve cihazlar) davranışlarına odaklanarak bu sorunu

doğrudan ele almakta ve geleneksel savunmaları aşan tehditleri belirlemek için kritik bir teknik haline gelmektedir. Kuruluşlar, kimlik ve erişim yönetimine (IAM) öncelik vermeli ve UEBA'yı daha geniş güvenlik bilgileri ve olay yönetimi (SIEM) ve güvenlik orkestrasyonu, otomasyonu ve yanıtı (SOAR) platformlarıyla entegre etmelidir. Bu, tehdit tespitinde "araçlar" kadar "insanların" da önemli olduğunu vurgulamaktadır.[17]

8. Proaktif Ağ Adli Bilişimi ve Otomatik Olay Müdahalesi

Bu teknik, güvenlik olaylarını belirlemek, araştırmak ve bunlara yanıt vermek için ağ trafiği verilerini sürekli olarak yakalamayı ve analiz etmeyi içerir ve genellikle YZ ve otomasyondan yararlanır. Reaktif olay sonrası analizin ötesine geçerek gizli tehditleri proaktif olarak avlar ve ilk müdahale eylemlerini otomatikleştirir.[1] Teknikler arasında ağ trafiği yakalama ve analizi, bellek analizi ve Windows eserlerinin incelenmesi yer almaktadır.[34] Otomatik olay müdahalesi, tehdit tespiti üzerine önceden tanımlanmış eylemleri (örneğin, ele geçirilmiş bir cihazı izole etme) tetiklemek için YZ/MÖ kullanır.

2025 yılında bu yaklaşım, tehdit avcılığını ve müdahaleyi hızlandırarak ağ güvenliğini önemli ölçüde artıracaktır.[1] Güvenlik açıklarını en aza indirerek ve tehditleri uzak tutarak şüpheli faaliyetleri belirleyerek geleneksel izlemeden kaçınan tehditleri belirler.[1] Tehditlerin neden olabileceği zararı azaltarak, anında bildirim ve önceliklendirme sağlayarak siber olaylardan kaynaklanan potansiyel zararı en aza indirir.[3] YZ ve otomasyon, büyük miktarda veriyi daha hızlı ve daha doğru bir şekilde analiz etmek için adli bilişim yeteneklerini artıracaktır.[13] Uygulama alanları arasında ağ saldırılarının araştırılması, fidye yazılımı ve tedarik zinciri saldırılarına yanıt verme, komuta ve kontrol (C2) iletişiminin belirlenmesi ve gelişen mobil ve IoT teknolojilerinden gelen verilerin analizi yer almaktadır.[3]

Wireshark [4], Tshark, Tcpdump, Tcpick, NGrep [4], Packetbeat [4], Ağ TAP'leri ve SPAN Portları [4] bu alandaki temel araçlardır. Spyder Forensics [34] gibi eğitim kursları da önemlidir. The CTO Club [1], Spyder Forensics [34], Labex.io [35], Exabeam [3], Oxygen Forensics [13], Blackcell.io [4] ve GDHInc.com [26] güvenilir referanslardır.

Vurgu, bir ihlalden sonra sadece temizlik yapmaktan, aktif olarak tehditleri aramaya ve dayanıklılık oluşturmaya kaymaktadır. "Proaktif izleme, sorunsuz ağ operasyonları sağlar" [1] ve "performans düşüşlerini... hizmet kesintileri olarak ortaya çıkmadan önce belirleme" [28] ifadeleri bunu açıkça göstermektedir. Otomatik müdahale mekanizmaları [3], saldırganlar için fırsat penceresini daha da daraltmaktadır. Bu, modern siber saldırıların hızı ve sofistikeliğinin doğrudan bir sonucudur.[12] Kuruluşların, ağ izleme, tehdit tespiti ve olay müdahale sistemlerini entegre etmesi gerekmektedir. Bu, yetenekli personele ve otomatikleştirilmiş oyun kitaplarına sahip olgun bir güvenlik operasyonları merkezini (SOC)

gerektirmektedir. Adli bilişim uzmanları için sürekli öğrenmeye ve ileri eğitime yatırım yapmak [13] kritik hale gelmektedir.

