Proaktif Tehdit Avcılığı: 2025 ve Ötesi İçin Ağ Güvenliği Analizi Stratejileri

Giriş: Siber Savunmada Paradigma Değişimi

Geleneksel, çevre tabanlı ve reaktif güvenlik anlayışının geçerliliğini yitirdiği bir döneme girmiş bulunmaktayız. Ağ çevresinin çözülmesi, yapay zekanın (AI) hasımlar tarafından bir silah olarak kullanılması ve hibrit çalışma modellerinin entegrasyonu gibi faktörlerle karakterize edilen modern tehdit manzarası, siber savunmada temel bir paradigma değişimini zorunlu kılmaktadır. Bu yeni dönemde proaktif tehdit avcılığı, artık gelişmiş bir yetenek olmaktan çıkıp, kurumsal beka için temel bir gereklilik haline gelmiştir. Bu rapor, 2025 ve sonrası için ağ güvenliği analizindeki en etkili teknikleri ve eğilimleri derinlemesine inceleyerek, proaktif tehdit avcılığı programlarının temelini oluşturacak stratejik bir yol haritası sunmaktadır.

Bu değişimin merkezinde, yeni "Kutup Yıldızı" olarak konumlandırılan **Siber Dayanıklılık (Cyber Resilience)** kavramı yer almaktadır.[1] Artık başarı, sadece olayların önlenmesiyle değil, bir kurumun saldırıları ne kadar etkin bir şekilde öngörebildiği, bunlara karşı koyabildiği, bunlardan kurtulabildiği ve bunlara adapte olabildiğiyle ölçülmektedir. "Sıfır hata toleransı" zihniyetinin, sürdürülebilir risk azaltımı sağlama konusunda zirveye ulaştığı ve güvenlik ekiplerinin tükenmişlik riskini artırmaktan başka bir işe yaramadığı giderek daha fazla kabul görmektedir.[1] Bu rapor, takip eden teknik tartışmaları bu stratejik dayanıklılık ve proaktif angajman bağlamında çerçeveleyecektir.

Bu paradigma değişimini tetikleyen temel faktörler üç ana başlık altında toplanabilir:

- **Teknolojik Tetikleyiciler:** Düşmanlar tarafından kullanılan yapay zeka güdümlü saldırıların artan karmaşıklığı, ağ trafiğinin neredeyse tamamını kapsayan şifreleme ve Bilgi Teknolojileri (IT), Operasyonel Teknolojiler (OT) ve Nesnelerin İnterneti (IoT) yakınsamasıyla saldırı yüzeyinin patlama noktasına gelmesi, geleneksel savunma mekanizmalarını yetersiz kılmaktadır.[2]
- **İş Odaklı Tetikleyiciler:** Güvenliğin bir engelleyici değil, bir iş kolaylaştırıcı olarak

konumlandırılması gerekliliği ve siber suçların maliyetinin 2025 yılına kadar 12 trilyon ABD dolarına ulaşacağı öngörüsü, siber güvenliğin artık bir yönetim kurulu seviyesinde öncelik olmasını zorunlu kılmaktadır.[1]
- **Operasyonel Tetikleyiciler:** Araç karmaşası, uyarı yorgunluğu ve güvenlik ekibi tükenmişliği gibi sorunlarla boğuşan geleneksel Güvenlik Operasyon Merkezi (SOC) modelinin sürdürülemezliği, daha akıllı, daha otomatize ve daha proaktif yaklaşımları gerektirmektedir.[1]

Bu rapor, bu zorluklara yanıt olarak geliştirilen ve 2025 ve ötesinde proaktif tehdit avcılığının temelini oluşturacak olan en önemli 10 strateji ve teknolojiyi ayrıntılı bir şekilde analiz edecektir.

Bölüm I: Modern Proaktif Güvenliğin Temel Dayanakları

Bu bölüm, belirli avcılık araçları veya teknikleri etkin bir şekilde uygulanmadan önce gerekli olan, pazarlığa kapalı stratejik ve mimari temelleri oluşturmaktadır.

Bölüm 1: Yönetişim Zorunluluğu: NIST CSF 2.0 ile Güvenliğin İş Stratejisiyle Hizalanması

Herhangi bir proaktif güvenlik programı için en kritik başlangıç noktası, NIST Siber Güvenlik Çerçevesi'nin (CSF) 2024 güncellemesidir. NIST CSF 2.0'a **"Yönet (Govern - GV)"** fonksiyonunun eklenmesi, siber güvenliğin artık finansal ve itibar riskiyle eşdeğer, yukarıdan aşağıya yönetilmesi gereken birincil bir iş riski olduğunun resmi olarak tanınması anlamına gelmektedir.[7] Bu fonksiyon, proaktif tehdit avcılığı çabalarının keyfi ve reaktif olmaktan çıkıp, doğrudan iş hedeflerine hizmet eden stratejik bir faaliyete dönüşmesini sağlar.

Yönet Fonksiyonunun Analizi

Yönet fonksiyonu, diğer beş fonksiyonu (Tanımla, Koru, Tespit Et, Müdahale Et, Kurtar)

destekleyen ve onlara stratejik bir yön veren kesişimsel bir katmandır. Bu fonksiyonun altı kategorisi, proaktif bir avcılık programı için doğrudan bir anlam ifade etmektedir [7]:

- **GV.OC (Kurumsal Bağlam):** Kurumun misyonunu anlamak ve bu misyonu engelleyebilecek riskleri belirlemek. Bu, tehdit avcılarının ne araması gerektiğini doğrudan bilgilendirir.
- **GV.RM (Risk Yönetimi Stratejisi):** Risk toleransını ve iştahını belirlemek. Bu, avcılık ve müdahale için "angajman kurallarını" tanımlar.
- **GV.RR (Roller, Sorumluluklar ve Yetkiler):** Hesap verebilirliği teşvik etmek ve kimin ne yapacağını tanımlamak, ki bu da verimli bir avcılık ekibi için kritik öneme sahiptir.
- **GV.PO (Politika):** Avcılık faaliyetlerine rehberlik eden yerleşik siber güvenlik politikalarını uygulamak.
- **GV.OV (Gözetim):** Stratejiyi bilgilendirmek ve ayarlamak için performans metriklerini kullanmak, avcılık programının ölçülebilir değer sunmasını sağlamak.
- **GV.SC (Siber Güvenlik Tedarik Zinciri Risk Yönetimi):** Tedarik zincirinin birincil bir saldırı vektörü olduğunu kabul etmek ve bu alana özel avcılık odağı gerektirmek.[11]

Yönetişimin Proaktif Avcılığa Bağlanması

Yönet fonksiyonu, tehdit avcılığı ekibi için temel "neden" ve "ne" sorularını yanıtlar. Bu stratejik yönlendirme olmadan, tehdit avcılığı amaçsız, reaktif ve yalnızca teknik odaklı bir egzersiz haline gelir. Yönetişim, avcılık çabalarının kurumun misyonuna en büyük riski teşkil eden unsurlara göre önceliklendirilmesini sağlar.[12]

Yönet fonksiyonunun uygulanması, yalnızca bir uyumluluk faaliyeti olmanın ötesinde, Gartner'ın 2025 için en önemli trendlerden biri olarak belirlediği güvenlik ekibi tükenmişliğiyle mücadele etmenin ve bir "dayanıklılık kültürü" oluşturmanın birincil mekanizmasıdır. Tükenmişliğin temel nedenleri arasında genellikle net önceliklerin olmaması, ezici uyarı hacmi ve güvenlik çabalarının iş hedefleriyle uyumlu olmadığı veya değer görmediği hissi bulunur.[1] NIST CSF 2.0'ın "Yönet" fonksiyonu, bu kök nedenlere doğrudan yapısal bir çözüm sunar. Üst yönetimi net bir risk yönetimi stratejisi (GV.RM) oluşturmaya, rolleri ve sorumlulukları (GV.RR) tanımlamaya ve gözetim (GV.OV) sağlamaya zorlar.[9] Bu yukarıdan aşağıya stratejik netlik, güvenlik ekibinin misyonunu "her şeyi önlemek" gibi imkansız ve tükenmişliğe yol açan bir görevden, "iş önceliklerine göre riski yönetmek" gibi daha anlamlı ve ulaşılabilir bir

hedefe dönüştürür. Dolayısıyla, Yönet fonksiyonunu uygulamak, tek başına "sağlık" programlarından çok daha etkili bir şekilde amaç, netlik ve yönetici desteği sağlayarak dayanıklılık inşa eder ve tükenmişlikle ilgili temel insani sorunu çözer.

