2025 Yılı İçin Ağ Güvenliği Dedektörlerinin (IDS/IPS) İşleyiş Analizi, Güçlü ve Zayıf Yönleri ve Güvenli Ağ Ortamı Oluşturma Önerileri

Yönetici Özeti

Bu rapor, 2025 yılı ve sonrasında siber güvenlik ortamında İzinsiz Giriş Tespit Sistemleri (IDS) ve İzinsiz Giriş Önleme Sistemleri (IPS) gibi ağ güvenliği dedektörlerinin işleyişini, güçlü ve zayıf yönlerini ve güvenli bir ağ ortamı oluşturmak için sunulan önerileri kapsamaktadır. Siber saldırıların karmaşıklığı ve sıklığı giderek artmakta olup [1], bu durum ağ güvenliği çözümlerinin sürekli evrimini zorunlu kılmaktadır.[5] Bu bağlamda, IDS ve IPS, ağ trafiğini izleyerek ve kötü niyetli aktiviteleri tespit ederek veya önleyerek kritik bir rol oynamaktadır.

Raporun bulguları, yapay zeka (AI) ve makine öğreniminin (ML) tehdit tespitindeki dönüştürücü etkisini, bulut tabanlı çözümlere geçişi, Sıfır Güven (Zero Trust) mimarileriyle entegrasyonun önemini, Siber Tehdit İstihbaratının (CTI) merkezi rolünü, Nesnelerin İnterneti (IoT) ortamlarının güvenliğini sağlama zorluklarını ve Güvenlik Bilgileri ve Olay Yönetimi (SIEM) ile Güvenlik Orkestrasyonu, Otomasyonu ve Yanıtı (SOAR) platformlarıyla olan sinerjiyi vurgulamaktadır. 2025 yılında ve sonrasında ağ güvenliğinde dayanıklılığı sürdürmek için entegre, uyarlanabilir ve istihbarat odaklı bir yaklaşımın benimsenmesi kaçınılmazdır.

---

1. İzinsiz Giriş Tespit ve Önleme Sistemlerine (IDS/IPS) Giriş

Bu bölüm, IDS ve IPS'in temel işlevlerini, temel farklılıklarını ve tespit metodolojileri ile dağıtım türlerinin evrimini açıklayarak konuya dair temel bir anlayış sunmaktadır.

1.1. IDS ve IPS'in Tanımı: Temel İşlevsellik ve Ana Farklar

İzinsiz Giriş Tespit Sistemi (IDS):
Bir IDS, ağ trafiğini veya sistem aktivitelerini şüpheli kalıplar ve potansiyel güvenlik ihlalleri açısından izlemek için tasarlanmış yazılım veya donanım tabanlı bir siber güvenlik aracıdır.8 Pasif olarak çalışır, öncelikli olarak tespiti ve yöneticileri belirlenen tehditler konusunda uyarmayı hedefler ve veri akışına doğrudan müdahale etmez.9 IDS'in temel görevi, erken tehdit tespiti sağlamak, düzenleyici uyumluluk için ayrıntılı günlükler ve aktivite raporları oluşturmak ve maliyet etkin bir ilk savunma katmanı olarak hizmet etmektir.9 Bir tehdit tespit edildiğinde, olayı günlüğe kaydeder ve daha fazla araştırma için güvenlik ekiplerine veya bir SIEM sistemine uyarılar gönderir.9
İzinsiz Giriş Önleme Sistemi (IPS):
Bir IPS, IDS yeteneklerini temel alarak tehditleri yalnızca tespit etmekle kalmaz, aynı zamanda

