2025 Wireshark Oyuncu Avı Projesi: Proaktif Ağ Güvenliği için En Son ve En Etkili 10 Gelişmiş Teknik ve Eğilim

1. Yönetici Özeti

Bu rapor, 2025 yılı için "Wireshark Oyuncu Avı Projesi" kapsamında en etkili ve gelişmekte olan on tekniği ve eğilimi detaylandırmaktadır. Bu proje, ağ merkezli proaktif bir tehdit avcılığı metodolojisi olarak tanımlanmaktadır. Yapay zeka (YZ) destekli saldırılar, genişleyen bulut ve Nesnelerin İnterneti (IoT)/Operasyonel Teknoloji (OT) saldırı yüzeyleri ve sofistike tehdit aktörleri gibi giderek karmaşıklaşan tehdit ortamında, geleneksel güvenlik önlemleri genellikle yetersiz kalmaktadır. Wireshark, temel bir araç olmakla birlikte, gelişmiş analitik, otomasyon ve özel ortamlarla entegre olarak modern güvenlik operasyonlarının vazgeçilmez bir bileşeni haline gelmektedir. Belirlenen teknikler, YZ/Makine Öğrenimi (ML) tabanlı anomali tespiti, gelişmiş davranışsal analitik, buluta özel görünürlük, otomatik tehdit istihbaratı, şifreli trafiğin derinlemesine incelenmesi ve özel IoT/OT analizi gibi alanlara odaklanmaktadır; tüm bunlar Wireshark'ın derin paket analizi yetenekleriyle desteklenmektedir. Başarılı bir uygulama için entegre platformlara stratejik yatırım, sürekli yetenek geliştirme ve proaktif bir güvenlik duruşu gerekmektedir.

2. Giriş: 2025'te "Oyuncu Avcılığı"nın Gelişen Manzarası

"Wireshark Oyuncu Avcılığı"nın Gelişmiş Ağ Merkezli Tehdit Avcılığı Olarak Tanımlanması

"Oyuncu avcılığı", mevcut güvenlik kontrollerini atlatmış gelişmiş tehditleri arama, tespit etme ve izole etme sürecini ifade eden proaktif ve yinelemeli bir yaklaşımdır. Bu, reaktif olay müdahalesinin ötesine geçerek tehdit aktörlerini öngörmeyi ve etkisiz hale getirmeyi amaçlar. Wireshark, "paket yakalama ve protokol analizi için endüstri standardı" olarak [1], ağ trafiğine derinlemesine nüfuz etmek için gerekli ayrıntılı görünürlüğü sağlar ve bu proaktif yaklaşımın kritik bir kolaylaştırıcısıdır. Güvenlik profesyonellerinin "ağlarını anlamalarına, sorun gidermelerine ve güvenli hale getirmelerine" olanak tanır.[2] Bu süreç, potansiyel güvenlik tehditlerini belirlemek, ağ sorunlarını gidermek ve siber suç soruşturmaları için kanıt toplamak amacıyla paketlerin başlıkları, yükleri ve kuyrukları dahil olmak üzere içeriklerinin incelenmesini içerir.[3]

2025'teki Dinamik Tehdit Ortamına Genel Bakış

2025 yılı, siber güvenlik alanında önemli dönüşümlerin yaşandığı bir dönem olarak öne çıkmaktadır. Tehdit ortamı, sürekli gelişen saldırı teknikleri ve genişleyen saldırı yüzeyleriyle karakterizedir.

- **YZ Destekli Saldırılar:** Siber suçlular, gelişmiş kimlik avı şemaları, deepfake dolandırıcılıkları ve adaptif kötü amaçlı yazılımlar dahil olmak üzere sofistike saldırılar geliştirmek için YZ'den giderek daha fazla yararlanmaktadır, bu da tespit ve azaltmayı daha zor hale getirmektedir.[4] YZ, ikna edici kimlik avı ve deepfake'ler geliştirmek için bir "güç çarpanı" görevi görmektedir.[6] Bu durum, hem saldırıların hem de savunmaların karmaşıklığında hızlı bir artışa işaret etmektedir. YZ'nin hem saldırganlar hem de savunmacılar tarafından kullanılması, dinamik ve hızla değişen bir ortam yaratmaktadır. Kuruluşların YZ destekli güvenlik çözümlerini benimsememesi, YZ ile güçlendirilmiş tehdit aktörlerine karşı önemli bir dezavantaj yaratacaktır. Bu durum, güvenlik profesyonellerinin YZ'nin saldırganlar tarafından nasıl kullanıldığını ve YZ destekli analitiklerle buna nasıl karşı konulacağını anlamalarını zorunlu kılmaktadır. Ayrıca, tüm çalışanlar için kapsamlı YZ eğitimi ve politika geliştirme ihtiyacını da beraberinde getirmektedir.[6]
- **Genişleyen Saldırı Yüzeyi:** Çoklu bulut ortamlarının, 2025 yılına kadar 75 milyar IoT cihazının ve hibrit çalışma modellerinin yaygınlaşması, yeni güvenlik açıkları yaratmaktadır.[7] Ortalama cihaz riskinde 2025 yılında yıllık %15 artış yaşanmış, yönlendiriciler kritik güvenlik açıklarının %50'sinden fazlasını oluşturmuştur.[8] Bağlı cihazların hacmi ve çeşitliliği, güvenliğin artık yalnızca çevre savunmalarına veya uç nokta aracılarının sağladığı korumaya dayanamayacağı anlamına gelmektedir.

Wireshark'ın sağladığı derin ağ görünürlüğü, bu genişleyen ve genellikle daha az izlenen ortamlarda yanal hareketin, anormal iç iletişimlerin ve geleneksel kontrolleri atlayan tehditlerin tespit edilmesi için hayati önem taşımaktadır. "Oyuncu Avı Projesi", proaktif, iç savunma gerekliliğini doğrudan ele almaktadır.

- **Fidye Yazılımı Evrimi:** Fidye yazılımı, saldırganların birincil hedef olarak veri sızdırmaya odaklanmasıyla baskın bir tehdit olmaya devam etmektedir, bu da fidye ödenmeden bile kurtarmayı zorlaştırmaktadır.[5] Fidye yazılımı saldırısından kurtulmanın ortalama maliyeti, fidye miktarı hariç, yaklaşık 2.73 milyon dolardır.[5]
- **Ağ Etkinliği İzlemeye Geçiş:** Uç nokta uyarılarına reaktif olarak yanıt vermek yerine, ağ etkinliğini izlemeye ve uç cihaz günlüklerini incelemeye yönelik artan bir odaklanma bulunmaktadır.[9] Bu proaktif duruş, diğer çözümlerin gözden kaçırabileceği şüpheli davranışları, kötü amaçlı Komuta ve Kontrol (C2) işlevlerini ve veri transferi anormalliklerini belirlemeyi amaçlamaktadır.[9]

Wireshark'ın Kalıcı Önemi ve Modern Güvenlik Operasyonlarındaki Genişleyen Rolü

Wireshark, "güçlü bir açık kaynak ağ protokol analizörü" ve "siber güvenlikte temel bir araç" olmaya devam etmektedir.[10] Ağ etkinliğine kapsamlı bir görünüm sağlayarak anormalliklerin, şüpheli davranışların ve protokol düzeyindeki iletişim sorunlarının belirlenmesini ve araştırılmasını mümkün kılar.[11] Temel yetenekleri – paket yakalama, ayrıntılı protokol analizi, filtreleme ve görselleştirme – ağ güvenliği izleme, performans optimizasyonu, protokol sorun giderme ve ağ adli bilişimi için temel niteliktedir.[11] 2025 yılında Wireshark, şifreli QUIC akışları için yerel destek ve 5G ağ dilimleri için yerleşik filtreler ekleyerek yeteneklerini geliştirmektedir.[1]

Wireshark'ın 2025'teki kalıcı önemi, yalnızca bağımsız yetenekleriyle değil, aynı zamanda daha büyük bir güvenlik ekosistemi içindeki uyarlanabilirliği ve genişletilebilirliği ile de ilgilidir. JSON veya CSV günlüklerini günlük toplama platformlarıyla entegrasyon için dışa aktarabilir [1], kardeş uygulaması Stratoshark prensiplerini sistem çağrısı analizine genişletir [13] ve Zeek veya Suricata gibi harici araçlarla birlikte anılmaktadır.[10] Özellikle, özel uzantılar için Lua betiklerini destekler.[10] Bu, "Wireshark Oyuncu Avcılığı"nın Wireshark'ı izole bir şekilde kullanmaktan çok, onu sofistike, çoklu araçlı bir tehdit avcılığı stratejisinin güçlü, ayrıntılı bir bileşeni olarak kullanmakla ilgili olduğu anlamına gelmektedir.