Bölüm 2: Mimari Doktrin Olarak Sıfır Güven: Yutturmacanın Ötesinde Pratik Uygulama

Sıfır Güven Mimarisi (Zero Trust Architecture - ZTA), "Yönet" fonksiyonunun stratejik niyetinin mantıksal mimari tezahürü olarak konumlandırılmalıdır. Eğer yönetişim kuralları tanımlıyorsa, ZTA bu kuralları sürekli olarak uygulayan sistemdir. Bu bölümde, ZTA'yı bir moda sözcük olmanın ötesine taşıyarak, konumundan veya önceki doğrulamalarından bağımsız olarak hiçbir kullanıcıya veya cihaza varsayılan olarak güvenilemeyeceği inancına dayanan bir güvenlik modeli olarak sunacağız.[14]

NIST SP 800-207 ve SP 1800-35'ten Yararlanma

Bu bölüm, NIST'in temel ZTA belgelerine yoğun bir şekilde atıfta bulunacaktır. SP 800-207'deki temel kavramları açıkladıktan sonra, Haziran 2025'te yayınlanan yeni SP 1800-35'in, ticari olarak temin edilebilen 19 pratik uygulama örneği sunarak ZTA'yı her zamankinden daha erişilebilir hale getirdiğini göstereceğiz.[14] Bu yeni kılavuz, kuruluşlara kendi ZTA'larını oluşturmaları için değerli başlangıç noktaları sunarak teoriyi pratiğe dökmektedir.

Tehdit Avcılığı için Bir Kolaylaştırıcı Olarak ZTA

Bir ZTA ortamı, doğası gereği daha "avlanabilir" bir yapıdadır. Tasarım gereği, her erişim talebinin açıkça doğrulanması gerektiğinden, kullanıcı ve cihaz davranışları hakkında zengin telemetri ve günlükler üretir. Bu, avcılara analiz için bir veri hazinesi sağlar. Ayrıca, ZTA yanal hareketi önleyerek saldırganları sınırlar ve ağ içinde hareket etmeye çalıştıkça daha fazla "gürültü" üretmeye zorlar, bu da onların tespit edilmesini

kolaylaştırır.[14]

Pratik ZTA Modelleri

NIST kılavuzunda özetlenen Gelişmiş Kimlik Yönetişimi (Enhanced Identity Governance - EIG), Yazılım Tanımlı Çevre (Software-Defined Perimeter - SDP) ve mikro segmentasyon gibi farklı ZTA oluşturma türlerini tartışarak, her birinin kuruluşlar için nasıl bir başlangıç noktası olabileceğini açıklayacağız.[15]

Sıfır Güven Mimarisi'nin uygulanması, XDR ve UEBA gibi gelişmiş, yapay zeka destekli güvenlik platformlarının etkin kullanımı için bir ön koşuldur. Bu araçları geleneksel, çevre tabanlı bir ağ üzerinde dağıtmaya çalışmak, yüksek performanslı bir motoru kirli yakıtla çalıştırmaya benzer. Geleneksel bir ağ mimarisi, örtük güven üzerine kuruludur; çevre içine girildiğinde, bir kullanıcı veya cihaz geniş erişime sahip olur ve günlük kaydı tutarsız olabilir. XDR ve UEBA gibi gelişmiş araçlar ise büyük miktarda veri alarak ve normalden sapan anormal davranışları belirlemek için AI/ML kullanarak çalışır.[17] Geleneksel bir ağda, yüksek derecede örtük güven ve izlenmeyen faaliyetler nedeniyle güvenilir bir "normal" davranış taban çizgisi oluşturmak son derece zordur; veri gürültülü ve eksiktir. Buna karşılık, bir ZTA, açık güven ilkesiyle çalışır. Bir kaynağa yapılan her erişim talebi doğrulanmalı ve yetkilendirilmelidir. Bu, kimin, nereden, ne zaman ve neye eriştiği hakkında sürekli, yüksek kaliteli ve ayrıntılı bir veri akışı üretir.[14] ZTA'dan gelen bu zengin, temiz ve kapsamlı telemetri, XDR ve UEBA platformları için ideal "yakıt"tır. Çok daha doğru taban çizgileri oluşturmalarını sağlayarak daha yüksek doğrulukta tespitlere ve daha az yanlış pozitif sonuca yol açar. Bu nedenle, ZTA sadece paralel bir güvenlik girişimi değil, yeni nesil, AI güdümlü tehdit tespiti ve avcılık araçlarının tam potansiyelini ortaya çıkaran temel veri üretim katmanıdır.

Bölüm II: Proaktif Tehdit Avcılığı için En İyi 10 Teknik ve Trend (2025+)

Bu, raporun özünü oluşturan ve her bir eğilimin entegre bir analizle derinlemesine incelendiği bölümdür.

1. Yapay Zeka Destekli Proaktif Savunma: Saldırı Yüzeyi Yönetimi (ASM) ve Tahminsel Analitiğin Yakınsaması

Bu eğilim, periyodik zafiyet taramasından, internete açık ve dahili tüm varlıkları sürekli olarak keşfetme, analiz etme ve izleme sürecine, yani kurumu bir saldırganın gözünden görme sürecine geçişi temsil etmektedir.[19] Bu, reaktif savunmadan proaktif bir stratejiye geçişin somut bir örneğidir.

Yapay Zekanın Rolü

Yapay zeka (AI) ve makine öğrenimi (ML), Saldırı Yüzeyi Yönetimi'ni (Attack Surface Management - ASM) manuel, emek yoğun bir görevden otomatikleştirilmiş, akıllı bir sürece dönüştürmektedir. AI güdümlü platformlar şunları yapabilir:

- **Otomatik Keşif:** Gölge BT (Shadow IT) ve yanlış yapılandırılmış bulut ortamları da dahil olmak üzere tüm dijital varlıkları sürekli olarak tarar ve haritalar.[20]
- **Risk Önceliklendirme:** Yalnızca CVSS puanlarına değil, aynı zamanda iş bağlamına, varlık kritikliğine ve aktif sömürü kanıtlarına dayalı olarak zafiyetleri önceliklendirmek için AI güdümlü analitikleri kullanır.[23]
- **Tahminsel Öngörüler Sağlama:** Potansiyel saldırı vektörlerini sömürülmeden önce tahmin etmek için büyük veri setlerini analiz ederek gerçek proaktif savunmayı mümkün kılar.[19]

Entegrasyon ve Uygulama

ASM, tek başına bir araç değildir. Diğer güvenlik fonksiyonlarıyla entegre olur ve onlara kritik bağlam sağlar. Örneğin, ASM verileri XDR araştırmalarını zenginleştirir ve yama yönetimi çabalarını önceliklendirmeye yardımcı olur.[24] Küresel ASM pazarının 2025'te yaklaşık 1 milyar ABD dolarından 2032'ye kadar 4 milyar ABD dolarının üzerine çıkması ve %22.6'lık bir bileşik yıllık büyüme oranı (CAGR) sergilemesi beklenmektedir, bu da büyük bir yatırım ve benimseme eğilimini göstermektedir.[25]

Yapay zeka destekli ASM'nin yükselişi, geleneksel varlık yönetiminin bulut çağında başarısız olmasına doğrudan bir yanıttır. Bulut altyapısının dinamik, geçici ve geliştirici odaklı doğası, manuel veya periyodik envanter tutmayı imkansız hale getirerek, yalnızca sürekli ve otomatik keşfin kapatabileceği bir "görünürlük boşluğu" yaratmaktadır. Geleneksel varlık yönetimi, nispeten statik varlıklara sahip şirket içi veri merkezleri için tasarlanmıştı. Bulutun benimsenmesi, hibrit çalışma ve IoT, liderlerin %43'üne göre "kontrolsüz bir şekilde büyüyen" bir dijital saldırı yüzeyi yaratmıştır.[25] Büyük işletmelerde saldırı yüzeyinin %50'ye kadarı bilinmemekte veya güvenlik ekipleri tarafından görülememektedir.[25] Bu "görünürlük boşluğu", birçok güvenlik programındaki en büyük zayıflıktır; çünkü görülemeyen şey korunamaz. AI destekli ASM, bu sorunu çözmek için özel olarak tasarlanmıştır. Konumdan bağımsız olarak tüm varlıkların gerçek zamanlı bir envanterini oluşturmak için sürekli, otomatik keşif teknikleri (IP taramaları, pasif algılama, API entegrasyonları) kullanır.[24] Bu nedenle, ASM sadece zafiyet yönetiminde kademeli bir iyileştirme değil; çevresiz, bulut merkezli bir dünyada görünürlüğü ve kontrolü yeniden kazanma zorunluluğundan doğan temelden yeni bir yaklaşımdır. Herhangi bir proaktif güvenlik programının temel adımıdır.

2. Birleşik SOC Platformu: Hiper-Otomasyon için XDR, SIEM ve SOAR Entegrasyonu

Bu eğilim, Gartner tarafından belirlenen "daha az araç karmaşası, daha fazla platform gücü" paradigmasını ele almaktadır.[1] Kuruluşlar, düzinelerce bağlantısız nokta çözümünü yönetmekten uzaklaşarak veri, analitik ve müdahale yeteneklerini birleştiren entegre platformlara yönelmektedir.