ağın güvenliğini tehlikeye atmalarını aktif olarak önler.8 Ağ trafiğiyle aynı hat üzerinde (inline) çalışır, bu da kötü niyetli paketleri engelleme, bağlantıları sıfırlama veya hatta zararlı içeriği değiştirme gibi otomatik eylemler gerçekleştirmesine olanak tanır.8 IPS, fidye yazılımları, güvenlik açığı istismarları ve yanal hareket gibi çok çeşitli siber tehditlere karşı proaktif bir savunma sağlayarak gerçek zamanlı güvenliği artırır.14 Güvenlik ekiplerinin iş yükünü otomatik yanıtlarla azaltır.10
IDS ve IPS Arasındaki Temel Farklar:
Bu iki sistem arasındaki temel fark, çalışma modlarındadır: IDS pasif bir izleme aracı iken, IPS aktif bir kontrol mekanizmasıdır.8 IDS, ağ paketlerini değiştirmez veya engellemez, bu da meşru trafiğin kesintiye uğramamasını sağlar.8 Buna karşılık, IPS aktif olarak müdahale eder, bu da etkili olmasına rağmen, meşru aktiviteleri yanlışlıkla engelleme (yanlış pozitifler) ve potansiyel olarak ağda yavaşlamalara veya darboğazlara neden olma riskini taşır.8
Güvenlik duvarları, trafiği bağlantı noktası numarasına ve IP adresine göre filtreleyerek ilk savunma hattı görevi görür.[8] IDS ve IPS ise genellikle güvenlik duvarının arkasına yerleştirilir ve gerçek zamanlı trafiği daha derinlemesine inceleyerek trafik modellerini arar.[8] IPS, gerçek zamanlı engelleme sağlamak için ağ trafiğinin doğrudan yoluna konumlandırılırken, IDS, trafiğin kopyalarını analiz etmek için herhangi bir yere yerleştirilebilir.[10]

Bu sistemlerin evrimi, güvenlik katmanlarının artan karşılıklı bağımlılığını ortaya koymaktadır. Güvenlik duvarları, IDS ve IPS'in ayrı ancak tamamlayıcı roller üstlendiği sürekli olarak vurgulanmaktadır. Güvenlik duvarları temel çevre filtrelemesini sağlarken, IDS/IPS daha derin içerik ve davranış analizi sunar.[8] IPS işlevselliğinin Yeni Nesil Güvenlik Duvarlarına (NGFW) entegrasyonu [2] gibi gelişmeler, yakınlaşan güvenlik çözümlerine yönelik bir eğilimi işaret etmektedir. Bu durum, yönetim karmaşıklığını azaltırken, sağlam bir şekilde tasarlanmadığı takdirde tek bir hata noktası yaratma riskini de beraberinde getirir. Kullanıcı sorgusunda bahsedilen "basit Python tabanlı IDS" gibi temel bir araç, gerçek dünya dağıtımlarında çok daha karmaşık ve entegre bir ekosistem içinde yer almaktadır. Kuruluşların 2025 yılında, birden fazla işlevi (güvenlik duvarı, IPS, hatta SIEM/SOAR gibi) tek bir entegre çözümde birleştiren birleşik güvenlik platformlarına yönelmesi beklenmektedir.

Tablo 1: IDS ve IPS: Karşılaştırmalı Bir Genel Bakış

Parametre	İzinsiz Giriş Tespit Sistemi (IDS)	İzinsiz Giriş Önleme Sistemi (IPS)
Amaç	Şüpheli aktiviteyi izler ve tespit eder, uyarı verir.	Tespit edilen tehditleri inceler ve önler.

Çalışma	Pasif modda çalışır, trafiği etkilemez.	Aktif olarak trafiği kontrol eder ve müdahale eder.
Yanıt	Yöneticilere uyarı gönderir, olayı günlüğe kaydeder.	Kötü amaçlı paketleri engeller, bağlantıları sıfırlar, kaynak adresleri engeller.
Ağ Etkisi	Minimum ağ etkisi, meşru trafiği kesintiye uğratmaz.	Ağ performansını yavaşlatabilir, yanlış pozitiflerde meşru trafiği engelleyebilir.
Tipik Konum	Güvenlik duvarının arkasında (trafik kopyalarını analiz etmek için herhangi bir yerde olabilir).	Güvenlik duvarından hemen sonra, iç ağa giden doğrudan trafik yolunda.
Evrim	Daha erken tanıtıldı (1984-1986).	Daha sonra tanıtıldı (2000'lerin ortaları).

1.2. Tespit Metodolojilerinin Evrimi: İmza Tabanlı, Anomali Tabanlı ve Davranışsal Analiz

IDS/IPS sistemlerinin etkinliği, kullandıkları tespit metodolojilerine bağlıdır. Zamanla bu metodolojiler, siber tehditlerin artan karmaşıklığına yanıt olarak önemli ölçüde gelişmiştir.