3. 2025'te Oyuncu Avcılığı için En İyi 10 Gelişmiş Wireshark Merkezli Teknik ve Eğilim

Tablo 1: 2025 İçin En İyi 10 Wireshark Oyuncu Avcılığı Tekniği/Eğilimi (Özet)

Teknik/Eğilim Adı	Kısa Açıklama	Birincil Wireshark Rolü	Oyuncu Avcılığı İçin Temel Fayda
1. YZ/ML Destekli Ağ Anomali Tespiti	Ağ davranışındaki sapmaları tespit etmek için gelişmiş ML modellerini kullanma.	Veri yakalama, anomali doğrulama, model besleme.	Bilinmeyen tehditleri ve sıfırıncı gün saldırılarını proaktif olarak belirleme.
2. Gelişmiş Kullanıcı ve Varlık Davranış Analitiği (UEBA)	Kullanıcı ve varlık davranışındaki anormallikleri belirlemek için YZ/ML kullanma.	Davranışsal veri sağlama, şüpheli aktiviteyi derinlemesine inceleme.	İç tehditleri, tehlikeye atılmış hesapları ve riskli kullanıcı davranışlarını tespit etme.
3. Buluta Özel Paket Yakalama ve Adli Bilişim	Geleneksel Wireshark yeteneklerini bulut ortamlarına genişletme.	Bulut kaynaklı sistem çağrılarını ve paketleri analiz etme.	Bulut tabanlı saldırılarda görünürlük sağlama, adli kanıt toplama.
4. Otomatik Tehdit İstihbaratı (TI) Entegrasyonu ve SOAR Playbook'ları	Tehdit istihbaratını güvenlik operasyonlarına entegre etme ve yanıtları otomatikleştirme.	IoC'leri doğrulama, derinlemesine bağlam sağlama, veri paylaşımını kolaylaştırma.	Tehdit tespitini hızlandırma, olay yanıtını otomatikleştirme, analist yükünü azaltma.
5. Şifreli Trafik İçin Derin Paket İncelemesi (DPI)	Şifrelenmiş ağ trafiğindeki gizli tehditleri analiz etme.	TLS/QUIC şifre çözme, özel protokol analizi, parmak izi çıkarma.	Şifreli tünellerde gizlenen kötü amaçlı etkinliği ortaya çıkarma.

6. IoT/OT Protokol Analizi ve Cihaza Özel Tehdit Avcılığı	Endüstriyel ve IoT ortamlarındaki güvenlik açıklarını hedefleme.	Tescilli protokolleri ayrıştırma, cihaz davranış anormalliklerini tespit etme.	Yakınsak BT/OT/IoT ağlarındaki kör noktaları ve güvenlik açıklarını kapatma.
7. Özel Otomasyon için Wireshark Betikleme (Lua/Python)	Tekrarlayan görevleri otomatikleştirmek ve Wireshark işlevselliğini genişletmek.	Özel ayrıştırıcılar oluşturma, analiz iş akışlarını otomatikleştirme.	Tehdit avcılığı yeteneklerini özelleştirme, verimliliği artırma, niş tehditleri hedefleme.
8. Ağ Analizi Yoluyla Proaktif Güvenlik Açığı Yönetimi	Ağ yapılandırma hatalarını ve açıkları istismardan önce belirleme.	Zayıf güvenlik hijyenini, yanlış yapılandırmaları ve açık hizmetleri tespit etme.	Saldırı yüzeyini azaltma, güvenlik duruşunu güçlendirme, ihlalleri önleme.
9. Sıfır Güven Ağ Görünürlüğü ve Politika Uygulaması	Sıfır Güven ilkelerinin etkinliğini doğrulama ve ihlalleri tespit etme.	Mikro segmentasyon ihlallerini izleme, anormal iç iletişimi belirleme.	İç tehditlere karşı koruma sağlama, yanal hareketi engelleme.
10. Büyük Ölçekli PCAP Analizi ve Veri Sızdırma Tespiti	Büyük hacimli paket yakalama dosyalarını verimli bir şekilde analiz etme.	Büyük veri kümelerini yönetme, sızdırma yollarını yeniden yapılandırma.	Geniş ölçekli veri ihlallerini ve kötü amaçlı yazılım yayılımlarını tespit etme.

Teknik/Eğilim 1: YZ/ML Destekli Ağ Anomali Tespiti

Bu teknik, kötü amaçlı etkinliği gösterebilecek normal ağ davranışından sapmaları belirlemek için özellikle denetimsiz ve hibrit yaklaşımlar olmak üzere gelişmiş makine öğrenimi modellerinden yararlanmayı içerir. Geleneksel imza tabanlı yöntemlerin aksine, YZ/ML yeni veya "sıfırıncı gün" tehditlerini tespit edebilir.[7] Ağ akışlarındaki anormallikleri tespit etmek için en çok kullanılan seçenek Otomatik Kodlayıcılar (Autoencoders) olup, bunu Destek Vektör Makineleri (SVM), ALAD veya SOM takip etmektedir.[18]

Wireshark, ML modellerini beslemek için ilk veri yakalama (PCAP/PCAPNG) için çok önemlidir.[3] Günlük toplama platformlarıyla sorunsuz entegrasyon için verileri JSON veya CSV gibi formatlarda dışa aktarabilir.[1] Analiz sonrası, Wireshark, ML sistemleri

tarafından işaretlenen anormallikleri doğrulamak ve derinlemesine araştırmak için kullanılır. Örneğin, bir Python betiği, yeniden iletimler, sıfırlama bayrakları, yüksek gecikme süresi, beklenmedik protokoller veya hatalı biçimlendirilmiş paketler gibi sorunları sınıflandırarak anomali tespiti için Isolation Forest algoritmasını kullanarak Wireshark PCAP dosyalarını analiz edebilir.[18] Random Forest (anomali tespiti için), Destek Vektör Makineleri (SVM) (siber tehdit sınıflandırması için) ve otomatik kodlayıcılar (veri ön işleme ve derin trafik analizi için) gibi algoritmaları birleştiren hibrit modeller, bireysel ML algoritmalarına kıyasla saldırı tespit doğruluğunu (%3-7 oranında) artırmakta ve yanıt süresini azaltmaktadır.[20] YZ/ML destekli araçlar artık trafik optimizasyonundan anomali tespitine ve düzeltmeye kadar her şeyi yöneterek insan hatasını azaltmakta ve ağ güvenilirliğini artırmaktadır.[21]

Geleneksel güvenlik genellikle tespit için önceden tanımlanmış kurallara veya bilinen imzalara dayanmaktaydı.[18] Ancak, sofistike, adaptif kötü amaçlı yazılımların yükselişi [4] ve bilinmeyen tehditleri tespit etme zorunluluğu [18], tespit metodolojilerinde temel bir değişimi gerektirmektedir. Denetimsiz öğrenme modelleri, "eğitilmemiş yeni tehditleri" tespit etme yetenekleri nedeniyle açıkça vurgulanmaktadır.[18] Bu evrim, "bilinen kötü" olanı bulmaktan, bir ağın dinamik "normal" durumunu oluşturmaya ve bundan sapmaları hızla belirlemeye odaklanmayı sağlar. Ayrıca, YZ/ML, kuruluşların potansiyel saldırıları ve güvenlik açıklarını tahmin etmelerine olanak tanıyan tahmine dayalı analitikleri mümkün kılmaktadır.[7] Bu durum, tehdit avcılığının belirli kötü amaçlı yazılım imzalarını bulmaktan çok, bir ağın dinamik "normal" durumunu anlamak ve ince sapmaları hızla belirlemekle ilgili hale geldiğini göstermektedir. Wireshark'ın rolü, yalnızca "ne olduğunu" göstermekten, ML algoritmalarının "ne olması gerektiğini" öğrenmesi için gerekli ham, ayrıntılı veriyi sağlamaya doğru genişlemektedir. Daha sonra, bir anomali ML sistemi tarafından işaretlendiğinde, Wireshark insan analistlerinin "gerçekte ne olduğunu" doğrulamasına ve derinlemesine araştırmasına olanak tanır. Bu, etkili ML modeli eğitimi ve doğrulaması için yalnızca bireysel paket başlıklarından ziyade ağ akışlarının [18] ve kapsamlı paket ayrıntılarının [19] daha derinlemesine anlaşılmasını gerektirir.

Tablo 2: Ağ Anomali Tespiti İçin Temel YZ/ML Algoritmaları (2025)

Algoritma	Anomali Tespitindeki Birincil İşlev	Temel Fayda/Kullanım Durumu	İlgili Kaynak

Otomatik Kodlayıcılar (Autoencoders)	Veri Ön İşleme, Anomali Tanımlama	Yeni tehditleri tespit eder, derin trafik analizi [18]	[18]
Isolation Forest	Anomali Tanımlama	Trafik modellerindeki anormallikleri verimli bir şekilde belirler, çeşitli anomali türlerini sınıflandırır [18]	[18]
Random Forest	Anomali Tespiti, Sınıflandırma	Yüksek doğrulukta saldırı tespiti, yanıt süresini azaltır (hibrit modellerde) [20]	[20]
Destek Vektör Makineleri (SVM)	Siber Tehdit Sınıflandırması, Anomali Tanımlama	Yüksek doğrulukta sınıflandırma, yeni tehditleri tespit eder [18]	[18]
Stochastic Gradient Descent	Sınıflandırma	Etiketli verilerle bilinen saldırı türlerini öğrenir [18]	[18]
K-Nearest Neighbor	Sınıflandırma	Etiketli verilerle bilinen saldırı türlerini öğrenir [18]	[18]
Gaussian Naive Bayes	Sınıflandırma	Etiketli verilerle bilinen saldırı türlerini öğrenir [18]	[18]
Karar Ağacı (Decision Tree)	Sınıflandırma	Etiketli verilerle bilinen saldırı türlerini öğrenir [18]	[18]
AdaBoost	Sınıflandırma	Etiketli verilerle bilinen saldırı türlerini öğrenir [18]	[18]

Teknik/Eğilim 2: Gelişmiş Kullanıcı ve Varlık Davranış Analitiği (UEBA)

UEBA sistemleri, YZ ve Makine Öğrenimi (ML) kullanarak ağ ve sistem etkinliğini izler, normal kullanıcı ve varlık davranışının temel çizgilerini oluşturur. Daha sonra, iç tehditleri, tehlikeye atılmış hesapları veya diğer güvenlik risklerini gösterebilecek sapmaları işaretler.[22] Bu, anormal oturum açma girişimlerini veya olağandışı veri erişim modellerini belirlemeyi içerir.[25] UEBA, riskleri önceliklendirir ve tehditleri ciddiyetine göre sıralayarak bir "akıllı gözetim sistemi" gibi hareket eder.[24]