XDR'ın Rolü

Genişletilmiş Tespit ve Müdahale (Extended Detection and Response - XDR), bu eğilimin merkezinde yer alır. Uç Nokta Tespiti ve Müdahalesi'nden (Endpoint Detection and Response - EDR) evrilerek, çok daha geniş bir kaynak yelpazesinden tehdit verilerini toplar ve ilişkilendirir: uç noktalar, bulut iş yükleri, ağ trafiği, e-posta ve kimlik sistemleri.[17] Bu, birden fazla araç arasında parçalanmış olacak bir saldırı zincirinin birleşik bir görünümünü sağlar.

Platform Mimarisi

Palo Alto Networks (Cortex XSIAM) ve CrowdStrike (Falcon) gibi satıcılar tarafından öngörülen modern bir birleşik platform, birkaç temel işlevi bir araya getirir [28]:

- **XDR:** Alanlar arası veri toplama ve korelasyon için.
- **Yeni Nesil SIEM:** Günlük yönetimi ve uyumluluk için.
- **SOAR (Güvenlik Orkestrasyonu, Otomasyonu ve Müdahalesi):** Araştırma ve müdahale oyun kitaplarını (playbook) otomatikleştirmek için.[31]
- **UEBA:** Davranışsal analiz ve içeriden gelen tehdit tespiti sağlamak için.

Tehdit Avcılığı için Faydaları

Bu birleşik yaklaşım, analistlere araştırma için tek bir konsol, güvenlik yığınının tamamından zenginleştirilmiş bağlam ve araç değiştirmeden müdahale eylemlerini yürütme yeteneği sunarak tehdit avcılığını önemli ölçüde geliştirir. Bu, Ortalama Tespit Süresini (MTTD) ve Ortalama Müdahale Süresini (MTTR) günler veya haftalardan dakikalara indirir.[17]

"Açık XDR" ve "Yerel XDR" arasındaki ayrım, "sınıfının en iyisi" esnekliği ile "tek satıcılı" entegrasyon verimliliği arasında temel bir seçimi yansıtan kritik bir stratejik karar noktasıdır. Bu seçimin maliyet, operasyonel karmaşıklık ve satıcıya bağımlılık üzerinde uzun vadeli etkileri vardır. XDR platformlarının birçok kaynaktan veri alması gerekir ve bu verileri nasıl elde ettikleri temel sorudur. **Yerel XDR** (örneğin, Palo Alto Networks veya Microsoft gibi tek bir büyük satıcıdan), kendi portföyündeki güvenlik araçlarını entegre eder. Avantajı, sıkı entegrasyon ve akıcı bir deneyimdir. Riski ise satıcıya bağımlılık ve satıcının belirli bir alandaki (örneğin, e-posta güvenliği) çözümünün sınıfının en iyisi olmaması durumunda potansiyel boşluklardır.[33]

Açık XDR (veya Forrester'ın adlandırdığı gibi Hibrit XDR), telemetri toplamak için üçüncü taraf entegrasyonlarına dayanır. Avantajı, bir kuruluşun mevcut "sınıfının en iyisi" araçlarını kullanmasına olanak tanıyan esnekliktir. Riski ise bu entegrasyonların karmaşıklığı ve potansiyel güvenilmezliğidir.[33] Bu seçim tamamen teknik değildir; stratejik bir karardır. Tek bir satıcının ekosistemine yoğun yatırım yapmış bir şirket, Yerel XDR'ı dağıtmayı daha kolay bulabilir. Esnekliğe değer veren ve çeşitli mevcut araçlara

sahip bir şirket, CrowdXDR Alliance tarafından savunulan gibi bir Açık XDR yaklaşımını tercih edebilir.[33] Bu nedenle, birleşik bir platformu benimserken, proje lideri yalnızca platformun özelliklerini değil, aynı zamanda entegrasyon felsefesini de değerlendirmelidir, çünkü bu, güvenlik mimarilerini ve satıcı ilişkilerini yıllarca şekillendirecektir.

3. Derinlemesine Aldatma (Deception-in-Depth): Pasif Savunmadan Aktif Düşman Angajmanına Geçiş

Aldatma teknolojisi, saldırganları cezbetmek, tespit etmek ve analiz etmek için yemler (honeypot'lar, sahte kimlik bilgileri, aldatıcı dosyalar vb.) kullanan proaktif bir savunma stratejisidir. Bir saldırıyı beklemek yerine, çekici, sahte bir hedef oluşturur.[34]

Tehdit Avcılığı için Nasıl Çalışır?

- **Yüksek Doğruluklu Uyarılar:** Bir yemle herhangi bir etkileşim, tanım gereği kötü niyetli veya yetkisizdir. Bu, diğer sistemleri rahatsız eden yanlış pozitifleri ortadan kaldırarak avcılara belirsiz, yüksek güvenilirlikli uyarılar sağlar.[36]
- **İstihbarat Toplama:** Aldatıcı ortamlar, yüksek düzeyde enstrümante edilmiş sanal alanlardır (sandbox). Güvenlik ekiplerinin bir saldırganın canlı TTP'lerini (Taktikler, Teknikler ve Prosedürler), araçlarını ve hedeflerini güvenli bir şekilde gözlemlemesine olanak tanır. Bu istihbarat, gerçek savunmaları güçlendirmek için paha biçilmezdir.[34]
- **Erken Tespit ve Yanal Hareket:** Sahte kimlik bilgilerini ekerek ve yemleri stratejik olarak yerleştirerek (örneğin, Active Directory'de), aldatma teknolojisi kimlik bilgisi hırsızlığını ve yanal hareket girişimlerini saldırı yaşam döngüsünün çok erken bir aşamasında tespit edebilir.[36]

AI Destekli Aldatma

Modern aldatma platformları, saldırganların tanımlaması daha zor olan daha gerçekçi ve uyarlanabilir yemler oluşturmak ve saldırgan davranışının analizini otomatikleştirmek

için yapay zeka kullanır.[34]

Aldatma teknolojisi, saldırgan-savunmacı asimetrisini temelden tersine çevirir. Geleneksel bir ağda, savunmacı %100 doğru olmak zorundayken, saldırganın yalnızca bir kez doğru olması yeterlidir. Aldatma özellikli bir ağda ise, saldırgan %100 doğru olmak (tüm yemlerden kaçınmak) zorundayken, savunmacının saldırganın yalnızca bir hata yapmasına ihtiyacı vardır. Geleneksel güvenlik modeli bir kale savunmasıdır; savunmacı duvarlar (güvenlik duvarları, EPP) inşa eder ve bunların dayanmasını umar. Saldırgan inisiyatife sahiptir ve tek bir zayıflık için yoklama yapabilir. Bu, saldırgan için asimetrik bir avantajdır. Aldatma teknolojisi, ağı bir mayın tarlası gibi yemlerle doldurur.[37] Çevreyi aşan bir saldırgan şimdi yeni bir zorlukla karşı karşıyadır: gördüklerine güvenemez. O dosya paylaşımı gerçek mi? O kimlik bilgisi geçerli mi? Her adım bir alarmı tetikleme riski taşır. Bu, saldırganı yavaş ve temkinli hareket etmeye zorlar veya anında tespit edilme riskini göze almasını gerektirir. Bu durum, "başarı yükünü savunmacı yerine saldırganın üzerine yıkar".[37] Bu nedenle, aldatma sadece başka bir tespit aracı değildir. Bir siber saldırının psikolojik ve operasyonel dinamiklerini değiştiren stratejik bir yetenektir. İnisiyatifi saldırgandan alır, onlara maliyet yükler ve savunmacının kendi ağını düşman için düşmanca bir ortama dönüştürür.