İmza Tabanlı Tespit:
Bu metodoloji, belirli kötü niyetli aktivitelerle (örneğin, kötü amaçlı yazılım kodu, belirli paket başlıkları, saldırı komutları) ilişkilendirilen bilinen saldırı "imzaları" veritabanına dayanır.9 IDS/IPS, gelen ağ trafiğini veya sistem olaylarını bu veritabanıyla karşılaştırır; bir eşleşme bulunursa, bir uyarı tetiklenir veya önleme eylemi başlatılır.23

- **Güçlü Yönleri:** Bilinen tehditleri yüksek doğrulukla ve nispeten düşük hesaplama maliyetiyle tespit etmede oldukça etkilidir.[12] Yerleşik tehditlere karşı neredeyse gerçek zamanlı koruma sağlar.[23]
- **Zayıf Yönleri:** Temel sınırlaması, veritabanında imzası bulunmayan yeni veya "sıfır gün" saldırılarını (daha önce bilinmeyen güvenlik açıkları veya kötü amaçlı yazılım varyantları) tespit edememesidir.[9] Gelişen tehditlere karşı etkinliğini sürdürmek için imza veritabanının sürekli ve genellikle manuel olarak güncellenmesini gerektirir.[9]

Anomali Tabanlı Tespit:
Bu yaklaşım, öncelikle normal ağ veya sistem davranışının bir "temelini" oluşturur ve tipik aktivite kalıplarını izleyerek ve öğrenerek çalışır.9 Daha sonra, gelen trafiği veya olayları bu temel ile sürekli olarak karşılaştırır. Oluşturulan normdan önemli herhangi bir sapma, bir anomali ve potansiyel bir tehdit olarak işaretlenir.9

- **Güçlü Yönleri:** En önemli avantajı, önceden tanımlanmış imzaları olmayan yeni, bilinmeyen veya sıfır gün saldırılarını tespit edebilmesidir, çünkü belirli kalıplar yerine olağandışı davranışları tanımlar.[9] Ağ ortamlarındaki değişikliklere karşı esneklik ve uyarlanabilirlik sunar.[12]
- **Zayıf Yönleri:** Anomali tabanlı sistemler, özellikle temel oluşturma veya doğal ağ dalgalanmaları sırasında, meşru ancak olağandışı aktivitelerin yanlışlıkla tehdit olarak işaretlenmesi nedeniyle daha yüksek oranda yanlış pozitif üretme eğilimindedir.[9] Ayrıca, temel oluşturma ve sürekli izleme için önemli kaynaklar gerektirdiğinden hesaplama açısından yoğundurlar.[12]

Davranışsal Analiz (Genellikle Anomali Tabanlı ile Entegre):
Bu metodoloji, şüpheli kalıpları tespit etmek için kullanıcıların, uygulamaların ve ağ varlıklarının zaman içindeki davranışlarını analiz etmeye odaklanır.16 Normal davranış profilleri oluşturmak için makine öğreniminden yararlanır ve kötü niyetli aktiviteyi gösteren sapmaları belirler.16

- **Önemi:** Basit trafik kalıplarının ötesine geçerek aktivitelerin "amacını" anlamayı amaçlar, bu da onu karmaşık, çok aşamalı saldırılara ve içeriden gelen tehditlere karşı daha etkili hale getirir. Bu yaklaşım, genellikle yanal hareket ve olağandışı şifreleme aktiviteleri içeren gelişmiş kalıcı tehditleri (APT) ve fidye yazılımlarını belirlemek için kritik öneme sahiptir.[16]

Politika Tabanlı Tespit:
Bağımsız bir yöntem olarak daha az yaygın olan bu yaklaşım, önceden tanımlanmış güvenlik politikalarını uygular. Bu belirlenmiş politikaları ihlal eden aktiviteler engellenir veya işaretlenir.26 Bu, güvenlik ilkelerinin başlangıçta dikkatli bir şekilde yapılandırılmasını gerektirir.
Yanlış pozitifler (meşru aktivitenin kötü niyetli olarak işaretlenmesi) ve yanlış negatifler (kötü niyetli aktivitenin gözden kaçırılması) arasındaki doğal ödünleşme, çeşitli kaynaklarda sürekli olarak vurgulanmaktadır.[12] İmza tabanlı sistemler bilinen tehditler için daha az yanlış negatif üretirken, sıfır gün saldırılarını kaçırır. Anomali tabanlı sistemler sıfır gün saldırılarını yakalayabilir ancak daha fazla yanlış pozitif üretir. Bu temel sınırlama, birleşik yaklaşımlara duyulan ihtiyacı artırmaktadır.