Wireshark, UEBA'nın veri toplama aşaması için kritik olan ayrıntılı "ağ trafiği verilerini" sağlar ve şüpheli bir etkinliğe dahil olan belirli paketler ve protokoller hakkında derinlemesine bilgi sunar.[3] İşletim sistemi, tarayıcı sürümü, ekran çözünürlüğü, eklentiler, dil ayarları ve ağ bilgileri (IP adresi, coğrafi konum) gibi özellikler kullanılarak cihaz parmak izi çıkarma, benzersiz tanımlama ve davranışsal analiz için UEBA'nın ayrılmaz bir parçasıdır.[26] Wireshark, şifreli trafiği analiz etmek için JA3/JA4 parmak izi çıkarma yeteneğiyle genişletilebilir, SSL/TLS el sıkışma özelliklerine dayanarak kötü amaçlı yazılımları veya olağandışı istemci-sunucu iletişimlerini belirleyebilir.[27] UEBA, şüpheli etkinlikler için Çok Faktörlü Kimlik Doğrulama (MFA) veya tam zamanında eğitim modülleri gibi otomatik yanıtları tetiklemek üzere SOAR platformlarıyla entegre olur ve kullanıcı risk puanlarına göre erişim düzeylerini dinamik olarak ayarlar.[24]

2025 Verizon veri ihlali raporu, işgücünün %8'inin olayların %80'inden sorumlu olduğunu vurgulayarak kritik bir güvenlik açığını ortaya koymaktadır.[24] Bu durum, insan unsurunun önemini açıkça göstermektedir. Davranışsal analitik, özellikle Açıklanabilir YZ (XAI) ile desteklendiğinde, "güvenlik uyarılarının arkasındaki somut gerekçeyi" sunar [24], şeffaflık ve eyleme geçirilebilir bilgiler sağlar. Bu yetenek, dinamik erişim düzeyi değişiklikleri veya tam zamanında eğitim modüllerinin tetiklenmesi gibi "gerçek zamanlı davranışsal müdahalelere" olanak tanır.[24] Bu durum, "oyuncu avcılığının" yalnızca teknik ağ analizinin ötesine geçerek insan davranışını da kapsadığını göstermektedir. Wireshark, insan psikolojisini doğrudan analiz etmese de, UEBA'nın yorumlayıp işaretlediği insan eylemlerinin (örneğin, olağandışı veri sızdırma, anormal erişim modelleri) ağ kanıtını sağlar. Davranışsal analitiğin adaptif eğitimle entegrasyonu [24], potansiyel "oyuncuları" (kötü niyetli veya ihmalkar içerdekiler) eğitmeye ve insan kaynaklı riskleri önemli ölçüde azaltmaya yönelik proaktif bir yaklaşımı işaret etmektedir. Bu durum, nihayetinde işgücünü "sağlam savunucular" haline getirme potansiyeli taşımaktadır.[24] Bu aynı zamanda, tek seferlik eğitimlerden ziyade sürekli güvenlik farkındalığına doğru bir geçişi de ima etmektedir.

Teknik/Eğilim 3: Buluta Özel Paket Yakalama ve Adli Bilişim

Kuruluşlar hızla çoklu bulut ortamlarına geçtikçe [7], bulut altyapısının geçici, dağıtık ve paylaşılan yapısı nedeniyle geleneksel ağ adli bilişimi önemli zorluklarla karşılaşmaktadır.[28] Bulut adli bilişimi, bu dinamik ortamlarda kanıt koruma, olay tespiti, analiz, atıf, sınırlama ve belgeleme üzerine odaklanmaktadır.[28] Bulut sağlayıcıları genellikle fiziksel donanıma doğrudan erişime izin vermediğinden, sanal araçlara bağımlılık zorunludur.[28]

Wireshark Vakfı'ndan (Sysdig) yeni bir açık kaynak araç olan Stratoshark, Wireshark'ın yeteneklerini bulut ortamlarına genişleterek bu sorunu doğrudan ele almaktadır.[13] Bir ana bilgisayardaki sistem çağrılarını ve günlük mesajlarını analiz eder, Wireshark'ın kullanıcı arayüzünü farklı bir alanın tanıdık etkileşimli analizi için yansıtır.[13] Stratoshark, Kubernetes, konteynerler ve diğer buluta özel ortamlardaki beklenmedik davranışlar için gerçek zamanlı tespit ve uyarıları etkinleştirmek üzere Sysdig'in Falco kütüphanelerini, depolarını ve eklentilerini kullanır.[14]

ksniff gibi Kubectl eklentileri, Kubernetes'i klasik ağ araçlarıyla birleştirerek hedef bir pod içindeki tcpdump'ın yerel bir Wireshark örneğine paketleri akışını sağlar.[18]

kubectl-capture, canlı Kubernetes pod'larından sistem çağrısı yakalamalarını tetikler, Falco ve Sysdig ile entegre olarak yan araçlara veya kalıcı aracılara ihtiyaç duymadan zengin izleme verileri üretir.[18] Datadog ve LogicMonitor gibi bulut tabanlı ağ izleme araçları, çoklu bulut işletmeleri ve Yönetilen Hizmet Sağlayıcıları (MSP'ler) için aracısız izleme ve YZ destekli analitik sunar.[30]

Bulut ortamları, özellikle fiziksel donanıma doğrudan erişimi kısıtlaması açısından geleneksel altyapıdan temelden farklıdır [28], bu da geleneksel paket yakalamayı zorlaştırmaktadır. Stratoshark [13] ve

kubectl eklentileri [29] gibi araçların ortaya çıkışı, sistem çağrılarına, günlüklere ve konteyner düzeyindeki trafiğe odaklanarak bu zorluğu açıkça ele almaktadır. Daha da önemlisi, bu araçlar Wireshark'ın tanıdık arayüzünü ve analitik prensiplerini korumaktadır. Bu durum, ağ adli bilişiminde kritik bir evrimi göstermektedir: derin paket analizinin (ayrıntılılık, filtreleme, etkileşimli kullanıcı arayüzü)

ilkeleri, buluta özel bağlamlarda yeni veri kaynaklarına (sistem çağrıları, günlükler) uygulanmaktadır. Bu, güvenlik ekiplerinin tutarlı bir soruşturma iş akışı sürdürmesine ve altyapıları buluta geçse bile mevcut Wireshark yeterliliğinden yararlanmasına olanak

tanır; tıpkı Wireshark'ın ağ paketi analizini demokratikleştirmesi gibi, bulut görünürlüğünü de etkili bir şekilde demokratikleştirmektedir.[15] Bulut bileşenlerinin geçici doğası [28], etkili "oyuncu avcılığı" için geriye dönük veri incelemesinden ziyade gerçek zamanlı yakalama ve analizin daha da kritik hale geldiği anlamına gelmektedir.

Teknik/Eğilim 4: Otomatik Tehdit İstihbaratı (TI) Entegrasyonu ve SOAR Playbook'ları

Siber Tehdit İstihbaratı (CTI), artan siber suç maliyetleri ve giderek sofistikeleşen tehdit aktörleri nedeniyle 2025 yılında stratejik bir avantajdan "operasyonel bir zorunluluk" haline gelmiştir.[7] CTI, tehditle ilgili bilgilerin sistematik olarak toplanmasını, titiz analizini ve "eyleme geçirilebilir bilgilere" dönüştürülmesini içerir.[7] Güvenlik Orkestrasyonu, Otomasyonu ve Yanıtı (SOAR) platformları, olay müdahale iş akışlarını otomatikleştirmek, güvenlik uyarılarını bağlamsal verilerle zenginleştirmek ve Güvenlik Operasyon Merkezi (SOC) operasyonlarını düzene sokmak için CTI beslemelerini entegre eder.[25] SOAR pazarının 2029 yılına kadar 3.39 milyar dolara hızla büyümesi beklenmektedir.[32]

Wireshark, bilinen kötü amaçlı göstergelerin (IoC'ler) otomatik olarak belirlenmesi için tehdit istihbaratı beslemeleri ve veritabanlarıyla entegre edilebilir.[27] Lua betikleme, analiz sırasında anında bağlamsal farkındalık sağlamak için IoC'leri doğrudan Wireshark ekranlarına eklemek için kullanılabilir.[27] Wireshark verileri, toplanan tehdit verilerinin daha geniş güvenlik topluluklarıyla paylaşılmasını kolaylaştırmak için MISP (Kötü Amaçlı Yazılım Bilgi Paylaşım Platformu) formatına aktarılabilir.[27] SOAR platformları, tehlikeye atılmış uç noktaları izole etme, kötü amaçlı IP'leri engelleme, ayrıntılı olay raporları oluşturma [25] ve otomatik güvenlik uyarısı triyajı gerçekleştirme gibi tespit edilen tehditlere yanıtları otomatikleştirir.[25] CTI ayrıca güvenlik duvarları ve saldırı tespit sistemlerinin yapılandırılmasında BT ekiplerini destekler [7], gözlemlenen trafik için bağlam sağlayarak ağ analizini geliştirir.

Tehdit verilerinin hacmi bunaltıcı olabilir ve değerli analist zamanını tüketen yüksek oranda yanlış pozitiflere yol açabilir.[7] Bu durum, mevcut siber güvenlik yetenek açığını daha da kötüleştirmektedir.[7] SOAR'ın birincil faydası, manuel müdahaleyi ve yanıt sürelerini azaltması [25] ve tekrarlayan soruşturmaları ele alarak analist yorgunluğunu hafifletmesidir.[25] YZ/ML ile desteklendiğinde CTI, kuruluşların saldırıları tahmin etmelerine olanak tanıyan tahmine dayalı analitik ve proaktif tehdit avcılığı sağlar.[7] Bu durum, insan analistlerini otomasyon ve istihbaratla destekleme ihtiyacının kritik

olduğunu vurgulamaktadır. Geleneksel olarak manuel bir analiz aracı olan Wireshark, otomatik bir hattın ayrılmaz bir parçası haline gelmektedir. Otomatik uyarıların derinlemesine doğrulanması veya üst düzey tehdit istihbaratına dayalı proaktif avlar için kullanılır. Bu, güvenlik profesyonellerinin yalnızca Wireshark'ın temel işlevlerinde değil, aynı zamanda betik oluşturma ve Wireshark'ın ayrıntılı çıktısını otomatik iş akışlarına nasıl entegre edeceklerini anlamada da yetkin olmaları gerektiği anlamına gelir; böylece sadece operatör olmaktan ziyade güvenlik araçlarının "orkestratörleri" haline gelirler. Bu entegrasyon, kıt insan kaynaklarının karmaşık, nüanslı tehditlere daha verimli bir şekilde tahsis edilmesini sağlar.