9. Gerçek Zamanlı Akış Trafiği Sınıflandırması ve Optimizasyonu

Bu teknik, akış ortamı ve iletişim trafiği modellerinin gerçek zamanlı olarak tanımlanmasına, analizine ve yönetimine odaklanmaktadır. Geniş bir ağ protokolü yelpazesini çözmeyi ve analiz etmeyi [35], ana bilgisayarlar arasındaki iletişim modellerini anlamayı [35] ve akış platformlarında hiper-kişiselleştirilmiş içerik sunumu ve uyarlanabilir kullanıcı arayüzleri için YZ/MÖ'den yararlanmayı içerir.[11] Ayrıca, yüksek hızlı ağlarda yetkisiz akış veya VoIP aramalarının tespitini de ele almaktadır.[36]

2025 yılında bu yetenek, iyileştirilmiş video sıkıştırma standartları (HEVC, VVC) aracılığıyla bant genişliğini azaltırken video kalitesini optimize edecektir.[11] Kişiselleştirme yoluyla meşru akış hizmetlerinde kullanıcı katılımını ve elde tutmayı artıracaktır.[11] Yüksek hızlı ağlarda iletişim kalitesini sağlamak, kötüye kullanımı (örneğin, yetkisiz VoIP) tespit etmek ve ağ performansını optimize etmek için kritik öneme sahiptir.[36] Uygulama alanları arasında uzaktan işbirliği ve BYOD ortamlarında web gerçek zamanlı iletişim (WebRTC) trafiğini yönetme [37], eğlence ve iş için canlı akışı optimize etme [11] ve yetkisiz akış veya VoIP aramalarını tespit etme yer almaktadır.[36]

Wireshark [35], Zeek [36], WebRTC SDK'ları ve API'leri [37], Yostream.io [38] gibi akış platformları ve VPlayed, Dacast [19] gibi güvenli akış platformları bu alandaki temel araçlardır. Labex.io [35], The Business Research Company [37], InterDigital [11], Zebracat [40], Contus.com [19], Expert Consumers [31], JETIR [36] ve Yostream.io [38] güvenilir referanslardır.

Akış trafiği, büyük bir büyüme alanıdır (WebRTC pazarı 2029'a kadar 81,65 milyar dolar [37]; video, 2025'e kadar internet trafiğinin %82'sini oluşturacak [38]). Bu durum, meşru işler (uzaktan çalışma, eğlence) için fırsatlar sunarken, aynı zamanda ağ yönetimi ve güvenliği için de zorluklar yaratmaktadır. Yetkisiz akış [36] veya iletişim kanallarının kötüye kullanılması (VoIP sahtekarlığı, kimlik avı [36]) bant genişliğini tüketebilir, uyumluluğu ihlal edebilir veya saldırıları kolaylaştırabilir. Bu nedenle, sınıflandırma ve optimizasyon sadece performans için değil, aynı zamanda güvenlik için de önemlidir. Kuruluşlar, meşru, iş açısından kritik akışı yetkisiz veya kötü amaçlı akıştan ayırt etmek için ayrıntılı trafik sınıflandırması uygulamalıdır. Bu, şifreli trafik içinde bile uygulamaları tanımlayabilen [5] ve QoS politikalarını etkili bir şekilde uygulayabilen araçlar gerektirmektedir.

10. Gelişmiş Ağ İzleme ve Gözlemlenebilirlik

Bu teknik, tüm ağ ekipmanlarından (yönlendiriciler, anahtarlar, güvenlik duvarları, sunucular, uç noktalar) sürekli olarak telemetri toplamayı ve bunu akıllıca analiz ederek temel çizgiler oluşturmayı, sapmaları tespit etmeyi, olası bozulmaları tahmin etmeyi ve sorunlu segmentleri izole etmeyi içerir.[28] Temel metriklerin (bant genişliği, gecikme, hata oranları) ötesine geçerek otomatik ağ topolojisi keşfı, YZ destekli anomali tespiti, özelleştirilebilir görselleştirmeler ve sofistike uyarı mekanizmaları içerir.[1] Gözlemlenebilirlik, modern bulut ve hibrit ortamlarda birleşik bir görünüm sağlamak için bunu genişletir.