2025 yılında, sağlam bir IDS/IPS stratejisi, "hibrit" bir tespit modelini gerektirecektir.[12] Bu model, bilinen tehditler için imza tabanlı tespitin verimliliğini, yeni ve sofistike saldırıları belirlemek için anomali ve davranışsal analizin (genellikle AI/ML destekli) uyarlanabilir yetenekleriyle birleştirir. Buradaki zorluk, bu metodolojileri etkili bir şekilde

entegre etmek ve hem yanlış pozitifleri hem de yanlış negatifleri en aza indirmek için sürekli olarak ayarlamaktır; bu da güvenlik ekiplerinin operasyonel verimliliğini doğrudan etkiler.[1]

Tablo 2: IDS/IPS Tespit Metodolojileri: Güçlü ve Zayıf Yönler

Metodoloji	Mekanizma (Kısa)	Güçlü Yönler	Zayıf Yönler
İmza Tabanlı	Bilinen kalıplarla karşılaştırır.	Bilinen tehditlerde etkili, düşük yanlış pozitif (bilinenler için), düşük hesaplama maliyeti.	Sıfır gün/varyantlara karşı etkisiz, sürekli güncelleme gerektirir, yüksek yanlış negatif (bilinmeyenler için).
Anomali Tabanlı	Normal davranış temelini oluşturur, sapmaları işaretler.	Bilinmeyen/yeni tehditleri tespit eder, esnek.	Yüksek yanlış pozitif, hesaplama açısından yoğun, temel oluşturma zorluğu.
AI/ML Destekli (Davranışsal Analiz)	Verilerden öğrenir, karmaşık kalıpları tanımlar.	Daha yüksek doğruluk, azaltılmış yanlış pozitif, sıfır gün tespiti, otomatik yanıt, sürekli iyileşme.	Yüksek hesaplama gereksinimleri, veri kalitesi sorunları, yorumlanabilirlik (kara kutu), düşmanca saldırılara karşı savunmasızlık.

1.3. IDS/IPS Dağıtım Türleri

IDS/IPS sistemleri, bir ağ içindeki konumlarına ve izledikleri trafiğin türüne göre çeşitli şekillerde dağıtılabilir. Bu farklı dağıtım türleri, modern siber güvenlik stratejilerinde çok katmanlı bir savunma yaklaşımının gerekliliğini vurgulamaktadır.

Ağ Tabanlı İzinsiz Giriş Tespit/Önleme Sistemleri (NIDS/NIPS):
Bu sistemler, ağ segmentleri arasında akan trafiği izlemek için bir ağ içindeki stratejik noktalara (örneğin, ağ anahtarları, hub'lar veya ağ geçitleri) dağıtılır.1 NIDS/NIPS, ağ paketlerini gerçek zamanlı olarak analiz eder, şüpheli kalıplar veya anormallikler için başlıkları ve yükleri inceler.22 Hizmet Reddi (DoS) saldırıları, bağlantı noktası taramaları ve botnet aktiviteleri gibi ağ çapındaki saldırıları tespit etmede etkilidirler.22

- **Güçlü Yönleri:** Ana bilgisayar tabanlı sistemlere kıyasla güvenliği daha kolaydır ve saldırganlar tarafından keşfedilmesi daha zordur.[22] Ağ genelinde geniş görünürlük sağlarlar.