Teknik/Eğilim 5: Şifreli Trafik İçin Derin Paket İncelemesi (DPI)

Ağ iletişimlerinde şifrelemenin (örneğin, TLS 1.3, QUIC) artan yaygınlığı, yükün çoğunun gizlenmesi nedeniyle geleneksel paket analizini zorlaştırmaktadır.[27] Buna rağmen, derin paket incelemesi, gizli güvenlik tehditlerini, kötü amaçlı yazılımları ve yetkisiz veri transferlerini belirlemek için kritik önemini korumaktadır.[3]

Wireshark, uygun oturum anahtarları sağlandığında TLS trafiğinin şifresini çözmeyi destekler.[10] Bu, uygulamalarda (örneğin, Chrome) oturum anahtarı günlüğünü etkinleştirmeyi ve Wireshark'ı anahtar günlük dosyasını kullanacak şekilde yapılandırmayı içerir.[10] 2025 yılında Wireshark, şifreli QUIC akışları için yerel destek ve 5G ağ dilimleri için yerleşik filtreler ekleyerek modern şifreli protokolleri analiz etme yeteneğini önemli ölçüde geliştirmektedir.[1] Tescilli veya daha az yaygın şifreli protokoller için özel ayrıştırıcılar geliştirilebilir, bu da Wireshark'ın yapılarını ve içeriklerini yorumlamasına olanak tanır.[10] Wireshark'a entegre edilebilen JA3/JA4 parmak izi çıkarma gibi teknikler, tam şifre çözme olmaksızın bile SSL/TLS el sıkışma özelliklerine dayanarak kötü amaçlı yazılımları veya olağandışı istemci-sunucu iletişimlerini belirleyerek şifreli trafiği analiz etmeye yardımcı olur.[27]

TLS'nin [10] ve QUIC gibi yeni protokollerin [1] yaygın olarak benimsenmesi, ağ trafiğinin önemli ve büyüyen bir kısmının geleneksel inceleme için "karanlık" olduğu, kötü amaçlı etkinliğin kolayca gizlenebileceği "karanlık bir ağ" oluşturduğu anlamına gelmektedir.[9] Şifreli trafiğin şifresini çözme veya parmak izini çıkarma yeteneği, ağ ve güvenlik analizi için kritik bir ihtiyaç olarak açıkça belirtilmektedir.[10] Bu durum, kapsamlı tehdit avcılığı için temel paket yakalamanın artık yeterli olmadığını göstermektedir. Tehdit avcıları, gelişmiş şifre çözme tekniklerinde ustalaşmalı ve tam yük şifre çözme olmaksızın şifreli akışlara görünürlük sağlayan araçlardan (örneğin, JA3/JA4 parmak izi çıkarma)

yararlanmalıdır. Bu, şifreli tünellerin içini "görme" veya şifreli meta verilerden kötü amaçlılığı çıkarabilme yeteneğinin, etkili "oyuncu avcılığı" için önemli bir farklılaştırıcı olduğu sürekli bir kedi-fare oyununu temsil etmektedir. Ayrıca, trafikin engellenmesi ve şifresinin çözülmesine ilişkin politika ve yasal sonuçların dikkatli bir şekilde değerlendirilmesini gerektiren veri gizliliği ve ağ güvenliği arasındaki artan gerilimi de vurgulamaktadır.

Teknik/Eğilim 6: IoT/OT Protokol Analizi ve Cihaza Özel Tehdit Avcılığı

IoT cihazlarının hızla yaygınlaşması ve BT ile Operasyonel Teknoloji (OT) ağlarının artan yakınsaması, yeni ve karmaşık güvenlik açıkları ortaya çıkarmaktadır.[4] 2025'teki en riskli cihazlar arasında IoMT cihazları (örneğin, görüntüleme cihazları, laboratuvar ekipmanları, infüzyon pompası kontrolörleri), OT cihazları (örneğin, evrensel ağ geçitleri, tarihçiler, Bina Yönetim Sistemleri (BYS), Kesintisiz Güç Kaynağı (UPS) cihazları) ve IoT cihazları (örneğin, Ağ Video Kaydediciler (NVR'lar), IP kameralar, Satış Noktası (PoS) sistemleri) bulunmaktadır.[8] Bu cihazlar genellikle eski işletim sistemlerini çalıştırmakta, tehlikeli derecede açık yönetim portlarına sahip olmakta, varsayılan kimlik bilgilerini kullanmakta veya şifresiz veri transferi yapmakta, bu da onları saldırganlar için birincil hedef haline getirmektedir.[8]

Wireshark, IoT ortamlarında "protokol incelemesi" için vazgeçilmezdir.[35] IoT cihazlarından gelen trafiği koklayarak iletişim modellerini anlamak ve beklenmedik sunucu iletişimlerini belirlemek için kullanılabilir, bu da gizli güvenlik açıklarını veya kötü amaçlı etkinliği ortaya çıkarabilir.[36] Tescilli veya daha az yaygın IoT/OT protokollerini analiz etmek için özel Wireshark ayrıştırıcıları kritik öneme sahiptir.[10] Omron FINS [37] ve Modbus, BACnet, OPC UA ve Zigbee gibi endüstriyel protokoller [38] belirli örneklere dahildir. Wireshark, IoT/OT ortamlarındaki ihlalleri veya yanlış yapılandırmaları belirlemek için son derece ilgili olan anormal ARP paketlerini veya normal trafik akışındaki değişiklikleri tespit edebilir.[10] Teknikler arasında derin paket incelemesi kullanarak pasif cihaz keşfi uygulama, DHCP/DNS/ARP günlükleriyle ilişkilendirme ve davranışsal imzalarına göre cihaz türlerini belirlemek için makine öğrenimi kullanma yer almaktadır.[38]

Forescout 2025 raporu, "BT, IoT, OT ve IoMT genelinde cihaz güvenlik açıklarında bir artış" olduğunu açıkça vurgulamaktadır.[8] Ayrıca, "çok sayıda güvenlik çözümünün silolar halinde çalıştığını, tehlikeli kör noktalar bıraktığını" açıkça belirtmektedir.[8] Bu silo yaklaşımı, saldırıların artık daha önce ayrı olan bu alanlar arasında yanal olarak hareket

edebilmesi nedeniyle özellikle sorunludur (örneğin, bir IP kamerasından (IoT) bir iş istasyonuna (BT) ve ardından PLC'leri (OT) devre dışı bırakan R4IoT saldırısı).[8] Bu durum, 2025'teki "oyuncu avcılığının" geleneksel BT ağlarıyla sınırlı kalmaması gerektiğini göstermektedir. IoT, OT ve IoMT ortamlarına

genişlemesi gerekmektedir; bu da onların benzersiz protokolleri, güvenlik açıkları ve operasyonel bağlamları hakkında özel bilgi gerektirmektedir. Wireshark, güçlü özel ayrıştırıcı yetenekleriyle, bu çeşitli ve genellikle tasarımdan güvenli olmayan ortamları anlamak için "Rosetta Taşı" haline gelmektedir. Zorluk sadece teknik değil, aynı zamanda kurumsal olup, kapsamlı görünürlük ve savunma sağlamak için birleşik bir güvenlik yaklaşımı ve daha önce silolanmış BT, OT ve IoT ekipleri arasında işbirliği çabaları gerektirmektedir.

Tablo 3: En Riskli IoT/OT/IoMT Cihazları ve İlişkili Güvenlik Zorlukları (2025)

Cihaz Kategorisi	En Riskli Cihazlar	İlişkili Güvenlik Zorlukları	İlgili Kaynak
Nesnelerin İnterneti (IoT)	Yönlendiriciler, Ağ Video Kaydediciler (NVR'lar), VoIP, IP Kameralar, Ağ Bağlantılı Depolama (NAS) cihazları, Satış Noktası (PoS) sistemleri	Açık yönetim portları, eski işletim sistemleri, varsayılan kimlik bilgileri, genel kötü amaçlı yazılım hedefleri, RAM kazıyıcıları [8]	[8]
Operasyonel Teknoloji (OT)	Evrensel Ağ Geçitleri, Tarihçiler (Historians), Bina Yönetim Sistemleri (BYS), Fiziksel Erişim Kontrol Sistemleri, Kesintisiz Güç Kaynağı (UPS) cihazları	Yanal hareket riski, BT/OT ağları arasındaki tehlikeli bağlantılar, çevrimiçi maruz kalma, varsayılan kimlik bilgileri, kritik altyapı etkisi [8]	[8]
Tıbbi Nesnelerin İnterneti (IoMT)	Görüntüleme cihazları (BT, PET-BT, X-ray), Laboratuvar ekipmanları (kan/idrar	Eski/güvenlik açığı olan işletim sistemleri, şifrelenmemiş veri	[8]

	analizörleri), Sağlık iş istasyonları, İnfüzyon pompası kontrolörleri	transferi (DICOM), hassas hasta verilerine erişim, fidye yazılımı hedefi, hasta güvenliği riski [8]	

Teknik/Eğilim 7: Özel Otomasyon için Wireshark Betikleme (Lua/Python)