4. Şifreli Trafik Analizi (ETA): Gizlilik Odaklı Bir Dünyada Tehditleri Ortaya Çıkarma

İnternet trafiğinin %80'inden fazlasının artık şifreli olmasıyla, geleneksel derin paket incelemesi (DPI) kör kalmaktadır. Saldırganlar, Komuta ve Kontrol (C2) iletişimlerini, veri sızıntısını ve kötü amaçlı yazılım dağıtımını gizlemek için şifrelemeden yararlanmaktadır.[42]

Çözüm - ETA

Şifreli Trafik Analizi (Encrypted Traffic Analysis - ETA), şifreli trafiği **şifresini çözmeden** tehditleri belirlemek için analiz eden bir teknikler bütünüdür, böylece gizliliği korur. Bu genellikle meta verileri ve desenleri analiz eden ML modelleri kullanılarak yapılır.[44]

Anahtar ETA Teknikleri

- **İlk Veri Paketi (IDP) Analizi:** TLS el sıkışmasının kendisi, TLS sürümü, sunulan şifreleme takımları ve sertifika bilgileri gibi şifrelenmemiş meta veriler içerir. Buradaki anormallikler (örneğin, kendi kendine imzalanmış bir sertifika, zayıf şifreler) kötü niyetli faaliyetlerin göstergeleri olabilir.[45]
- **Paket Uzunlukları ve Zamanları Dizisi (SPLT):** Paketlerin boyutu, zamanlaması ve sırası, farklı uygulamalar ve faaliyetler için benzersiz bir parmak izi oluşturabilir. ML modelleri, zararsız trafiğin (örneğin, Google'da gezinme) SPLT profilini, kötü niyetli trafiğe (örneğin, C2 sinyalleşmesi veya veri sızıntısı) karşı öğrenebilir.[45]
- **Akış Veri Analizi:** Ağ cihazlarından (Cisco'nun uygulaması gibi) gelen gelişmiş NetFlow verilerini kullanarak, ETA, trafiği sınıflandırmak için bayt tahsislerini ve diğer akış özelliklerini analiz edebilir.[43]

Akademik Gelişmeler

Zengin bir akademik araştırma alanı, daha doğru ve sağlam sınıflandırma için Transformer'lar, GNN'ler ve LLM'ler gibi gelişmiş modelleri kullanarak ETA'nın sınırlarını zorlamaktadır.[46]

ETA'nın benimsenmesi sadece teknik bir seçim değil, aynı zamanda güvenlik ihtiyaçlarını artan gizlilik baskıları ve "kır ve denetle" şifre çözmenin operasyonel sürdürülemezliği ile dengeleyen stratejik bir karardır. Şifreli tehditlere karşı "bariz" çözüm, denetim için tüm trafiğin şifresini çözmektir ("ortadaki adam" yaklaşımı).[42] Ancak bu yaklaşım üç büyük engelle karşı karşıyadır:

Performans: Tüm trafiği hat hızında şifrelemek ve yeniden şifrelemek, hesaplama açısından pahalıdır ve ağ performansını düşürebilir. **Gizlilik/Yasal:** Özellikle GDPR gibi güçlü gizlilik yasalarına sahip bölgelerde kullanıcı trafiğinin şifresini çözmek, önemli yasal ve etik endişeler doğurur. **Teknik Kırılma:** Birçok modern uygulama, TLS oturumu kesintiye uğradığında bozulmalarına neden olan sertifika sabitleme (certificate pinning) ve diğer teknikleri kullanır. ETA bir "üçüncü yol" sunar. İçeriği görmeden şifreli trafiğin *davranışı* hakkında güvenlik görünürlüğü sağlar.[44] Bu, kuruluşların kullanıcı gizliliğine saygı duyarken, yasal engellerden kaçınırken ve ağ performansını korurken tehditleri tespit etmelerini sağlar. Bu nedenle, ETA, tüm durumlarda tam şifre çözmeden "daha iyi" olduğu için değil, kurumsal trafiğin büyük

çoğunluğu için en ölçeklenebilir, sürdürülebilir ve yasal olarak savunulabilir strateji olduğu için şifreli trafiği analiz etmede varsayılan yaklaşım haline gelmektedir.

5. Yeni Şantaj Ekonomisi: GenAI ile Güçlendirilmiş Bilgi Hırsızları ve Deepfake'lerle Mücadele

Forrester, 2025 yılı için tehdit manzarasında büyük bir değişim öngörmektedir. Fidye yazılımı ödemelerinin azalmasıyla birlikte, saldırganlar Üretken Yapay Zeka (Generative AI) ile güçlendirilmiş veri hırsızlığı ve şantaja yönelmektedir.[2]

Bir Saldırı Aracı Olarak GenAI

- **Şantaj için Veri Analizi:** Daha önce, milyonlarca e-postayı çalmak, suçlayıcı bilgileri bulmak için gereken zaman nedeniyle sınırlı bir değere sahipti. Şimdi, saldırganlar çalınan veriler üzerinde hızlı duygu analizi ve özetleme yapmak için GenAI kullanarak şantaj planları için kaldıraç bulabilirler.[2] Bu, "bilgi hırsızı" (infostealer) kötü amaçlı yazılımlarını fidye yazılımlarından daha büyük bir tehdit haline getirir.
- **Yüksek Kaliteli Deepfake'ler:** Açık kaynaklı araçların yaygınlaşması, son derece hedefli sosyal mühendislik ve dolandırıcılık için ikna edici deepfake ses ve video oluşturmayı kolay ve ucuz hale getirir.[2]
- **AI'ı İnsanlaştırma:** Çalışanların GenAI araçlarına aşırı güvenme eğilimi, veri sızıntısı ve manipülasyon riski yaratır.[2]

Avcılık Odağı

Tehdit avcıları adapte olmalıdır. Odak, şifreleme ikili dosyalarını (fidye yazılımı) aramaktan, bilgi hırsızlarının TTP'lerini, veri hazırlama ve sızdırma faaliyetlerini ve çalışanlar tarafından GenAI araçlarının anormal kullanımını avlamaya kaymaktadır. Güçlü kimlik doğrulama ve kullanıcı eğitimi, deepfake'lere karşı kritik savunmalar haline gelmektedir.[2]

GenAI güdümlü şantajın yükselişi, kurumsal verilerin değer önerisini temelden değiştirir. Artık mesele sadece yapılandırılmış Kişisel Tanımlanabilir Bilgileri (PII) veya finansal verileri korumak değildir; şimdi e-postalar, sohbet günlükleri ve dahili belgeler gibi yapılandırılmamış veriler hızla silah haline getirilebilir, bu da kapsamlı veri sınıflandırmasını ve içeriden gelen risk yönetimini her şeyden önemli kılar. Geleneksel veri koruma, iyi tanımlanmış hassas veri türlerine (kredi kartı numaraları, sosyal güvenlik numaraları, sağlık kayıtları) odaklanır. GenAI, saldırganların daha önce manuel olarak analiz edilmesi çok zor olan büyük miktardaki yapılandırılmamış verilerde "değer" bulmasını sağlar.[2] Utanç verici bir e-posta, hassas bir iş müzakeresi veya bir müşterinin dahili eleştirisi, hepsi şantaj için kullanılabilir. Bu, bir kuruluşun "hassas veri" ayak izinin, neredeyse tüm yapılandırılmamış iletişimlerini içerecek şekilde genişlediği anlamına gelir. Bu nedenle, güvenlik stratejileri gelişmelidir. Proaktif tehdit avcılığının, bu yeni değerli yapılandırılmamış veriyi keşfetmek, sınıflandırmak ve korumak için sağlam bir Veri Güvenliği Durum Yönetimi (Data Security Posture Management - DSPM) programıyla (Forcepoint tarafından belirtildiği gibi[6]) sıkı bir şekilde entegre edilmesi gerekir. Ayrıca, GenAI içeriden gelenleri daha güçlü bir tehdit haline getirdiğinden, anormal veri erişimini ve sızmasını tespit etmek için içeriden gelen risk yönetimi programları daha kritik hale gelir.[2]

6. Yakınsanmış IT/OT/IoT Ortamının Güvenliğini Sağlama

Bilgi Teknolojileri (IT) ve Operasyonel Teknolojiler (OT) ağlarının yakınsaması ve IoT cihazlarının patlaması, bir zamanlar kritik altyapıyı koruyan hava boşluğunu (air gap) ortadan kaldırmıştır. OT sistemlerinin %70'inin IT ağlarına bağlanması ve OT saldırılarının %75'inin bir IT ihlali olarak başlaması öngörülmektedir.[48]

Spesifik Riskler

- **Yanal Hareket:** Saldırganlar daha az güvenli olan IT ağına sızar ve yüksek değerli OT ağına yönelir.[48]
- **Eski Sistemler:** OT ortamları, son derece savunmasız olan eski, yamalanamayan sistemlerle doludur.[48]
- **Güvensiz Uzaktan Erişim:** OT ortamlarının %65'i 2024'te güvensiz uzaktan erişim koşullarına sahipti.[48]

- **Fiziksel Sonuçlar:** Saldırılar artık sadece veri hırsızlığıyla ilgili değildir; fiziksel zarara neden olabilir, temel hizmetleri (enerji, su) kesintiye uğratabilir ve jeopolitik sonuçları olabilir.[4]

Avcılık Stratejileri

OT'de tehdit avcılığı, özel bilgi ve araçlar gerektirir. Anahtar stratejiler arasında ağ segmentasyonu (yanal hareketi önlemek için), OT sistemleri için kimlik tabanlı erişim kontrolleri ve ISA/IEC 62443 ve NIST SP 800-82 gibi çerçeveler tarafından yönlendirilen anormal davranışlar için sürekli izleme yer alır.[48]