2025 yılında bu yetenek, ağ yönetimini reaktif "yangın söndürme"den proaktif bakıma kaydırarak daha yüksek hizmet güvenilirliği sağlar ve operasyonel maliyetleri azaltır.[1] Güvenlik açıklarını en aza indirmek ve tehditleri uzak tutmak için temel görünürlük sağlayarak ağ güvenliğini artırır.[1] Ağ performansını artırır ve maliyetleri kontrol altında tutar.[1] Hiper bağlantılı ortamlarda kesintileri önlemek ve güvenlik kör noktalarını azaltmak için kritik öneme sahiptir.[29] Uygulama alanları arasında performans izleme, güvenlik izleme (tehdit tespiti entegrasyonu), bant genişliği kullanımı analizi, yapılandırma yönetimi ve çoklu satıcılı, bulut ve hibrit ortamlardaki ağ sorunlarının giderilmesi yer almaktadır.[1]

SolarWinds Network Performance Monitor [28], PRTG Network Monitor [28], Nagios XI [28], Zabbix [28], ManageEngine OpManager [28], LogicMonitor [29], Datadog [29] ve Dynatrace [28] bu alandaki temel araçlardır. The CTO Club [1], Uptrace.dev [28], Cloudnuro.ai [29] ve Gartner [30] güvenilir referanslardır.

Bulut, uç, 5G ve IoT'nin yaygınlaşması, son derece parçalanmış ve dağıtık ağlar yaratmaktadır.[6] Bunları yönetmek ve güvence altına almak, merkezi bir izleme yaklaşımının ötesine geçmeyi gerektirmektedir. Bunun yerine, "birleşik izleme yaklaşımı" (PRTG [28]) ve "birleşik gözlemlenebilirlik platformu" (Dynatrace [28]) gibi çözümler gereklidir. Bu, kör noktaları ve tutarsızlıkları ortadan kaldırmak için çeşitli kaynaklardan telemetri toplamak ve bunları akıllıca ilişkilendirmek anlamına gelmektedir.[7] Kuruluşlar, silo halindeki izleme araçlarından, tüm BT altyapılarında uçtan uca görünürlük sağlayan entegre platformlara geçmelidir. Bu, yönetimi basitleştirir, sorun gidermeyi hızlandırır ve dağıtık ortamdaki konumlarından bağımsız olarak tüm trafik "yayıncılarını" tanımlamak için kritik olan kapsamlı bir tehdit tespiti görünümü sağlar.

IV. Temel Etkinleştiriciler ve Genel Zorluklar

YZ ve Makine Öğreniminin Yaygın Rolü

YZ/MÖ, 2025 yılında ağ güvenliğini dönüştüren sadece bir araç değil, temel bir unsurdur.[11] Gelişmiş anomali tespiti, davranışsal analitik, gerçek zamanlı uyum ve tahmine dayalı yeteneklerin neredeyse tüm modern ağ güvenliği tekniklerinde temelini oluşturmaktadır.[1] YZ destekli analitikler, saniyede milyarlarca olayı işleyebilir, ince sapmaları belirleyebilir ve yanlış pozitifleri azaltabilir.[18]

Verilerin katlanarak büyümesi [23] ve siber saldırıların artan sofistikeliği [17], manuel veya kural tabanlı güvenliği sürdürülemez hale getirmektedir. YZ, büyük veri akışlarını işlemek için gerekli ölçeklenebilirliği ve insan veya daha basit sistemlerin gözden kaçıracağı karmaşık, gelişen saldırı modellerini belirlemek için zekayı sağlamaktadır. Bu, YZ'nin "işletmelerin gerçek zamanlı bilgiyi kullanma biçimini dönüştürdüğü" [42] ve "daha doğru tehdit tespiti ve iyileştirilmiş performans" sağladığı [9] açıkça belirtilmiştir. Veri akışı ve gelişmiş tehditler YZ'nin benimsenmesini tetiklemekte, bu da gerçek zamanlı işlemeyi, anomali tespitini ve tahmine dayalı yetenekleri mümkün kılmakta ve böylece genel ağ güvenliği duruşunu iyileştirmektedir.