Wireshark, işlevselliğini genişletmek, tekrarlayan analiz görevlerini otomatikleştirmek ve özel ayrıştırıcılar oluşturmak için başta Lua olmak üzere kapsamlı betiklemeyi destekler.[10] Python,

pyshark gibi kütüphaneler aracılığıyla, gelişmiş analiz ve harici araçlarla entegrasyon için PCAP dosyalarıyla da etkileşime girebilir.[19]

- **Özel Ayrıştırıcılar:** Tescilli veya belgelenmemiş protokoller için özel ayrıştırıcılar geliştirmek, özellikle niş veya endüstriyel ortamlarda özel ağ trafiği hakkında derinlemesine görünürlük elde etmek için hayati öneme sahiptir.[10]
- **Analizi Otomatikleştirmek:** Betikler, makine öğrenimi modelleri için özellik çıkarma [19], özel filtreler oluşturma, belirli raporlar üretme veya gözlemlenen paket modellerine göre harici eylemleri tetikleme gibi tekrarlayan görevleri otomatikleştirebilir.[39] Örneğin, bir Python betiği protokol türünü, paket uzunluğunu, kaynak/hedef IP'lerini/portlarını, TCP yeniden iletimlerini/sıfırlama bayraklarını çıkarabilir ve ardından anormallikleri belirlemek için Isolation Forest algoritmasını uygulayabilir.[18]
- **Tehdit Avcılığı Geliştirmeleri:** Lua betikleri, özel bağlam menüleri ekleyerek veya Tehlike Göstergelerini (IoC'ler) doğrudan ekrana entegre ederek Wireshark'ın kullanıcı arayüzünü geliştirebilir, tehdit avları sırasında anında bağlamsal farkındalık sağlayabilir.[27]

Wireshark'ın açık kaynak doğası ve güçlü betikleme yetenekleri (Lua, Python) temel özellikleri olarak defalarca vurgulanmaktadır.[10] Tescilli protokoller için özel ayrıştırıcılara duyulan açık ihtiyaç [10] ve otomatik anomali tespiti için betikleme kullanımı [19], özel çözümlere olan talebi vurgulamaktadır. Bu durum, 2025 yılında son derece etkili "oyuncu avcılarının" yalnızca mevcut araçların yetkin kullanıcıları değil, giderek kendi analitik yeteneklerinin

yaratıcıları ve *özelleştiricileri* olduğunu göstermektedir. Betik yazma veya özel

ayrıştırıcılar geliştirme yeteneği, analistlerin Wireshark'ı benzersiz kurumsal ortamlara uyarlamasına, belirsiz veya özel protokolleri analiz etmesine veya hazır çözümlerin gözden kaçırabileceği yeni saldırı tekniklerine yanıt vermesine olanak tanır. Bu, genel ağ analizinin ötesine geçerek, tehdit avcılığı ekibi içinde ağ, güvenlik ve programlama becerilerinin sofistike bir karışımını gerektiren, son derece hedefe yönelik, özel tehdit avcılığına doğru bir geçişi temsil etmektedir.

Teknik/Eğilim 8: Ağ Analizi Yoluyla Proaktif Güvenlik Açığı Yönetimi

Bu teknik, saldırganlar tarafından istismar edilmeden önce ağ yapılandırma hatalarının, yamalanmamış sistemlerin ve açıkta kalan hizmetlerin sürekli olarak belirlenmesini ve giderilmesini içerir. Bu, ağ trafiği analizinin zayıflıkları tespit etmeye ve güvenlik hijyenini sağlamaya yardımcı olduğu proaktif bir güvenlik duruşuna doğru stratejik bir geçişi temsil eder.[9]

Wireshark, olağandışı port etkinliğini, şifrelenmemiş hassas verileri [40] ve zayıf güvenlik hijyeni veya yanlış yapılandırmaların diğer işaretlerini tespit edebilir.[3] Ağ segmentasyon politikalarının etkinliğini doğrulamak [38] ve cihaz yapılandırmalarını güçlendirmenin bir parçası olarak kullanılmayan hizmetlerin veya arayüzlerin (örneğin, USB, SSH, Telnet, SNMPv1) devre dışı bırakıldığından emin olmak için kullanılabilir.[38] Paket analizi, açık portlar veya yanlış yapılandırılmış güvenlik duvarları gibi ağ yapılandırma hatalarını belirlemeye yardımcı olur.[3] 2025'te temel odak noktalarından biri, uç noktalar ve SIEM'lerden gelen uyarılara yalnızca reaktif olarak yanıt vermek yerine, proaktif güvenlik için "ağ etkinliğini izlemek ve uç cihaz günlüklerini incelemektir".[9]

"Proaktif" güvenlik açığı yönetimine verilen önem [38] ve riskleri belirlemek için ağ etkinliğini izlemeye yönelik geçiş [9], ağ trafiğinin yalnızca saldırı tespiti için değil, aynı zamanda güvenlik açığı istihbaratı için de zengin ve yeterince kullanılmayan bir kaynak olduğunu düşündürmektedir. Ağ trafiği içinde düz metin parolaları [40] veya şifrelenmemiş aygıt yazılımı güncellemelerini [41] doğrudan gözlemleme yeteneği, kritik yapılandırma hatalarını veya güvenli olmayan uygulamaları anında ortaya çıkarır. Geleneksel olarak olay sonrası analiz veya sorun giderme için kullanılan Wireshark,

önleyici güvenlik için hayati bir araç haline gelmektedir. Ağdaki yanlış yapılandırmaları, güvensiz protokolleri ve zayıf güvenlik hijyeni uygulamalarını aktif olarak avlayarak, kuruluşlar bilinen zayıflıkları saldırganlar istismar etmeden önce duruşlarını güçlendirebilirler. Bu, "oyuncu avcılığının" aynı zamanda bir kuruluşu kolay bir hedef

haline getiren *iç* güvenlik açıklarını bulma ve düzeltme, böylece genel saldırı yüzeyini ve başarılı ihlallerin olasılığını azaltma ile de ilgili olduğu fikrini pekiştirmektedir.

Teknik/Eğilim 9: Sıfır Güven Ağ Görünürlüğü ve Politika Uygulaması

Sıfır Güven, 2025'te varsayılan güvenlik modeli haline gelmekte olup, hiçbir kullanıcının veya cihazın konumundan bağımsız olarak doğal olarak güvenilir olmadığı ilkesiyle çalışmaktadır.[4] Bu model, tüm ağ etkileşimlerinin sıkı kimlik doğrulaması, mikro segmentasyon ve sürekli izlenmesini gerektirir.[4]

Wireshark, segmentlere ayrılmış bölgeler arasındaki trafik akışını analiz ederek, yetkisiz yanal hareketin önlendiğinden ve politikaların doğru bir şekilde uygulandığından emin olarak mikro segmentasyonun etkinliğini doğrulamak için kullanılabilir.[38] Sıfır Güven politikalarına karşı gerçek ağ davranışını gözlemleyerek politika tabanlı erişim kontrollerinin ve cihaz duruşu kontrollerinin doğrulanmasına yardımcı olur.[38] UEBA sistemleri, SOAR ile entegre olarak, Sıfır Güven çerçevesinde kullanıcı risk puanlarına göre erişim düzeylerini dinamik olarak ayarlayabilir, şüpheli etkinlikler için MFA'yı tetikleyebilir veya erişimi engelleyebilir.[24] Wireshark, Sıfır Güven ilkelerinin ihlalini gösterebilecek anormallikleri, örneğin segmentler arasında beklenmedik iletişimi, olağandışı erişim girişimlerini veya güvenlik kontrollerini atlama girişimlerini tespit etmeye yardımcı olabilir.[10]

Sıfır Güven, "hiçbir kullanıcının veya cihazın doğal olarak güvenilir olmadığı" [4] ilkesini benimsemekte ve mikro segmentasyon ile sürekli izlemeye büyük önem vermektedir.[4] Bu mimari değişim, her etkileşimin titizlikle incelendiği, son derece ayrıntılı ve dinamik bir ağ ortamı yaratmaktadır. Sıfır Güven mimarisinde, "oyuncu avcılığı" temelden çevre ihlallerini tespit etmekten, ağ içindeki herhangi bir yetkisiz veya anormal etkinliği, ne kadar küçük veya önemsiz olursa olsun, belirlemeye doğru kaymaktadır. Wireshark'ın paket düzeyinde eşsiz derin görünürlük yeteneği, Sıfır Güven politikalarının gerçekten amaçlandığı gibi uygulandığını doğrulamak ve tehlikeye atılmış bir kimliği, sözde güvenli bir segment içindeki yanal hareket girişimini veya bir politika atlatmayı gösterebilecek ince sapmaları tespit etmek için çok önemlidir. Bu, tüm ağı bir dizi küçük, gözlemlenebilir ve sürekli izlenen avlanma alanına dönüştürmekte, bu da daha öncekinden daha ayrıntılı analiz gerektirmektedir.