IT/OT yakınsaması, kurumsal IT güvenlik ekipleri ile tesis düzeyindeki mühendislik ekipleri arasında gerekli, ancak genellikle zorlu bir kültürel ve organizasyonel yakınsamayı zorlar. Bu kültürel boşluğu kapatmadaki bir başarısızlık, herhangi bir tekil teknik zafiyetten daha büyük bir risktir. IT güvenlik ekipleri gizlilik, bütünlük ve kullanılabilirliği (CIA üçlüsü) önceliklendirir. Yamalama, yeniden başlatma ve hızlı değişikliklerle rahattırlar. OT/mühendislik ekipleri ise her şeyden önce güvenliği ve kullanılabilirliği önceliklendirir. Onların sloganı "bozuk değilse, tamir etme"dir. Kesintiye veya öngörülemeyen fiziksel davranışlara neden olabilecek değişikliklere karşı son derece dirençlidirler. IT ve OT ağları yakınsadığında, bu iki kültür çarpışır. IT ekibi ajanları dağıtmak ve zafiyetleri taramak isterken, OT ekibi bunun kritik süreçleri kesintiye uğratacağından korkar. Sonuç olarak, güvenlik girişimleri genellikle teknik sınırlamalardan değil, organizasyonel sürtünmeden dolayı duraklar. Bu nedenle, başarılı bir OT güvenlik programı (ve dolayısıyla proaktif bir OT tehdit avcılığı programı), yönetişimle (NIST CSF 2.0'a göre) başlamalıdır. Ortak bir IT/OT güvenlik komitesi kurmayı, ortak politikalar oluşturmayı ve karşılıklı anlayış ve güven inşa etmeyi gerektirir. Teknoloji (örneğin, pasif izleme, OT'ye özgü IDS), insanları ve süreçleri hizalamaktan sonra gelir.

7. Bir Avcılık Disiplini Olarak Siber Güvenlik Tedarik Zinciri Risk Yönetimi (C-SCRM)

Siber Güvenlik Tedarik Zinciri Risk Yönetimi (Cybersecurity Supply Chain Risk Management - C-SCRM), artık niş bir uyumluluk görevi değildir; NIST CSF 2.0 Yönet fonksiyonunda (GV.SC) açıkça belirtilen temel bir güvenlik fonksiyonudur.[7] Salt

Typhoon telekom saldırısı gibi yüksek profilli saldırılar [5] ve yazılım tedarik zinciri ihlallerinin sürekli tehdidi, aciliyeti vurgulamaktadır. Gartner, 2025 yılına kadar dünya çapındaki kuruluşların %45'inin bir yazılım tedarik zinciri saldırısından etkileneceğini öngörmektedir.[11]

Proaktif Avcılık Yaklaşımı

- **Üçüncü Taraf İzleme:** Kritik satıcıların dış saldırı yüzeyini sürekli olarak izlemek için ASM araçlarını kullanmak.[19]
- **Davranışsal Analiz:** Üçüncü taraf ortamlara veya bu ortamlardan gelen anormal ağ bağlantılarını avlamak.
- **Yazılım Malzeme Listesi (SBOM):** Ticari ve açık kaynaklı yazılımlardaki savunmasız bileşenleri belirlemek ve bunların sömürülmesine dair herhangi bir işareti avlamak için SBOM'ları kullanmak.
- **XDR/UEBA Entegrasyonu:** Bir uç noktadaki şüpheli etkinliği bilinen bir üçüncü taraf ortağa giden ağ trafiğiyle ilişkilendirmek için birleşik platformları kullanmak.

Etkili C-SCRM, "güven ama doğrula" (anketlere ve denetimlere dayalı) paradigmasından, Sıfır Güven ilkelerini yansıtan "asla güvenme, her zaman doğrula" (sürekli, gerçek zamanlı teknik izlemeye dayalı) paradigmasına bir geçiş gerektirir. Geleneksel C-SCRM, güvenlik anketleri ve üçüncü taraf denetimleri gibi periyodik, anlık değerlendirmelere dayanır. Bu, bir satıcının bir sonraki denetime kadar güvende kabul edildiği bir "güven ama doğrula" modeli yaratır. Bu model, sürekli dağıtım ve karmaşık saldırılar dünyasında temelden bozuktur. Bir satıcı Pazartesi günü güvende olabilir ve Salı günü ihlal edilebilir. Modern, proaktif bir C-SCRM yaklaşımı, tedarik zincirine Sıfır Güven ilkelerini uygular. Herhangi bir üçüncü taraf bağlantısının bir saldırı vektörü olabileceğini varsayar. Bu, satıcıların sürekli saldırı yüzeyi izlenmesi [19], üçüncü taraf bağlantıları için katı ağ segmentasyonu ve erişim kontrolleri (bir ZTA ilkesi) ve iş ortaklarına/ortaklarından gelen tüm trafiğin davranışsal olarak izlenmesi gibi teknik kontrollerin benimsenmesine yol açar. Bu nedenle, C-SCRM sadece daha iyi sözleşmeler ve anketlerle ilgili değildir. Kuruluşun proaktif avcılık ve izleme yeteneklerini dijital tedarik zincirine genişletmekle, satıcı bağlantılarını dahili kullanıcı erişimiyle aynı düzeyde titizlikle ele almakla ilgilidir.

8. Gelişmiş Kimlik Tehdit Tespiti ve Müdahalesi (ITDR)

Ağ çevresinin çözülmesiyle birlikte, kimlik birincil güvenlik sınırı haline gelmiştir. Kimlik Tehdit Tespiti ve Müdahalesi (Identity Threat Detection and Response - ITDR), kimlik sistemlerini korumaya ve kötüye kullanımlarını tespit etmeye odaklanan özel bir disiplindir. XDR ve Sıfır Güven'i tamamlar ve bunların kritik bir bileşenidir.

Avcılık için Anahtar Odak Alanları

- **Kimlik Bilgisi Kötüye Kullanımı:** Çalınan kimlik bilgilerinin, pass-the-hash saldırılarının vb. kullanımını tespit etmek.
- **Ayrıcalık Yükseltme:** Bir saldırganın izinlerini yükseltmeye çalıştığını belirlemek.
- **Anormal Kimlik Doğrulama:** Olağandışı konumlardan, imkansız seyahat senaryolarından veya yönetilmeyen cihazlardan yapılan oturum açmaları işaretlemek.[50]
- **Yanal Hareket:** Bir saldırganın ele geçirilmiş bir kimliği sistemden sisteme geçmek için nasıl kullandığını izlemek.

UEBA'nın Rolü

Kullanıcı ve Varlık Davranış Analitiği (User and Entity Behavior Analytics - UEBA), ITDR'ın arkasındaki temel teknolojidir. Normal kullanıcı ve varlık davranışını temel alarak, UEBA, ele geçirilmiş bir kimliği gösteren ince sapmaları tespit edebilir.[18]

Makine Kimlikleri

Tehdit yüzeyi sadece insan kullanıcılardan oluşmaz. Makine kimliklerini (örneğin, hizmet hesapları, API anahtarları) yönetmek ve güvence altına almak, ITDR'ın ele alması gereken büyüyen bir zorluktur.[6]

ITDR'ın yükselişi, endüstrinin nihayet Active Directory'nin (ve bulut eşdeğeri Entra ID'nin) çoğu kuruluşta "taç mücevheri" varlığı olduğunu ve kritik bir üretim veritabanı

kadar titizlikle savunulması gerektiğini kabul ettiğini göstermektedir. Yıllarca güvenlik, uç noktaları ve sunucuları korumaya odaklandı. Active Directory genellikle birincil bir güvenlik varlığı olarak değil, bir IT altyapısı olarak görüldü. Ancak, neredeyse her büyük ihlal, AD'nin ele geçirilmesini içerir. Bir saldırgan AD'yi kontrol ettiğinde, tüm kuruluşu kontrol eder. Hesaplar oluşturabilir, izinler atayabilir ve cezasız bir şekilde hareket edebilirler. ITDR, kimlik altyapısının kendisini savunmanın her şeyden önemli olduğunun farkına varılmasını temsil eder. Bu, sadece oturum açma olaylarını izlemekle kalmaz, aynı zamanda kimlik sistemi *içindeki* ihlal belirtilerini aktif olarak avlamayı da içerir: keşif (örneğin, BloodHound), sahte etki alanı denetleyicilerinin oluşturulması, izinlerin değiştirilmesi vb. Aldatma teknolojisi, bu keşif ve kötü niyetli faaliyetleri erken tespit etmek için Active Directory içine yerleştirilen yemler ve kırıntılarla burada kilit bir rol oynar.[36] Bu nedenle, olgun bir proaktif avcılık programı, kimlik yapısını yüksek değerli bir hedef olarak ele alan ve tehditleri sadece kenarlarında değil,

içinde avlayan özel bir ITDR çalışma akışına sahip olmalıdır.