Şifreli Trafiği Yönetme

Gizlilik ve güvenlik için şifreleme protokollerinin (örneğin, SSL/TLS 1.3, ESNI) yaygın olarak benimsenmesi, geleneksel ağ görünürlüğü araçları için bir "kör nokta" yaratmaktadır.[3] Şifreli Trafik Analizi (ETA) ve Şifreli Trafik İstihbaratı (ETI) gibi teknikler, *şifre çözmeye gerek kalmadan* meta verilere ve davranışsal desenlere odaklanarak şifreli veri akışları hakkında içgörü elde etmek için kritik öneme sahiptir.[3] YZ destekli DPI da meta veriler aracılığıyla şifreli trafiği analiz etmede rol oynamaktadır.[5]

ETA/ETI çözümler sunsa da, "TLS İçindeki TLS" sorunu [33] ve TLS parmak izlemesinin devam eden "kedi fare oyunu" [32], şifreli trafiğin sürekli bir zorluk olmaya devam ettiğini göstermektedir. Saldırganlar her zaman şifreli kanalların içinde saklanmaya çalışacaklardır. Bu, güvenlik çözümlerinin gizliliği ihlal etmeden görünürlüğü sürdürmek için sürekli olarak gelişmesi gerektiği anlamına gelmektedir. Kuruluşlar, gelişmiş şifreli trafik analizi yetenekleri sunan güvenlik çözümlerine öncelik vermeli ve bunları genel güvenlik stratejileriyle entegre etmelidir. Bu aynı zamanda, şifreli verilerle uğraşırken mevzuata uyumun önemini de vurgulamaktadır.

5G ve Uç Bilişimin Etkisi

5G ağları, önemli ölçüde daha yüksek hızlar, daha düşük gecikme ve daha fazla cihaz yoğunluğu sunarak gelişmiş kullanım durumlarını mümkün kılmaktadır.[14] Uç bilişim, veri işlemeyi kaynağa daha yakın bir noktaya taşımakta olup, Gartner 2025 yılına kadar kurumsal verilerin %75'inin uçta işleneceğini tahmin etmektedir.[12] Bu dağıtık ortam, yeni saldırı yüzeyleri ortaya çıkarmakta ve gelişmiş siber güvenlik stratejileri gerektirmektedir.[12] 5G'deki ağ dilimleme, özelleştirilmiş ağ segmentlerine olanak tanıyarak trafik analizinin karmaşıklığını artırmaktadır.[14]

5G ve uç bilişime doğru hareket, ağ mimarisini temelden merkezsizleştirmektedir. Bu, güvenliğin merkezi bir darboğaz olamayacağı anlamına gelmektedir. Bunun yerine, güvenlik dağıtık, akıllı ve otonom olmalı, uçta kendi başına çalışmalıdır. Uçta YZ destekli tehdit tespiti [12] kritik hale gelmektedir. Bu aynı zamanda, geleneksel ağ adli bilişim araçlarının yüksek hızlı 5G ağları üzerinden iletişimleri ve veri paketlerini izlemek için uyum sağlaması gerektiği anlamına gelmektedir.[13] Güvenlik mimarları, 5G ve uç dağıtımlarında güvenliği baştan sona tasarlamalıdır, sonradan eklemeye çalışmamalıdır. Bu, her uç cihaz ve ağ dilimi için sıfır güven prensiplerini benimsemeyi içerir.

Sıfır Güven Mimarisi ile Entegrasyon

Sıfır Güven'in "asla güvenme, her zaman doğrula" prensibi, modern, dağıtık ağların güvenliğini sağlamak için temeldir.[8] Konumdan bağımsız olarak her kullanıcı ve cihaz için sürekli kimlik doğrulama ve katı erişim kontrolü gerektirmektedir.[8] Tartışılan ağ trafiği kaynağı tanımlama teknikleri (örneğin, UEBA, YZ destekli anomali tespiti, gelişmiş ağ izleme), Sıfır Güven politikalarını uygulamak için gerekli sürekli izleme, davranışsal temel oluşturma ve ayrıntılı görünürlüğü sağlayarak ZTA'yı doğrudan desteklemekte ve güçlendirmektedir.[8]