- **Zayıf Yönleri:** Yüksek trafik hacimleri tarafından aşırı yüklenebilirler, bu da potansiyel olarak kaçırılan saldırılara (yanlış negatifler) yol açabilir.[19] Şifreli trafiği analiz etmekte genellikle zorlanırlar, bu da güvenlikte kör noktalar yaratır.[13]

Ana Bilgisayar Tabanlı İzinsiz Giriş Tespit/Önleme Sistemleri (HIDS/HIPS):
Bu sistemler, tek tek ana bilgisayar makinelerine (sunucular, iş istasyonları, uç noktalar) doğrudan kurulur ve o ana bilgisayara özgü aktiviteleri izler.1 HIDS/HIPS, kötü niyetli davranışları tespit etmek için sistem günlüklerini, dosya bütünlüğünü, süreç yürütmeyi ve kullanıcı aktivitelerini analiz eder.22 Bir saldırıya hangi süreçlerin veya kullanıcıların dahil olduğunu ortaya çıkarabilirler.22

- **Güçlü Yönleri:** Dahili ana bilgisayar aktivitelerine ayrıntılı görünürlük sağlarlar ve ağ düzeyindeki savunmaları atlayan saldırıları tespit edebilirler.[22]
- **Zayıf Yönleri:** Ana bilgisayarın kendisi tehlikeye girerse, HIDS/HIPS de zayıflatılabilir.[22] Ana bilgisayardan kaynak tüketirler ve birçok uç noktada yönetilmesi karmaşık olabilir.

Kablosuz İzinsiz Giriş Önleme Sistemleri (WIPS):
Bunlar, kablosuz ağ trafiğini izlemek ve güvenliğini sağlamak için özel olarak tasarlanmış sistemlerdir.21 WIPS, kablosuz iletişimleri hedef alan anormallikleri, yetkisiz erişimi ve saldırıları, örneğin sahte erişim noktalarını veya Wi-Fi ağlarına yönelik hizmet reddi saldırılarını tespit eder.21
Protokol Tabanlı (PIDS) / Uygulama Protokol Tabanlı (APIDS):
Bunlar, belirli ağ protokollerini (PIDS) veya uygulama katmanı protokollerini (APIDS) beklenen davranıştan sapmalar açısından izleyen ve analiz eden özel IDS türleridir.10 Belirli hizmetler için daha derinlemesine inceleme sunarlar.
Çeşitli dağıtım türlerinin (ağ, ana bilgisayar, kablosuz) varlığı, tek bir savunma noktasının yeterli olmadığını göstermektedir. Tehditler dışarıdan, içeriden veya belirli cihazları hedef alarak ortaya çıkabilir.[28] Uzaktan çalışmanın ve bulut ortamlarının yükselişi, saldırı yüzeyini daha da merkezsizleştirmektedir.[1] Bu durum, 2025 yılı için kapsamlı bir ağ güvenliği stratejisinin, çok katmanlı, "derinlemesine savunma" yaklaşımını benimsemesini gerektirmektedir.[20] Bu, ağ çevrelerinde ve kritik dahili segmentlerde NIDS/NIPS ile hassas sunucular ve uç noktalarda HIDS/HIPS'in bir kombinasyonunun dağıtılması anlamına gelir. Kablosuz ve IoT cihazlarının artan yaygınlığı da özel WIPS çözümlerini gerekli kılmaktadır. Bu katmanlı yaklaşım, bir savunma mekanizması atlatılsa bile, tehdidi tespit etmek ve azaltmak için başka mekanizmaların mevcut olmasını sağlayarak yedeklilik ve dayanıklılık sunar.[20]

---

2. Ağ Güvenliğinde IDS/IPS'in Mevcut Durumu (2025 Perspektifi)

Bu bölüm, IDS/IPS'in güncel avantajlarını ve doğal sınırlamalarını eleştirel bir şekilde

değerlendirerek 2025 için gerçekçi bir bakış açısı sunmaktadır.

2.1. Modern IDS/IPS'in Güçlü Yönleri ve Avantajları

Modern İzinsiz Giriş Tespit ve Önleme Sistemleri (IDS/IPS), siber güvenlik savunmalarının vazgeçilmez bileşenleri olarak önemli avantajlar sunmaktadır.