9. Hiper-Otomasyon ve Orkestrasyon (SOAR)

SOAR platformları, modern SOC'nin bağlayıcı dokusudur. Oyun kitapları (playbook) olarak bilinen karmaşık iş akışlarını otomatikleştirmek ve düzenlemek için tüm güvenlik yığınıyla (SIEM, XDR, tehdit istihbaratı beslemeleri vb.) entegre olurlar.[31]

Proaktif Avcılıkta Rolü

Genellikle olay müdahalesiyle ilişkilendirilse de, SOAR proaktif avcılık için güçlü bir kolaylaştırıcıdır:

- **Otomatik Triyaj ve Zenginleştirme:** Bir avcı potansiyel bir ihlal göstergesi (IOC) belirlediğinde, bir SOAR oyun kitabı bunu otomatik olarak tehdit istihbaratıyla zenginleştirebilir, diğer sistemlerde varlığını kontrol edebilir ve bağlamsal verileri toplayarak analiste saatlerce süren manuel işten tasarruf ettirebilir.
- **Otomatik Avcılık Oyun Kitapları:** Kuruluşlar, avcılık hipotezlerini SOAR oyun kitaplarına kodlayabilirler. Örneğin, belirli türdeki PowerShell kötüye kullanımını periyodik olarak avlamak, EDR günlüklerini otomatik olarak sorgulamak, sonuçları analiz etmek ve bir eşleşme bulunursa uyarı vermek için bir oyun kitabı

oluşturulabilir.
- **Avcılığı Ölçeklendirme:** Otomasyon, küçük bir avcı ekibinin manuel olarak yapabileceğinden çok daha fazla avcılık görevini yürütmesine olanak tanır ve çabalarının ölçeğini ve tutarlılığını önemli ölçüde artırır.

Forrester Wave™ ve SANS anketleri, SOAR'ın olgun bir pazar olduğunu ve anahtar kullanım durumlarının olay müdahalesi, tehdit istihbaratının operasyonelleştirilmesi ve zafiyet yönetimi olduğunu vurgulamaktadır.[31]

SOAR'ın proaktif avcılık bağlamındaki gerçek değeri sadece müdahaleyi otomatikleştirmek değil, aynı zamanda *merakı* otomatikleştirmektir. Güvenlik ekiplerinin, ortamlarına sistematik ve tekrarlı bir şekilde, tek başına insanların yapmasının imkansız olduğu bir ölçekte sorular sormasına olanak tanır. Bir tehdit avı bir hipotezle başlar: "Bir saldırganın kalıcılık için WMI kullanıyor olabileceğine inanıyorum." Manuel bir süreçte, bir analistin EDR/SIEM'i için doğru sorguları formüle etmesi, bunları çalıştırması, verileri toplaması ve analiz etmesi gerekir. Bu zaman alıcıdır ve yalnızca ara sıra yapılabilir. SOAR ile bu tüm süreç bir oyun kitabına kodlanabilir. Oyun kitabı, bu "soruyu" belirli bir program dahilinde (örneğin, günlük olarak) ortama sorar. Bu, tehdit avcılığını geçici, kahraman odaklı bir faaliyetten sistematik, programatik bir sürece dönüştürür. Bu nedenle, SOAR'ın rolü insan avcıyı değiştirmek değil, onun güç çarpanı olarak hareket etmektir. Avcının yaratıcılığı ve sezgisi hipotezleri (oyun kitaplarını) tasarlamak için kullanılır ve SOAR'ın otomasyonu bunları yorulmadan ve ölçekli bir şekilde yürütmek için kullanılır. Bu, avcıyı yeni hipotezler geliştirmeye ve otomatik avların ortaya çıkardığı karmaşık bulguları araştırmaya odaklanması için serbest bırakır.

10. Siber Dayanıklılık İnşa Etmek: İnsan Merkezli, Tükenmişliğe Dirençli Bir Güvenlik Kültürü

Gartner tarafından vurgulanan bu son eğilim, en gelişmiş teknolojinin bile doğru insanlar ve kültür olmadan etkisiz olduğunu kabul etmektedir.[1] Proaktif bir avcılık programı, özellikle insan analistlerinin becerisine, yaratıcılığına ve motivasyonuna bağlıdır.

Tükenmişlik Krizi

Siber güvenliğin hızlı değişim hızı ve yüksek basınçlı ortamı, yüksek tükenmişlik oranlarına yol açmaktadır. Gartner, 2027 yılına kadar dayanıklılık programlarına yatırım yapan CISO'ların, yapmayan meslektaşlarına göre %50 daha az tükenmişlikle ilgili personel kaybı göreceğini öngörmektedir.[1]

Dayanıklılık için Stratejiler

- **Yönetici Yönetişimi:** Trend #1'de tartışıldığı gibi, net stratejik yönlendirme ve yönetici desteği, tükenmişliği önlemedeki en önemli faktörlerdir.
- **Bir Güçlendirici Olarak Otomasyon:** Tekrarlayan, düşük değerli görevleri ele almak için SOAR ve AI güdümlü platformları kullanmak, analistleri yüksek etkili, yaratıcı işlere (örneğin, hipotez geliştirme, karmaşık araştırmalar) odaklanmaları için serbest bırakmak.[30]
- **Sürekli Öğrenme ve Eğitim:** Eğitime (SANS kursları gibi[54]) yatırım yapmak ve araştırma için zaman tanımak, becerileri keskin tutar ve katılımı yüksek tutar.
- **Psikolojik Güvenlik Kültürü:** Analistlerin deney yapabildiği, yeni hipotezler önerebildiği ve hatta misilleme korkusu olmadan başarısız olabildiği bir ortamı teşvik etmek, tehdit avcılığının gerektirdiği yaratıcılık için esastır.

Bir İş Kolaylaştırıcı Olarak Güvenlik

Bu kültürel değişim, güvenliğin bir maliyet merkezinden, işletmenin hesaplanmış riskler almasını ve güvenli bir şekilde yenilik yapmasını sağlayan bir ortağa dönüşmesini içerir.[1]

En etkili proaktif tehdit avcılığı ekipleri, geleneksel bir SOC'den daha çok, dahili bir Ar-Ge veya istihbarat analiz birimi gibi çalışanlar olacaktır. Geleneksel bir SOC, genellikle bir kuyruktan gelen uyarıları işlemeye odaklanan reaktif, bilet güdümlü bir ortamdır. Bu tekrarlayıcıdır ve tükenmişliğe yol açabilir. Proaktif tehdit avcılığı, doğası gereği, araştırmacı ve yaratıcı bir süreçtir. Merak, derin teknik bilgi ve önceden tanımlanmış bir uyarı olmadan verileri keşfetme özgürlüğü gerektirir. Bu beceri seti ve zihniyet, bir yardım masası teknisyeninden çok bir araştırma bilimcisine veya bir istihbarat analistine daha yakındır. Bu nedenle, sürdürülebilir ve etkili bir avcılık programı oluşturmak için kuruluşlar ekibi buna göre yapılandırmalı ve yönetmelidir. Bu

şu anlama gelir: **Metrikler:** Başarıyı "kapatılan biletler" ile değil, "keşfedilen yeni tehditler" veya "geliştirilen avcılık oyun kitapları" ile ölçmek. **Zaman Tahsisi:** Sadece operasyonel görevler için değil, açık uçlu araştırma, eğitim ve araç geliştirme için resmi olarak zaman ayırmak. **İşe Alım:** Sadece araca özgü sertifikalara sahip olanları değil, doğuştan meraklı ve analitik becerilere sahip bireyleri işe almak. Tehdit avcılığı ekibini yüksek değerli bir Ar-Ge işlevi olarak ele alarak, kuruluşlar düşmanların önünde kalmak için gereken üst düzey yetenekleri çekebilir ve elinde tutabilir ve geleneksel güvenlik operasyonlarını rahatsız eden tükenmişliği önleyebilir.

Bölüm III: Sentez ve Stratejik Uygulama Yol Haritası

Bölüm 3: Entegre Uygulama ve Sinerji: Birleşik Bir Proaktif Savunma Modeli

Bu sonuç bölümü, 10 eğilimi tutarlı bir operasyonel modelde sentezleyerek bunların birbirine bağımlılığını gösterecektir. Bu basit bir özet olmayacak, gerçek dünya senaryosunda nasıl birlikte çalıştıklarının bir illüstrasyonu olacaktır.