Teknik/Eğilim 10: Büyük Ölçekli PCAP Analizi ve Veri Sızdırma Tespiti

Artan veri hacimleri, uç noktaların çoğalması ve sofistike saldırıların giderek veri sızdırmaya odaklanmasıyla [9], veri ihlallerini, kötü amaçlı yazılım yayılımını ve yetkisiz veri transferlerini belirlemek için büyük paket yakalama dosyalarını verimli bir şekilde analiz etmek kritik önem taşımaktadır.[3] Veri sızdırma, saldırganlar için genellikle daha kazançlıdır ve mağdur kuruluşların tespit etmesi ve önlemesi önemli ölçüde daha zordur.[9]

Wireshark, belirli paketlere derinlemesine nüfuz etmek için mükemmel olsa da, uzun süreli, yüksek hacimli yakalama için dumpcap gibi araçlar önerilmektedir.[39]

large-pcap-analyzer, çok büyük PCAP dosyaları üzerinde yaygın işlemleri yüksek hızda gerçekleştirmek için özel olarak tasarlanmıştır.[39]

editcap ve mergecap gibi diğer yardımcı programlar, büyük yakalama dosyalarını yönetmek ve işlemek için esastır.[39] Arkime (eski adıyla Moloch) gibi tamamlayıcı araçlar, büyük ölçekli, açık kaynaklı, indekslenmiş paket yakalama ve arama aracı [39], Brim [39] ve Brute Shark (PCAP dosyalarının derinlemesine işlenmesi ve incelenmesi için bir Ağ Adli Analiz Aracı (NFAT), [39]), Wireshark'ın etkileşimli yeteneklerini aşan devasa veri kümelerini işlemek, indekslemek ve analiz etmek için hayati öneme sahiptir. Wireshark'ın gelişmiş filtreleme yetenekleri ve akış yeniden yapılandırma özellikleri [44], veri sızdırma yollarını izlemek, iletişim akışlarını yeniden yapılandırmak ve şüpheli paket içeriklerini incelemek için paha biçilmezdir.[3]

Ağ trafiğinin büyük hacmi [18] ve veri sızdırmanın tespitine kritik odaklanma [9], tekil, etkileşimli Wireshark analizinin büyük ölçekli kurumsal ortamlar için yetersiz olduğu anlamına gelmektedir. Arkime, Brim ve

large-pcap-analyzer gibi devasa PCAP dosyaları için tasarlanmış araçların açıkça belirtilmesi [39], terabaytlarca veriyi işleme gerekliliğini doğrudan ele almaktadır. Bu durum, 2025'te etkili "oyuncu avcılığının" özel araçlardan oluşan bir

ekosistem gerektirdiğini vurgulamaktadır. Wireshark, belirli olayların veya anormalliklerin derinlemesine, ayrıntılı analizi için vazgeçilmez bir "büyüteç" olmaya devam etmektedir, ancak adli ve avcılık amaçları için büyük paket verilerinin yaşam döngüsünü yönetebilen yüksek performanslı yakalama, depolama, indeksleme ve görselleştirme çözümleriyle tamamlanmalıdır. Zorluk sadece bireysel paketleri analiz etmek değil, tüm ağ verilerini ölçekli olarak yönetmek ve bunlardan istihbarat

çıkarmaktır; bu da sağlam depolama ve işleme altyapısına önemli bir yatırım gerektirmektedir.

Tablo 4: Wireshark Destekli Tehdit Avcılığı İçin Tamamlayıcı Araçlar (2025)

Araç Adı	Birincil İşlev	Wireshark'ı Nasıl Tamamlar?	İlgili Kaynak
Dumpcap	Uzun süreli, yüksek hacimli paket yakalama	Wireshark'ın yakalama motoru olarak görev yapar, büyük veri kümeleri için idealdir.	[39]
Editcap / Mergecap	Yakalama dosyalarını düzenleme ve birleştirme	Yakalama dosyalarının ön/son işlenmesini sağlar, analiz için veriyi hazırlar.	[39]
Arkime (eski Moloch)	Büyük ölçekli, indekslenmiş paket yakalama ve arama	Wireshark'ın etkileşimli analizini tamamlayan geniş ölçekli PCAP yönetimi ve araması sunar.	[39]
Brim	Günlük ve PCAP arşivleme ve tarama	Günlük ve PCAP verilerini düzenli bir şekilde depolama ve kolayca gözden geçirme imkanı sağlar.	[39]
Brute Shark	Ağ Adli Analiz Aracı (NFAT)	PCAP dosyalarının derinlemesine işlenmesi ve incelenmesi için özel yetenekler sunar.	[39]
CloudShark	Tarayıcı tabanlı yakalama görüntüleme ve analiz	Yakalamaları tarayıcıda görüntüleme, etiketleme ve URL ile	[39]

		paylaşma yeteneği sağlar.	
Dshell	Genişletilebilir ağ adli analiz çerçevesi	Ağ paketi yakalamalarının ayrıştırılmasını destekleyen eklentilerin hızlı gelişimini sağlar.	[39]
NetworkMiner	Ağ adli analiz aracı	PCAP dosyalarını analiz ederek HTTP başlıklarını, aktarılan ikili dosyaları ve belgeleri çıkarır.	[3]
Stratoshark	Buluta özel sistem çağrısı ve günlük analizi	Wireshark'ın prensiplerini bulut ortamlarına genişleterek sistem çağrısı görünürlüğü sağlar.	[13]
Ksniff (Kubectl eklentisi)	Kubernetes pod'larından ağ paketi yakalama	Kubernetes ortamlarında tcpdump'ı Wireshark'a akışını sağlayarak buluta özel görünürlük sağlar.	[29]

4. 2025 Oyuncu Avcılığı İçin Zorluklar ve Değerlendirmeler

Veri Yükünü ve Yanlış Pozitifleri Ele Alma

"Tehdit verilerinin muazzam hacmi bunaltıcı olabilir" [7], bu da değerli analist zamanını ve kaynaklarını tüketen yüksek oranda yanlış pozitiflere yol açmaktadır.[7] YZ/ML modelleri

güçlü olmakla birlikte, "belirli ağ ortamları için ayarlama gerektirebilir" [19] ve etkinliklerini tehlikeye atabilecek "zehirleme saldırılarına" da maruz kalabilirler.[6] Analiz için "daha fazla veri daha iyidir" sözü genellikle doğru olsa da, siber güvenlikte gerçeklik, uygun işleme ve akıllı filtreleme olmaksızın çok fazla

ham, yapılandırılmamış verinin doğrudan bilgi yüklenmesine ve yönetilemez bir yanlış pozitif hacmine yol açmasıdır.[7] Bunu azaltmak için tasarlanmış gelişmiş YZ/ML araçları bile tak ve çalıştır değildir; belirli ağ ortamları için dikkatli ayarlama gerektirirler ve kendileri de zehirleme gibi yeni saldırı vektörlerine karşı savunmasızdırlar.[6] Bu durum, yalnızca daha fazla veri toplamanın veya YZ araçlarını dağıtmanın etkili "oyuncu avcılığı" için yeterli olmadığını göstermektedir. Bunun yerine, başarı, sofistike veri filtrelemesine, uyarıların akıllıca önceliklendirilmesine [25] ve tespit modellerinin sürekli olarak iyileştirilmesine bağlıdır. Temel zorluk sadece veriyi

elde etmek değil, aynı zamanda onu büyük ölçekte *anlamlandırmak* ve eyleme geçirilebilir istihbarat çıkarmaktır; bu da tehdit avcılığı ekipleri içinde veri bilimi becerilerinin ve sağlam veri yönetimi çerçevelerinin artan önemini vurgulamaktadır.

Siber Güvenlik Yetenek Açığı ve Sürekli Eğitim İhtiyacı

"Yetenekli güvenlik personelinin eksikliği", SOAR platformlarının hızla büyümesinin ve benimsenmesinin ana faktörüdür.[32] "Siber güvenlik yetenek açığı", yaygın olarak kabul görmüş ve devam eden bir zorluktur.[7] Birçok işletme şu anda 7/24 izleme yeteneklerinden veya yerleşik acil durum müdahale protokollerinden yoksundur.[4] Gelişen tehdit ortamı, bu alanın "sürekli öğrenmeye ve yüksek standartlara" bağlı bireyler gerektirdiğini zorunlu kılmaktadır.[43] Güvenlik teknolojilerindeki önemli ilerlemelere, YZ ve SOAR dahil olmak üzere, rağmen, araştırmalar boyunca tekrar eden tema, yetenekli personel eksikliğidir.[7] Yeni teknolojilerin ve ortamların (bulut, IoT, YZ) artan karmaşıklığı, edinilmesi ve sürdürülmesi zor olan yüksek derecede uzmanlaşmış uzmanlık gerektirmektedir.[13] Bu durum, en gelişmiş araçların bile onları kullanan analistler kadar etkili olduğunu ortaya koymaktadır. "Oyuncu avcılığı" projesi, doğası gereği, karmaşık ağ verilerini yorumlayabilen, sofistike tehdit aktörü Taktiklerini, Tekniklerini ve Prosedürlerini (TTP'ler) anlayabilen ve yeni teknolojilere hızla uyum sağlayabilen yüksek vasıflı bireyler gerektirmektedir. Bu, kuruluşların agresif işe alım, elde tutma ve sürekli, hedefe yönelik eğitime [5] – temel "YZ eğitimi, yönergeleri veya politikaları" dahil [6] – öncelik vermesi gerektiği anlamına gelir; bu da gelişmiş araçlardan yararlanabilecek ve onları optimize edebilecek dayanıklı ve adaptif bir insan

savunma katmanı oluşturmak için hayati önem taşır.