- **Erken Tehdit Tespiti:** IDS/IPS, ağ trafiğinin sürekli gözetimini sağlayarak şüpheli kalıpların, bilinen saldırı imzalarının veya davranışsal anormalliklerin erken belirlenmesini mümkün kılar.[9] Bu, kuruluşların tehditler tam teşekküllü ihlallere dönüşmeden önce yanıt vermesine olanak tanır.[9] Gerçek zamanlı gözlemler, güvenlik ekiplerinin olağandışı davranışları anında fark etmesi için kritik öneme sahiptir.[13]
- **Düzenleyici Uyumluluk ve Raporlama:** IDS/IPS, ayrıntılı günlükler ve aktivite raporları oluşturarak kuruluşların çeşitli düzenleyici standartlara (örneğin, NIST, GDPR, PCI DSS) uymalarına ve hesap verebilirliği ve denetim hazırlığını sağlamalarına yardımcı olur.[3] Bu raporlar, güvenlik olaylarının kanıtını sağlar ve uyumluluk denetimlerini kolaylaştırır.
- **Maliyet Etkin Bir Savunma Katmanı:** Tek başına tam bir çözüm olmasalar da, IDS/IPS, ekipleri ortaya çıkan riskler konusunda uyararak potansiyel zararı önemli ölçüde azaltabilen hızlı bir ilk koruma hattı sunar ve böylece potansiyel bir ihlalin genel maliyetini düşürür.[9]
- **Daha Geniş Güvenlik Çözümleriyle Entegrasyon:** Modern IDS/IPS, özellikle Güvenlik Bilgileri ve Olay Yönetimi (SIEM) sistemleri ve Güvenlik Orkestrasyonu, Otomasyonu ve Yanıtı (SOAR) platformları gibi diğer güvenlik araçlarıyla sorunsuz bir şekilde entegre olacak şekilde tasarlanmıştır.[5] Bu entegrasyon, genel durumsal farkındalığı artırır ve koordineli, otomatik yanıtları mümkün kılar.
- **Proaktif Savunma (IPS):** IPS, şüpheli ağ trafiğini aktif olarak izler ve engeller, yetkisiz erişimi, saldırıları ve istismarları gerçek zamanlı olarak önler.[14] Bu proaktif yetenek, sistem kesinti süresini ve hasarı en aza indirmeye yardımcı olur ve kritik verilerin, sistemlerin ve kaynakların korunmasını sağlar.[14]
- **Ortaya Çıkan Tehditlere Uyarlanabilirlik (Anomali Tabanlı):** Anomali tabanlı IDS/IPS, özellikle makine öğreniminden yararlananlar, normal ağ aktivitelerine uymayan yeni tehditleri, imza tabanlı sistemlerin kaçıracağı sıfır gün saldırıları da dahil olmak üzere tespit edebilir.[9] Bu, evrimleşen tehdit ortamına karşı daha dinamik bir savunma sağlar.

IDS'in geleneksel olarak tespiti odaklanmasına rağmen, IPS'e evrimi ve SIEM/SOAR ile entegrasyonu [5], aktif önleme ve otomatik yanıta doğru açık bir stratejik değişimi göstermektedir. Bu, tehditleri yalnızca tanımlamaktan, aktif olarak dayanıklılık oluşturmaya ve etkilerini en aza indirmeye yönelik bir değişimi işaret eder. Azaltılmış

kesinti süresi ve geliştirilmiş güvenlik gibi faydalar [14] bu yönelimi pekiştirmektedir. 2025 yılında, IDS/IPS'in değer teklifi basit uyarının ötesine geçmektedir. Kuruluşlar, erken tespitin hemen ardından otomatik veya orkestrasyonlu önleme ve yanıtın geldiği bütünsel bir "dijital dayanıklılık" stratejisine katkıda bulunan çözümlere giderek daha fazla öncelik verecektir. Bu, bir IDS/IPS'in "başarısının" sadece bir saldırıyı tespit etmekle ilgili olmadığını, aynı zamanda onu (veya entegre güvenlik ekosistemini) ne kadar hızlı ve etkili bir şekilde etkisiz hale getirebildiği ve normal operasyonları geri yükleyebildiği ile ilgili olduğunu ifade eder.

2.2. Geleneksel IDS/IPS'in Doğal Zayıf Yönleri ve Sınırlamaları

IDS/IPS sistemleri önemli avantajlar sunsa da, etkinliklerini etkileyen ve dikkatli yönetimi gerektiren doğal zayıf yönlere ve sınırlamalara sahiptir.