Örnek Senaryo: "GenAI ile Güçlendirilmiş Bir Bilgi Hırsızı Saldırısını Avlamak"

1. **Yönetişim (#1)** ve **Dayanıklılık (#10)** sahneyi hazırlar: CISO, marka itibarını ve müşteri güvenini korumanın en önemli iş önceliği olduğunu tanımlamıştır. Avcılık ekibi yetkilendirilmiş ve bu hedefi takip etmek için kaynaklara sahiptir.
2. **ZTA (#2)** temeli sağlar: Her erişim talebi günlüğe kaydedilir ve temiz veri sağlanır.
3. **ASM (#1)**, pazarlama departmanı tarafından kullanılan yeni, onaylanmamış bir bulut hizmetini tespit ederek saldırı yüzeyini artırır.
4. **Aldatma (#3)** yüksek doğruluklu bir uyarıyı tetikler: Yem olarak yerleştirilmiş sahte bir AWS anahtarına bir çalışanın makinesinden erişilir.
5. Uyarı, **Birleşik Platform (#2)** tarafından alınır. **SOAR (#9)** bileşeni otomatik olarak bir oyun kitabını başlatır:
    - Uyarıyı uç noktadaki **XDR** ajanından ve kullanıcının davranışının anormal hale

geldiğini gösteren **UEBA/ITDR (#8)**'den gelen verilerle zenginleştirir.
    - **C-SCRM (#7)** veritabanını sorgular ve kullanıcının yakın zamanda yeni bir satıcıdan "ücretsiz" bir pazarlama analitik aracı yüklediğini bulur.
6. İnsan avcı, birleşik platformdaki ilişkili verileri araştırır. Şifreli bir kanal üzerinden büyük miktarda verinin sızdırıldığını görür. **ETA (#4)**, şifresini çözmeden bile veri akışını veri sızıntısıyla tutarlı olarak anormal olarak işaretler.
7. Avcı, bunun muhtemelen GenAI'dan yararlanan bir **Bilgi Hırsızı saldırısı (#5)** olduğunu fark eder. Oyun kitabı, uç noktayı otomatik olarak izole eder ve kullanıcının kimliğini askıya alır.
8. Ekip ayrıca, saldırı vektörünün kurumsal ağdan bulut tabanlı bir **IoT/OT benzeri (#6)** pazarlama otomasyon platformuna geçtiğini ve yanal hareketi izleyebildiklerini fark eder.

Bu anlatı, hiçbir tek eğilimin sihirli bir değnek olmadığını göstermektedir. Etkili proaktif savunma, sistemlerin entegre bir sistemidir.

Bölüm 4: Uygulanabilirlik Değerlendirmesi ve Önceliklendirme Çerçevesi

Bu son bölüm, kullanıcının bu eğilimleri uygulaması için pratik, eyleme geçirilebilir bir çerçeve sunmaktadır. Hiçbir kuruluşun 10 eğilimi aynı anda benimseyemeyeceğini kabul edecek ve olgunluk, bütçe ve risk iştahına dayalı bir önceliklendirme yöntemi sunacaktır.

Merkezde, ayrıntılı bir karşılaştırmalı analiz tablosu yer alacaktır. Bu tablo, nitel bir tartışmanın ötesine geçerek 10 eğilimin yapılandırılmış, nicel tarzda bir karşılaştırmasını sunan güçlü bir karar verme aracı olarak tasarlanmıştır. Bu, Proje Liderinin hem teknik ekiplerle hem de liderlikle stratejik bir görüşme yapmasına olanak tanır ve teknolojileri belirli hedeflere, maliyetlere ve bağımlılıklara açıkça eşleyerek yatırım kararlarını gerekçelendirir. Raporun derin analizini bir bakışta stratejik bir planlayıcıya dönüştürür.

Tablo 1: Proaktif Tehdit Avcılığı Teknolojilerinin Karşılaştırmalı Analizi (2025+)

Teknik/Trend	Proaktif Potansiyel	Birincil Kullanım Alanı	Uygulama Karmaşıklığı	Maliyet Profili	Anahtar Bağımlılıklar	Tehdit Türüne Uygunluk

1. AI Destekli ASM	Yüksek	Keşif, Önceliklendirme	Orta	Orta-Yüksek	Bulut Odaklı Altyapı	Yanlış Yapılandırma, Gölge BT, Zafiyet Sömürüsü
2. Birleşik SOC Platformu (XDR)	Yüksek	Tespit, Araştırma	Yüksek	Yüksek	Olgun EDR, Bulut/Ağ Telemetrisi	APT, Fidye Yazılımı, Yanal Hareket
3. Derinlemesine Aldatma	Yüksek	Tespit, İstihbarat Toplama	Orta	Orta	Bölümlenmiş Ağ	İçeriden Gelen Tehdit, APT, Yanal Hareket
4. Şifreli Trafik Analizi (ETA)	Orta	Tespit, Görünürlük	Orta-Yüksek	Orta	ML Yetenekli Ağ Cihazları/Yazılımı	C2 İletişimi, Kötü Amaçlı Yazılım, Veri Sızıntısı
5. GenAI Tehdit Savunması	Yüksek	Tehdit İstihbaratı, Kimlik	Düşük (İstihbarat), Yüksek (Savunma)	Değişken	Güçlü Kimlik Doğrulama, Kullanıcı Eğitimi	Sosyal Mühendislik, Şantaj, Bilgi Hırsızları
6. IT/OT/IoT Güvenliği	Yüksek	Sınırlama, Tespit	Çok Yüksek	Yüksek	IT/OT Organizasyonel Uyum, Pasif Sensörler	Kritik Altyapı Saldırıları, Sabotaj
7. C-SCRM Avcılığı	Orta	Görünürlük, Risk Yönetimi	Orta	Orta	ASM, Satıcı Sözleşmeleri	Tedarik Zinciri Saldırıları, 3. Taraf İhlali
8. Gelişmiş	Yüksek	Tespit, Önleme	Yüksek	Orta-Yüksek	Olgun Kimlik	Kimlik Bilgisi

ITDR					Programı, UEBA	Hırsızlığı, İçeriden Gelen Tehdit, Fidye Yazılımı
9. SOAR / Hiper-Otomasyon	Orta	Verimlilik, Ölçeklendirme	Yüksek	Yüksek	İyi Tanımlanmış Süreçler, API Odaklı Araçlar	Tümü (bir güç çarpanı olarak)
10. İnsan Merkezli Dayanıklılık	Yüksek	Sürdürülebilirlik, Strateji	Yüksek (Kültürel)	Düşük-Orta (Eğitim)	Yönetici Desteği (Yönetişim)	Tükenmişlik, İnsan Hatası, İçeriden Gelen Tehdit

Alıntılanan çalışmalar

1. Key Trends from Gartner® Cybersecurity Research | Rapid7 Blog, erişim tarihi Haziran 14, 2025, https://www.rapid7.com/blog/post/2025/05/01/ai-and-resilience-take-the-spotlight-in-2025-key-trends-from-gartner-r-cybersecurity-research/
2. Forrester's Top Threats For 2025, erişim tarihi Haziran 14, 2025, https://www.forrester.com/blogs/forresters-top-threats-for-2025/
3. Navigating Data Security in 2025: Key Insights from Cisco's ..., erişim tarihi Haziran 14, 2025, https://www.kiteworks.com/cybersecurity-risk-management/data-security-ai-threats-cisco-cybersecurity-readiness-index-2025/
4. Trends and expectations for OT security in 2025 | Nomios Group, erişim tarihi Haziran 14, 2025, https://www.nomios.com/news-blog/trends-ot-security-2025/
5. Cybercrime expected to cost $12 trillion in 2025. Forrester Predictions 2025 Report., erişim tarihi Haziran 14, 2025, https://blog.biocomm.ai/2025/04/13/cybercrime-expected-to-cost-12-trillion-in-2025-forrester-predictions-2025-report/
6. Gartner's Top Cybersecurity Trends for 2025—Are You Securing AI? - Forcepoint, erişim tarihi Haziran 14, 2025, https://www.forcepoint.com/blog/insights/gartner-top-cybersecurity-trends-2025-secure-ai
7. NIST CSF 2.0: Key Updates and Why They Matter - NRI Secure, erişim tarihi Haziran 14, 2025, https://www.nri-secure.com/blog/nist-csf-2
8. NIST CSF 2.0: Everything You Need to Know About the Update - Hyperproof,