Gelişen Şifreleme Standartları ve Görünürlük Üzerindeki Etkileri

SSL/TLS ve ardıllarının yaygın olarak benimsenmesi, ağ iletişimlerinde verileri korumak için şifrelemeyi kullanıma sokar, ancak bu aynı zamanda verileri geleneksel ağ ve güvenlik analizinden gizler.[27] QUIC gibi yeni protokoller ve 5G'nin artan kullanımı, yeni şifreleme katmanları ve trafik modelleri sunarak derin paket incelemesini daha da karmaşık hale getirmektedir.[1] Şifreleme doğası gereği iki ucu keskin bir kılıçtır: meşru trafik için kritik veri koruması sağlar, ancak aynı zamanda kötü amaçlı etkinlik için önemli bir örtü sunar, bu da savunmacıların ağda neler olup bittiğini "görmesini" zorlaştırır.[27] Wireshark QUIC/5G için yerel destek kazanırken [1] ve oturum anahtarlarıyla şifre çözme yetenekleri sunarken [10], bu anahtarları büyük ölçekte elde etmek veya tam şifre çözme olmadan etkili analiz yapmak [27] önemli bir teknik ve bazı bağlamlarda yasal/etik bir zorluk olmaya devam etmektedir. Bu durum, 2025'te "oyuncu avcılığının", ağ yüklerine tam görünürlüğün giderek zorlaştığı karmaşık bir ortamda gezinmesi gerektiğini göstermektedir. Kuruluşların, ya büyük ölçekte şifre çözmeyi yönetebilecek (örneğin, SSL inceleme cihazları aracılığıyla) ya da meta verilerden ve davranışsal modellerden (örneğin, JA3/JA4, akış analizi) kötü amaçlılığı çıkarabilecek çözümlere yatırım yapması gerekmektedir, yalnızca derin yük incelemesine güvenmek yerine. Bu devam eden zorluk, güvenlik amaçlı trafik şifre çözme ile bireysel gizlilik endişeleri arasındaki tartışmayı da yoğunlaştırmaktadır.

Hibrit, Çoklu Bulut ve Birleşik BT/OT/IoT Ortamlarının Karmaşıklığı

Çoklu buluta hızlanan geçiş [7], uç bilişimin yaygınlaşması [21] ve IoT/OT/IoMT cihazlarının katlanarak büyümesi [4] topluca oldukça dağıtık, heterojen ve dinamik ağ ortamları yaratmaktadır. Kritik bir sorun, mevcut birçok güvenlik çözümünün bu çeşitli BT, IoT, OT ve IoMT alanlarında "silolar halinde çalışmaya devam etmesi ve tehlikeli kör noktalar bırakmasıdır".[8] Modern ağların (geleneksel BT, bulut, uç, IoT, OT ve IoMT'yi kapsayan) çeşitli ve birbirine bağlı yapısı, tehditlerin artık tek alanlarla sınırlı olmadığı ve daha önce ayrılmış ortamlar arasında hızla geçiş yapabileceği anlamına gelmektedir.[8] Bu karmaşık ortamlar arasında güvenliği etkili bir şekilde yönetmek doğası gereği zordur ve silolanmış güvenlik çözümleri açıkça önemli bir zayıflık olarak tanımlanmaktadır.[8] Bu

durum, 2025'te etkili "oyuncu avcılığının" tüm dijital ekosistemde bütünsel ve birleşik bir görünüm gerektirdiğini göstermektedir. Wireshark, ayrıntılı paket düzeyinde güçlü olsa da, çeşitli kaynaklardan (ağ trafiği, uç nokta günlükleri, bulut günlükleri, OT protokolleri, sistem çağrıları) verileri ilişkilendirebilen daha geniş gözlemlenebilirlik platformlarına entegre edilmelidir. Zorluk sadece bir segmentten gelen trafiği analiz etmek değil, karmaşık saldırı yollarını doğru bir şekilde izlemek ve tüm işletme genelinde yanal hareketi belirlemek için farklı ağ alanları arasındaki

ilişkileri, *bağımlılıkları* ve *ara bağlantıları* anlamaktır.

YZ Destekli Siber Saldırılarla Silahlanma Yarışı

YZ, saldırganlar tarafından daha güçlü kötü amaçlı yazılımlar, sofistike fidye yazılımları ve son derece yenilikçi kimlik avı şemaları geliştirmek için aktif olarak kullanılmakta, saldırıların etkinliğini ve inandırıcılığını artırmaktadır.[4] Saldırganlar, geleneksel güvenlik önlemlerinin meşru ve kötü amaçlı eylemleri ayırt etmesini zorlaştırmak için YZ'yi kullanarak normal kullanıcı etkinliğini taklit etmektedir.[24] YZ destekli siber saldırıların sürekli ve hızlı evrimi, statik, reaktif güvenlik önlemlerinin hızla eskidiği anlamına gelmektedir. Kaynaklar, güvenlik savunmalarının da bu ortaya çıkan tehditlere karşı sürekli olarak uyum sağlaması ve YZ'den yararlanması gerektiğini sürekli olarak vurgulamaktadır.[24] Bu dinamik etkileşim, açıkça devam eden bir "silahlanma yarışı" olarak karakterize edilmektedir.[6] Bu durum, "oyuncu avcılığının" statik bir teknikler bütünü değil, sürekli gelişen ve son derece dinamik bir disiplin olduğunu ima etmektedir. Kuruluşlar, sürekli öğrenme, yeni saldırı vektörlerine yönelik proaktif araştırma ve yeni tespit ve yanıt yeteneklerinin hızlı bir şekilde dağıtılması kültürünü teşvik etmelidir. Bu, yeni siber tehditlerin önünde kalmak için güvenlik duruşlarını proaktif olarak geliştirebilen, avcılık metodolojilerini uyarlayabilen ve YZ'den yararlanabilen dayanıklı sistemler ve çevik ekipler oluşturmakla ilgilidir; bu da uzun vadeli kurumsal dayanıklılığı sağlar.[24]

5. Stratejik Uygulama İçin Öneriler

Entegre Güvenlik Platformlarına Yatırım (SOAR, UEBA, NDR)

Wireshark'ın derin paket analizi yeteneklerini Güvenlik Orkestrasyonu, Otomasyonu ve Yanıtı (SOAR) platformlarıyla entegre etmek, olay müdahalesini otomatikleştirmek, tehdit istihbaratı zenginleştirmesini artırmak ve uyarı triyajını düzene sokmak için kritik öneme sahiptir.[25] SOAR pazarının hızla büyümesi, bunun gerekliliğini vurgulamaktadır.[32] YZ/ML kullanan Kullanıcı ve Varlık Davranış Analitiği (UEBA) sistemlerinden yararlanmak, kullanıcı ve varlık davranışını anormallikler açısından izleyerek, geleneksel imza tabanlı tespiti atlatabilecek iç tehditleri ve tehlikeye atılmış hesapları etkili bir şekilde belirler.[22] Endüstriyel ve tescilli protokolleri ayrıştırabilen Ağ Tespit ve Yanıt (NDR) araçlarını benimsemek, karmaşık IoT/OT ortamlarına temel görünürlük sağlar.[38] Tekil çözümlerin yetersiz olduğu bir gerçektir. Entegre platformlar, birleşik bir görünüm sağlar, iş akışlarını otomatikleştirir ve korelasyonu iyileştirir. Bu, "oyuncu avcılarının" reaktif yangın söndürmeden proaktif, stratejik savunmaya geçmesine olanak tanır.

Yetenek Geliştirme ve İnsan-YZ İşbirliğine Öncelik Verme

Ağ adli bilişimi, YZ/ML, bulut güvenliği ve IoT/OT protokolleri için sürekli eğitime yatırım yaparak yetenek açığını kapatmak gerekmektedir.[7] Wireshark özelleştirmesi ve otomasyonu için betikleme becerilerini (Lua, Python) geliştirmeye vurgu yapılmalıdır.[10] YZ'nin tekrarlayan görevleri ele aldığı ve anormallikleri işaretlediği, insan uzmanlarının ise derinlemesine analiz ve doğrulama yaptığı bir insan-YZ işbirliği kültürü teşvik edilmelidir.[24] Geleceğin analisti sadece bir araç kullanıcısı değil, aynı zamanda bir geliştirici ve stratejisttir. Teknik derinlik, programlama yeteneği ve analitik düşünmenin bu birleşimi çok önemlidir. İnsan-YZ işbirliği, verimliliği ve etkinliği en üst düzeye çıkararak analistlerin karmaşık, nüanslı tehditlere odaklanmasını sağlar.

Kapsamlı Veri Yakalama ve Yönetim Stratejileri Uygulama

Büyük hacimli ağ trafiği verilerini yakalamak ve depolamak için sağlam, ölçeklenebilir çözümler (dumpcap, large-pcap-analyzer, Arkime gibi) önerilmektedir.[39] Etkili geri

çağırma ve analiz için, uygun indeksleme ve meta veri etiketleme dahil olmak üzere yapılandırılmış veri yönetimine vurgu yapılmalıdır.[39] Şifreli trafiği ele almak için, seçici şifre çözme (yasal ve etik olarak izin verilen yerlerde) ve meta veri analizi (örneğin, JA3/JA4 parmak izi çıkarma) dahil olmak üzere stratejiler geliştirilmelidir.[10] Yüksek doğruluklu veriler temel taşıdır. Etkili veri yönetimi, "oyuncu avcılarının" ölçek veya şifreleme ne olursa olsun gerekli bilgilere hızlı ve verimli bir şekilde erişmesini sağlar. Bu proaktif veri stratejisi, ham ağ trafiğini kalıcı, aranabilir bir adli kaynak haline getirir.

Proaktif, Tehdit Avcılığı Zihniyetini Benimseme

Reaktif olay müdahalesinden proaktif tehdit avcılığına geçiş teşvik edilmeli, ilk savunmaları atlatmış tehditler aktif olarak aranmalıdır.[3] Tehdit istihbaratına ve gözlemlenen ağ modellerine dayalı tehdit avcılığı hipotezlerinin formüle edilmesi desteklenmelidir.[37] Savunmaları test etmek ve avcılık tekniklerini iyileştirmek için, gelişmiş düşman TTP'lerini simüle etmek de dahil olmak üzere, düzenli olarak kırmızı takım tatbikatları ve simülasyonlar yapılmalıdır.[24] Güvenlik artık sadece duvar örmekle ilgili değil, aynı zamanda aktif olarak devriye gezmekle ilgilidir. Proaktif bir zihniyet, düzenli testlerle birleştiğinde, kuruluşların tespit yeteneklerini sürekli olarak geliştirmesini ve gelişen tehditlere uyum sağlamasını sağlayarak, ağı dinamik bir avlanma alanına dönüştürür.