Gelişmiş tekniklerin çoğu (YZ anomali tespiti, UEBA, ETA) ağ trafiği "yayıncıları" ve onların davranışları hakkında istihbarat üretmektedir. Sıfır Güven, bu istihbarat için politika uygulama katmanını sağlamaktadır. Örneğin, UEBA anormal kullanıcı davranışı tespit ederse, Sıfır Güven prensipleri erişimin derhal iptal edilmesini veya sorgulanmasını gerektirir. Bu, istihbaratın politikayı bilgilendirdiği ve politikanın güvenliği uyguladığı sinerjik bir ilişki yaratmaktadır. Kuruluşlar, Sıfır Güven'i bağımsız bir çözüm olarak değil, çeşitli gelişmiş güvenlik araçlarını ve tekniklerini entegre eden ve etkinliğini maksimize eden bir mimari felsefe olarak görmelidir. Bu, bütünsel bir güvenlik stratejisi ve kimlik ve erişim yönetimine güçlü bir vurgu gerektirmektedir.

Operasyonel Zorluklar

- **Beceri Açığı:** Bulut güvenliği uzmanları ve genel siber güvenlik personelinde önemli bir eksiklik devam etmektedir.[6] Modern bulut güvenliği, yeni bir zihniyet ve özel beceriler gerektirmektedir.[6]
- **Veri Kalitesi:** YZ destekli sistemler temiz verilerle gelişir, ancak ağ günlükleri gürültülü olabilir ve kapsamlı ön işlem gerektirebilir.[18]
- **Hibrit/Çoklu Bulut Karmaşıklığı:** Karmaşık hibrit ve çoklu bulut ortamlarını işletmek, görünürlük, tek tip güvenlik politikalarını uygulama, erişim kontrollerini yönetme ve gölge BT'yi izleme konularında zorluklar yaratmaktadır.[7]
- **Mevzuata Uyum:** Veri gizliliği ve yerelleştirme için giderek karmaşıklaşan mevzuat ortamı, özellikle küresel işletmeler için önemli zorluklar yaratmaktadır.[7]
- **Uygulama Maliyeti:** DPI gibi gelişmiş çözümlerin yüksek uygulama maliyetleri ve karmaşıklığı önemli zorluklar oluşturabilir.[9]

YZ ve otomasyondaki ilerlemelere rağmen, insan faktörleri ve operasyonel karmaşıklıklar önemli engeller olmaya devam etmektedir. "Beceri açığı" [6], kuruluşların bu gelişmiş sistemleri etkin bir şekilde dağıtma, yönetme ve yorumlama konusunda uzmanlığa sahip olmayabileceği anlamına gelmektedir. "Veri kalitesi" [18], YZ'nin etkinliği için temel bir ön koşuldur ve teknolojinin tek başına bir gümüş kurşun olmadığını vurgulamaktadır. "Hibrit/çoklu bulut karmaşıklığı" [7] ve "maliyet" [9], teknik faydalar açık olsa bile benimsemeyi engelleyebilir. Stratejik yatırımlar sadece teknoloji satın almanın ötesine geçmelidir. Beceri açıklarını kapatmak ve operasyonel karmaşıklıkları yönetmek için sağlam eğitim programları, süreç yeniden mühendisliği ve potansiyel olarak yönetilen güvenlik hizmetlerini içermelidir. YZ için etik hususlar [18] ayrıca bir yönetişim karmaşıklığı katmanı eklemektedir.

V. Stratejik Tavsiyeler ve Geleceğe Yönelik Hazırlık

Bu İleri Teknikleri Benimseme ve Entegre Etme için Önceliklendirme Çerçevesi

- **Mevcut Durumu Değerlendirme ve Boşlukları Belirleme:** 2025 tehditleri ve mimari değişimler (bulut, uç, 5G) bağlamında mevcut ağ görünürlüğü ve güvenlik yeteneklerinin kapsamlı bir denetimini yapın. En yüksek risk maruziyetine sahip alanlara (örneğin, hassas veriler, kritik altyapı) öncelik verin.
- **Sıfır Güven'in Aşamalı Uygulaması:** Yüksek riskli alanlardan başlayarak kademeli olarak genişletin, ZTNA çözümlerini ve mikro-segmentasyonu entegre edin. Bu, uyarlanabilir kimlik doğrulama kullanarak güvenlik ile kullanıcı deneyimi arasında denge kurar.[20]
- **YZ Destekli Çözümlere Yatırım Yapın:** Ağ izleme, DPI ve UEBA genelinde anomali tespiti, tehdit avcılığı ve otomatik yanıt için YZ/MÖ'yi