- **Yüksek Yanlış Pozitif Oranları:** Özellikle anomali tabanlı sistemler için önemli bir dezavantaj, çok sayıda yanlış alarm üretmesidir. Bu durum, güvenlik ekiplerini bunaltabilir ve meşru tehditlerin gürültü arasında gözden kaçırılmasına neden olan "uyarı yorgunluğuna" yol açabilir.[1] Bir IPS'ten gelen yanlış pozitifler, meşru işlevleri yanlışlıkla engelleyebilir ve operasyonel kesintilere neden olabilir.[18]
- **Sınırlı Eylem Yeteneği (IDS):** Geleneksel IDS araçları yalnızca tespit ve uyarıya odaklanır. Saldırıları kendi başlarına engelleme veya azaltma yeteneğinden yoksundurlar, bu da aktif yanıt için manuel müdahale veya IPS veya SIEM/SOAR gibi diğer araçlarla entegrasyon gerektirir.[9] Bu, onları öncelikli olarak reaktif hale getirir.[9]
- **Kaynak Talepleri:** Bir IDS/IPS'i sürdürmek kaynak yoğun olabilir. Gerçek zamanlı veri analizi için önemli hesaplama gücü ve bant genişliği, sık yükseltmeler, izleme ve analiz için bilgili personel ve kapsamlı kapsama alanı için hassas sensör yerleşimi gerektirir.[9] Bu durum, ağ performansını ve BT kaynaklarını zorlayabilir.[12]
- **Şifreli Trafik İçin Sınırlı Görünürlük:** Önemli bir engel, şifreli trafiği izlemedeki zorluktur. Şifreleme verileri korurken, aynı zamanda kötü niyetli aktiviteyi de gizleyebilir ve IDS/IPS için kör noktalar oluşturabilir; bu durum, şifre çözme proxy'leri veya gelişmiş davranışsal analiz kullanılmadıkça geçerlidir.[13]
- **Yeni/Sıfır Gün Saldırılarına Karşı Savunmasızlık (İmza Tabanlı):** İmza tabanlı sistemler, bilinen tehditleri tespit etmekle sınırlıdır. Mevcut imzaları olmayan yeni, daha önce görülmemiş saldırılara veya varyantlara karşı etkisizdirler, bu da önemli bir güvenlik açığı penceresi bırakır.[12]
- **Yönetim ve Bakım Karmaşıklığı:** IDS/IPS tarafından üretilen büyük hacimli veriler, sürekli güncellemeler, ince ayar ve uyarıların yorumlanması ihtiyacıyla birleştiğinde, özel uzmanlık ve sürekli operasyonel gider gerektirir.[1]
- **Darboğaz Potansiyeli (IPS):** IPS, ağ trafiğiyle aynı hat üzerinde çalıştığı için, IPS

veya altta yatan ağ altyapısı beklenen trafik verimini işleyemezse, bir darboğaz haline gelebilir ve ağ yavaşlamalarına veya IPS'in çökmesi durumunda sistem arızalarına yol açabilir.[18]

Birden fazla kaynak, yanlış pozitiflerin uyarı yorgunluğuna yol açtığı zorluklara [9] ve ayarlama ve bakım için yetenekli personele duyulan ihtiyaca işaret etmektedir.[1] Bu durum, en gelişmiş teknolojinin bile ancak onu yöneten insan uzmanlığı kadar etkili olduğunu göstermektedir. Küresel siber güvenlik beceri açığı [1], bu sorunları daha da kötüleştirmektedir. 2025 yılında, insan faktörünü ele almak, IDS/IPS etkinliği için teknolojik gelişmeler kadar kritik olacaktır. Bu, yalnızca siber güvenlik uzmanlarına eğitim ve onları elde tutmaya yatırım yapmakla kalmayıp, aynı zamanda tekrarlayan görevlerin yükünü azaltmak, insan hatasını en aza indirmek ve analistlerin yüksek öncelikli, karmaşık araştırmalara odaklanmasını sağlamak için otomasyondan (örneğin, AI/ML, SOAR) yararlanmayı da içerir.[5] İnsan faktörü hem en zayıf halka (uyarı yorgunluğu veya beceri eksikliği yoluyla) hem de en güçlü varlık (uzman analizi ve stratejik karar verme yoluyla) olabilir.

---

3. 2025 ve Sonrasında IDS/IPS'i Şekillendiren Temel Eğilimler

Bu bölüm, IDS/IPS'in geleceğini etkileyen dönüştürücü eğilimleri derinlemesine incelemekte, potansiyel etkilerini ve uygulama alanlarını vurgulamaktadır.