Alanlar Arası İşbirliğini Teşvik Etme (BT/OT/IoT/Bulut)

Birleşik görünürlük ve tüm saldırı yüzeyinde koordineli yanıt sağlamak için BT, OT, IoT ve bulut güvenlik ekipleri arasındaki siloların yıkılması savunulmalıdır.[8] Alanlar arası tehdit anlayışını geliştirmek için paylaşılan istihbarat platformları ve ortak eğitim programları uygulanmalıdır.[7] Modern altyapının birbirine bağlı doğası, birleşik bir güvenlik stratejisi gerektirmektedir. İşbirliği, "oyuncu avcılarının" potansiyel saldırı yollarının tam bir resmine sahip olmasını ve farklı ağ segmentlerini aşan tehditlere etkili bir şekilde yanıt verebilmesini sağlayarak kör noktaları azaltır ve genel dayanıklılığı güçlendirir.

Alıntılanan çalışmalar

1. Top 10 best Free Cybersecurity Software for Researchers in 2025, erişim tarihi Haziran 16, 2025, https://top2percentscientists.com/best-free-cybersecurity-software-for-researchers/
2. How to Use Wireshark on Kali Linux (Beginner's Tutorial) in 2025 - YouTube, erişim tarihi Haziran 16, 2025, https://www.youtube.com/watch?v=Wo-U55Jar8s
3. Mastering Packet Analysis in Digital Forensics - Number Analytics, erişim tarihi Haziran 16, 2025, https://www.numberanalytics.com/blog/mastering-packet-analysis-digital-forensics
4. 9 cybersecurity trends to watch in 2025 – CyberCom | Digital Forensics Experts, erişim tarihi Haziran 16, 2025, https://cybercom.africa/9-cybersecurity-trends-to-watch-in-2025/
5. Top Cybersecurity Trends in 2025: 9 Trends to Watch | Splunk, erişim tarihi Haziran 16, 2025, https://www.splunk.com/en_us/blog/learn/cybersecurity-trends.html
6. 2025 Forensic Predictions - Security Metrics, erişim tarihi Haziran 16, 2025, https://www.securitymetrics.com/blog/2025-forensic-predictions
7. Everything You Need To Know About Cyber Threat Intelligence, erişim tarihi Haziran 16, 2025, https://cyble.com/knowledge-hub/cyber-threat-intelligence-2025/
8. Forescout's 2025 report reveals surge in device vulnerabilities ..., erişim tarihi Haziran 16, 2025, https://industrialcyber.co/reports/forescouts-2025-report-reveals-surge-in-device-vulnerabilities-across-it-iot-ot-and-iomt/
9. 2025 Cybersecurity Threats - PacketWatch, erişim tarihi Haziran 16, 2025, https://packetwatch.com/resources/blog/2025-cybersecurity-threats?hsLang=en
10. How Is Wireshark Used in Cybersecurity?, erişim tarihi Haziran 16, 2025, https://kings-guard.com/how-is-wireshark-used-in-cybersecurity/
11. How to use Wireshark for monitoring network activity in Cybersecurity | LabEx, erişim tarihi Haziran 16, 2025, https://labex.io/tutorials/wireshark-how-to-use-wireshark-for-monitoring-network-activity-in-cybersecurity-415120
12. Chapter 1. Introduction - Wireshark, erişim tarihi Haziran 16, 2025, https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html
13. PP062: Hunting for Host Security and Performance Issues with Stratoshark | Packet Pushers, erişim tarihi Haziran 16, 2025, https://packetpushers.net/podcasts/packet-protector/pp062-hunting-for-host-security-and-performance-issues-with-stratoshark/
14. New Stratoshark by Sysdig extends Wireshark capabilities to the cloud | SC Media, erişim tarihi Haziran 16, 2025, https://www.scworld.com/brief/new-stratoshark-by-sysdig-extends-wireshark-capabilities-to-the-cloud
15. Stratoshark: Extending Wireshark's legacy into the cloud | Sysdig, erişim tarihi Haziran 16, 2025, https://sysdig.com/blog/stratoshark-extending-wiresharks-legacy-into-the-cloud

/
16. Wireshark for Security Professionals, erişim tarihi Haziran 16, 2025, https://computerscience.unicam.it/marcantoni/reti/laboratorio_wireshark/Wireshark%20for%20Security%20Professionals%20-%20Using%20Wireshark%20and%20the%20Metasploit%20Framework.pdf
17. Lua/Examples - Wireshark Wiki, erişim tarihi Haziran 16, 2025, https://wiki.wireshark.org/Lua/Examples
18. A systematic literature review of unsupervised learning algorithms ..., erişim tarihi Haziran 16, 2025, https://arxiv.org/pdf/2503.08293
19. mayanknauni/Wireshark-Capture-Anomaly-Detection - GitHub, erişim tarihi Haziran 16, 2025, https://github.com/mayanknauni/Wireshark-Capture-Anomaly-Detection
20. HYBRID MODEL OF NETWORK ANOMALIES DETECTION USING ..., erişim tarihi Haziran 16, 2025, https://science.lpnu.ua/ictee/all-volumes-and-issues/volume-5-number-1-2025/hybrid-model-network-anomalies-detection-using
21. 8 Trends That Will Define Networking in 2025 and Beyond - PacketFabric, erişim tarihi Haziran 16, 2025, https://packetfabric.com/blog/8-trends-that-will-define-networking-in-2025-and-beyond
22. What is User and Entity Behavior Analytics (UEBA)? - CrowdStrike.com, erişim tarihi Haziran 16, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/identity-protection/user-and-entity-behavior-analytics-ueba/
23. What is User Behavior Analytics? - CyberArk, erişim tarihi Haziran 16, 2025, https://www.cyberark.com/what-is/user-behavior-analytics/
24. Behavioral analytics based on AI can stop cyberattacks before they ..., erişim tarihi Haziran 16, 2025, https://www.scworld.com/perspective/behavioral-analytics-based-on-ai-can-stop-cyberattacks-before-they-occur
25. Top 10 SOAR Platform Use Cases in 2025 for Cybersecurity - Securaa, erişim tarihi Haziran 16, 2025, https://securaa.io/top-10-use-cases-for-a-soar-platform-in-2025/
26. What is Device Fingerprinting? How Does It Fight Fraud? - FOCAL, erişim tarihi Haziran 16, 2025, https://www.getfocal.ai/knowledgebase/what-is-device-fingerprinting
27. Decoding Cyber Threats: Wireshark Tips and Tricks for Analyzing Suspicious Traffic Patterns - PacketFest, erişim tarihi Haziran 16, 2025, https://packetfest.ntop.org/slides/Hofstetter.pdf
28. What is Cloud Forensics? | CrowdStrike, erişim tarihi Haziran 16, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/cloud-forensics/
29. Top 15 Kubectl plugins for security engineers in 2025 - Sysdig, erişim tarihi Haziran 16, 2025, https://sysdig.com/blog/top-15-kubectl-plugins-for-security-engineers/

30. Top 10 Network Monitoring Tools for Optimal Performance (2025), erişim tarihi Haziran 16, 2025, https://www.cloudnuro.ai/blog/top-10-network-monitoring-tools-for-optimal-performance-2025
31. 16 Best Network Monitoring Tools in 2025 - 10XSheets, erişim tarihi Haziran 16, 2025, https://www.10xsheets.com/blog/best-network-monitoring-tools/
32. Security Orchestration, Automation And Response Market Statistics 2025, erişim tarihi Haziran 16, 2025, https://www.thebusinessresearchcompany.com/market-insights/security-orchestration-automation-and-response-market-overview-2025
33. How to Write Wireshark Dissector - Sewio RTLS, erişim tarihi Haziran 16, 2025, https://www.sewio.net/open-sniffer/develop/how-to-write-wireshark-dissector/
34. 9.2. Adding a basic dissector - Wireshark, erişim tarihi Haziran 16, 2025, https://www.wireshark.org/docs/wsdg_html_chunked/ChDissectAdd.html
35. 19 Best IoT Testing Tools Reviewed in 2025 - The CTO Club, erişim tarihi Haziran 16, 2025, https://thectoclub.com/tools/best-iot-testing-tools/
36. Wireshark Basics for IoT Hacking - YouTube, erişim tarihi Haziran 16, 2025, https://www.youtube.com/watch?v=8vYyHZpplqE
37. PipeDream/InController: From High-Level Alert to Hands-On Threat Hunting - Insane Cyber, erişim tarihi Haziran 16, 2025, https://insanecyber.com/pipedream-incontroller-from-high-level-alert-to-hands-on-threat-hunting/
38. Best Practices to Secure IoT Devices in 2025 - Sattrix, erişim tarihi Haziran 16, 2025, https://www.sattrix.com/blog/iot-security-best-practices-2025/
39. Tools - Wireshark Wiki, erişim tarihi Haziran 16, 2025, https://wiki.wireshark.org/Tools
40. LEARN Wireshark with this Full course Tutorial 2025 - YouTube, erişim tarihi Haziran 16, 2025, https://www.youtube.com/watch?v=1VmTk2UlpLY
41. 14 - A traffic analysis of IoT Devices in Wireshark - YouTube, erişim tarihi Haziran 16, 2025, https://www.youtube.com/watch?v=oMfDWzURUx0
42. Top 5 Network Traffic Analysis Software in 2025 - Research AIMultiple, erişim tarihi Haziran 16, 2025, https://research.aimultiple.com/network-traffic-analysis-software/
43. Digital Forensics Round-Up, March 26 2025, erişim tarihi Haziran 16, 2025, https://www.forensicfocus.com/news/digital-forensics-round-up-march-26-2025/
44. Analyzing a packet capture using Wireshark - Search - Informatica, erişim tarihi Haziran 16, 2025, https://knowledge.informatica.com/s/article/Analyzing-a-packet-capture-using-Wireshark?language=en_US