yerleştiren çözümlere öncelik verin. İnsan analistlere yardımcı olmak için açıklanabilir YZ sunan platformlara odaklanın.[23]
- **Şifreli Trafik İstihbaratını Benimseyin:** Şifre çözmeye gerek kalmadan görünürlüğü sürdürmek, uyumluluğu ve gizliliği sağlamak için güçlü ETA/ETI yeteneklerine sahip NDR çözümlerini dağıtın.[3]
- **Uç ve 5G Dağıtımlarını Güvence Altına Alın:** Uçta YZ destekli tehdit tespitini uygulayın ve güvenlik stratejilerini 5G ağ dilimleme stratejilerine baştan itibaren entegre edin.

YZ/MÖ'den Yararlanma, Şifreli Trafiği Yönetme ve Dağıtık Ortamları Güvence Altına Alma için En İyi Uygulamalar

- **YZ için Veri Yönetişimi:** YZ modelleri için yüksek kaliteli veri akışları sağlamak, yanlış pozitifleri ve yanlılıkları en aza indirmek için sağlam veri ön işleme ve yönetişim çerçeveleri oluşturun.[18]
- **İnsan-YZ Ekip Çalışması:** İnsan-YZ işbirliği kültürünü teşvik edin. Güvenlik ekiplerini YZ ile çalışmak, çıktılarını yorumlamak ve stratejik gözetim sağlamak için eğitmek için yatırım yapın.[18]
- **Birleşik Gözlemlenebilirlik Platformları:** Hibrit ve çoklu bulut ortamlarında uçtan uca görünürlük elde etmek, kör noktaları ortadan kaldırmak için izleme araçlarını birleşik gözlemlenebilirlik platformlarında birleştirin.[28]
- **Proaktif Tehdit Avcılığı:** Reaktif olay müdahalesinin ötesine geçerek YZ destekli içgörüler ve ağ adli bilişim araçlarıyla özel tehdit avcılığı ekipleri kurun.[1]
- **Düzenli Güvenlik Denetimleri ve Değerlendirmeleri:** Yanlış yapılandırmaları ve güvenlik açıklarını belirlemek için kapsayıcı ve sunucusuz mimariler de dahil olmak üzere bulut ve uç ortamlarının güvenlik duruşunu sürekli olarak değerlendirin.[7]

Sürekli İzleme, Uyarlanabilir Güvenlik Duruşları ve İnsan-YZ İşbirliğine Vurgu

2025'teki güvenlik, statik bir durum değil, sürekli bir süreçtir. Kuruluşlar, tehdit ortamı ve teknolojik gelişmelerle birlikte gelişebilen uyarlanabilir güvenlik duruşlarını benimsemelidir. YZ tarafından yönlendirilen ve Sıfır Güven prensipleriyle entegre olan sürekli izleme, bu uyarlanabilirliğin temel taşıdır. İnsan uzmanlığı ile YZ'nin işlem gücü arasındaki sinerji, ağ trafiği kaynağı tanımlamasının ve tehdit avcılığının etkinliğini belirleyecektir.

VI. Sonuç

Ağ trafiği "yayıncılarını" hassas bir şekilde tanımlama, analiz etme ve yönetme yeteneği, 2025 yılında siber güvenlik dayanıklılığı için lüks olmaktan çıkıp temel bir gereklilik haline gelmiştir. Bulut, 5G, IoT ve YZ destekli tehditlerin birleşimi, çevre savunmasından derin, akıllı ve sürekli ağ görünürlüğüne geçişi zorunlu kılmaktadır.

Ağ güvenliğinin geleceği, YZ ve makine öğrenimi ile içsel olarak bağlantılıdır ve giderek daha otonom ve tahmine dayalı yeteneklere doğru ilerlemektedir. Odak noktası, Sıfır Güven'in yol gösterici prensibiyle, verilerin nerede olursa olsun ve nasıl akarsa aksın güvenliğini sağlamak olmaya devam edecektir. Bu ileri teknikleri proaktif olarak benimseyen ve sürekli uyum kültürünü teşvik eden kuruluşlar, gelişen siber tehditler karşısında dijital varlıklarını korumak ve operasyonel sürekliliği sürdürmek için en iyi konumda olacaktır.