erişim tarihi Haziran 14, 2025, https://hyperproof.io/resource/nistcsf2-0-update/
9. Why is NIST adding Governance to the NIST CSF 2.0? - Expel, erişim tarihi Haziran 14, 2025, https://expel.com/blog/why-is-nist-adding-governance-to-nist-csf-2-0/
10. What is NIST Cybersecurity Framework (CSF) 2.0? - Balbix, erişim tarihi Haziran 14, 2025, https://www.balbix.com/insights/nist-cybersecurity-framework/
11. What's New in NIST CSF 2.0: The Top 4 Changes | UpGuard, erişim tarihi Haziran 14, 2025, https://www.upguard.com/blog/key-changes-nist-csf-version-2
12. Unpacking the NIST cybersecurity framework 2.0 - IBM, erişim tarihi Haziran 14, 2025, https://www.ibm.com/think/insights/nist-cybersecurity-framework-2
13. Understanding NIST Cybersecurity Framework 2.0 - LogicGate, erişim tarihi Haziran 14, 2025, https://www.logicgate.com/blog/understanding-nist-csf-2-0-cybersecurity-framework/
14. NIST Offers 19 Ways to Build Zero Trust Architectures | NIST, erişim tarihi Haziran 14, 2025, https://www.nist.gov/news-events/news/2025/06/nist-offers-19-ways-build-zero-trust-architectures
15. NIST Publishes New Zero Trust Implementation Guidance - Infosecurity Magazine, erişim tarihi Haziran 14, 2025, https://www.infosecurity-magazine.com/news/nist-zero-trust-implementation/
16. NIST SPECIAL PUBLICATION 1800-35 Implementing a Zero Trust Architecture, erişim tarihi Haziran 14, 2025, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-35.pdf
17. What is XDR? Extended Detection & Response - CrowdStrike.com, erişim tarihi Haziran 14, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/extended-detection-and-response-xdr/
18. What Is User and Entity Behavior Analytics (UEBA)? | Microsoft Security, erişim tarihi Haziran 14, 2025, https://www.microsoft.com/en-us/security/business/security-101/what-is-user-entity-behavior-analytics-ueba
19. Top Attack Surface Management Trends for 2025 - Cyble, erişim tarihi Haziran 14, 2025, https://cyble.com/blog/attack-surface-management-in-2025/
20. How AI Is Transforming Attack Surface Management - Cyble, erişim tarihi Haziran 14, 2025, https://cyble.com/knowledge-hub/ai-attack-surface-management/
21. Mandiant Attack Surface Management | Google Cloud, erişim tarihi Haziran 14, 2025, https://cloud.google.com/security/products/attack-surface-management
22. Top 11 Attack Surface Management Tools For 2025 - SentinelOne, erişim tarihi Haziran 14, 2025, https://www.sentinelone.com/cybersecurity-101/cybersecurity/attack-surface-management-tools/
23. Attack Surface Management - Darktrace, erişim tarihi Haziran 14, 2025, https://www.darktrace.com/attack-surface-management
24. Proactive Attack Surface Management Solutions | Qualys, erişim tarihi Haziran 14, 2025, https://www.qualys.com/faqs-resources-attack-surface-management/

25. Attack Surface Management Market Size, Share | Growth [2032] - Fortune Business Insights, erişim tarihi Haziran 14, 2025, https://www.fortunebusinessinsights.com/attack-surface-management-market-110386
26. Top 10 XDR Solutions for 2025 - SentinelOne, erişim tarihi Haziran 14, 2025, https://www.sentinelone.com/cybersecurity-101/endpoint-security/xdr-solutions/
27. www.crowdstrike.com, erişim tarihi Haziran 14, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/extended-detection-and-response-xdr/#:~:text=Extended%20detection%20and%20response%20(XDR)%20collects%20threat%20data%20from%20previously,%2C%20threat%20hunting%2C%20and%20response.
28. 2025 Cybersecurity Predictions - Palo Alto Networks, erişim tarihi Haziran 14, 2025, https://www.paloaltonetworks.com/why-paloaltonetworks/cyber-predictions
29. Cortex XDR Named 2025 Gartner Customers' Choice for Endpoint Security, erişim tarihi Haziran 14, 2025, https://www.paloaltonetworks.com/blog/2025/05/cortex-xdr-named-gartner-customers-choice-endpoint-security/
30. XDR EXPLAINED | CrowdStrike, erişim tarihi Haziran 14, 2025, https://www.crowdstrike.com/wp-content/uploads/2023/02/crowdstrike-xdr-explained.pdf
31. Orchestrating Cyber Defense - Number Analytics, erişim tarihi Haziran 14, 2025, https://www.numberanalytics.com/blog/orchestrating-cyber-defense-guide
32. Planning Guide 2023: Security & Risk - Forrester, erişim tarihi Haziran 14, 2025, https://www.forrester.com/bold/planning-guide-2023-security-risk/
33. Open XDR vs Native XDR: Key Differences - CrowdStrike, erişim tarihi Haziran 14, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/open-xdr-vs-native-xdr/
34. Primer on Deception Technology - HALOCK Security Labs, erişim tarihi Haziran 14, 2025, https://www.halock.com/a-primer-to-deception-technology/
35. What Is Deception Technology? - Check Point Software, erişim tarihi Haziran 14, 2025, https://www.checkpoint.com/cyber-hub/cyber-security/what-is-deception-technology/
36. Deception Technology Solution - Fidelis Security, erişim tarihi Haziran 14, 2025, https://fidelissecurity.com/solutions/deception/
37. What is Deception Technology? Importance & Benefits - Zscaler, erişim tarihi Haziran 14, 2025, https://www.zscaler.com/resources/security-terms-glossary/what-is-deception-technology
38. Deception Technology 101 | Smokescreen, erişim tarihi Haziran 14, 2025, https://www.smokescreen.io/deception-technology-101/
39. Deception for Threat Hunting: A Cyber Defense Strategy You Can't Ignore | Fidelis Security, erişim tarihi Haziran 14, 2025,

https://fidelissecurity.com/cybersecurity-101/deception/deception-for-threat-hunting/
40. What Is Deception Technology? Definition | Proofpoint US, erişim tarihi Haziran 14, 2025, https://www.proofpoint.com/us/threat-reference/deception-technology
41. Deception vs. Traditional Threat Detection: A Detailed Comparison | Fidelis Security, erişim tarihi Haziran 14, 2025, https://fidelissecurity.com/threatgeek/threat-detection-response/deception-vs-traditional-threat-detection/
42. (PDF) Decrypting SSL/TLS traffic for hidden threats detection - ResearchGate, erişim tarihi Haziran 14, 2025, https://www.researchgate.net/publication/386624783_Decrypting_SSLTLS_traffic_for_hidden_threats_detection
43. Decrypting SSL/TLS Traffic for Hidden Threats Detection - arXiv, erişim tarihi Haziran 14, 2025, https://arxiv.org/pdf/1904.08383
44. Cisco Secure Network Analytics - Blog - IPTel Solutions, erişim tarihi Haziran 14, 2025, https://blog.iptel.com.au/cisco-secure-network-analytics
45. Cisco ETA feature (Encrypted Traffic Analysis) at glance, erişim tarihi Haziran 14, 2025, https://community.cisco.com/t5/security-knowledge-base/cisco-eta-feature-encrypted-traffic-analysis-at-glance/ta-p/4783197
46. linwhitehat/ETA-Resource: Materials about Encrypted ... - GitHub, erişim tarihi Haziran 14, 2025, https://github.com/linwhitehat/ETA-Resource
47. How ETA Works | LiveAction, erişim tarihi Haziran 14, 2025, https://www.liveaction.com/wp-content/uploads/2022/01/How-ETA-Works.pdf
48. OT Security Trends 2025: Defending Against Escalating Threats and Evolving Tactics, erişim tarihi Haziran 14, 2025, https://zeronetworks.com/blog/ot-security-trends-2025-escalating-threats-evolving-tactics
49. Emerging trends in Operational Technology (OT) in 2025 and beyond - Eviden, erişim tarihi Haziran 14, 2025, https://eviden.com/publications/digital-security-magazine/cybersecurity-predictions-2025/operational-technology-security-trends/
50. 2025 Cisco Cybersecurity Readiness Index, erişim tarihi Haziran 14, 2025, https://newsroom.cisco.com/c/dam/r/newsroom/en/us/interactive/cybersecurity-readiness-index/2025/documents/2025_Cisco_Cybersecurity_Readiness_Index.pdf
51. What is UEBA (User and Entity Behavior Analytics)? - Palo Alto Networks, erişim tarihi Haziran 14, 2025, https://www.paloaltonetworks.com/cyberpedia/what-is-user-entity-behavior-analytics-ueba
52. Microsoft Sentinel UEBA: 2025 Guide to Behavior Analytics, erişim tarihi Haziran 14, 2025, https://secureazcloud.com/microsoft-security/f/microsoftsentinelueba2025guidetobehavioranalytics
53. Market Guide for Security Orchestration, Automation and Response Solutions,

erişim tarihi Haziran 14, 2025, https://ransomware.databreachtoday.com/whitepapers/market-guide-for-security-orchestration-automation-response-w-7028
54. SEC541: Cloud Security Threat Detection - SANS Institute, erişim tarihi Haziran 14, 2025, https://www.sans.org/cyber-security-courses/cloud-security-threat-detection/
55. SEC503: Network Monitoring and Threat Detection In-Depth - SANS Institute, erişim tarihi Haziran 14, 2025, https://www.sans.org/cyber-security-courses/network-monitoring-threat-detection/