3.1. Tehdit Tespitinde Yapay Zeka ve Makine Öğreniminin Yükselişi

Nedir: Yapay zeka (AI) tabanlı IDS/IPS, büyük miktarda ağ trafiği ve sistem verisini analiz etmek için makine öğrenimi (ML) ve derin öğrenme (DL) algoritmalarını kullanır. Bu sistemler, geçmiş verilerden öğrenerek normal davranış profilleri oluşturur, ince anormallikleri tespit eder, karmaşık saldırı kalıplarını belirler ve hatta potansiyel tehditleri tahmin eder.[12]

Nasıl Çalışır: ML modelleri (denetimli, denetimsiz, yarı denetimli), kötü niyetli aktiviteyi veya normdan sapmaları belirlemek için etiketli veya etiketsiz veri kümeleri üzerinde eğitilir. Derin öğrenme modelleri (CNN'ler, RNN'ler, Otoenkoderler) özellikle yüksek boyutlu verileri işlemekte ve karmaşık, çok aşamalı saldırı kalıplarını ortaya çıkarmakta ustadır.[12]

Neden Önemlidir: AI/ML, geleneksel imza tabanlı sistemlerin sınırlamalarını aşmak için kritik öneme sahiptir, özellikle yeni, bilinmeyen ve sıfır gün saldırılarını tespit etmede.[12] Sınıflandırma doğruluğunu artırarak ve yüksek güvenilirlikli uyarıları önceliklendirerek yanlış pozitifleri önemli ölçüde azaltır ve uyarı yorgunluğuyla mücadele eder.[12] AI ayrıca

otomatik tehdit yanıtını ve tespit yeteneklerinin sürekli iyileştirilmesini sağlar.[7]

2025'teki Potansiyel Etkileri ve Uygulama Alanları:

- **Gelişmiş Sıfır Gün ve APT Tespiti:** Yapay zeka destekli IDS/IPS, ince davranışsal değişimleri tanımlayarak sofistike, daha önce görülmemiş saldırılara ve gelişmiş kalıcı tehditlere karşı birincil savunma olacaktır.[12]
- **Otomatik Olay Yanıtı:** Yapay zeka, tehlikeye atılmış uç noktaları izole etme, kötü niyetli e-postaları silme veya güvenlik duvarı kurallarını güncelleme gibi eylemleri giderek daha fazla otomatikleştirecek ve yanıt sürelerini önemli ölçüde azaltacaktır.[7]
- **Azaltılmış Uyarı Yorgunluğu:** Sınıflandırma doğruluğunu artırarak ve yüksek güvenilirlikli uyarıları önceliklendirerek, yapay zeka güvenlik analistlerini kritik olaylara odaklanmaları için serbest bırakacaktır.[12]
- **Proaktif Tehdit Avcılığı:** Yapay zeka, güvenlik açıklarını ve potansiyel saldırı vektörlerini istismar edilmeden önce belirlemek için büyük veri kümelerini analiz edebilir, güvenliği reaktiften proaktife kaydırır.[7]
- **Zorluklar:** Eğitim ve gerçek zamanlı tespit için yüksek hesaplama gereksinimleri (CPU, GPU, bellek), veri gizliliği endişeleri, "kara kutu" sorunu (yorumlanabilirlik eksikliği) ve düşmanca saldırılara karşı savunmasızlık zorluklar olarak kalmaya devam etmektedir.[12]

Güvenilir Kaynak: "Comparison of Traditional vs. AI-Based Intrusion Detection and Prevention Systems: Efficiency and Accuracy" (Oluwaseyi Joseph ve Raymond Ajax, Mart 2025) [12]; Otorio.com Blog [9]; AI Multiple [16]; ResearchGate [12]; ControlAudits.com [25]; APUS.edu.[22]

3.2. Bulut Tabanlı IDS/IPS Çözümlerine Geçiş

Nedir: Bulut tabanlı IDS/IPS çözümleri, şirket içi donanım veya yazılım kurulumu gerektirmeyen, bulut üzerinden sunulan güvenlik hizmetleridir. Bulut ortamlarındaki, hibrit ve çoklu bulut altyapılarındaki ağ trafiğini ve sistem aktivitelerini izler ve korurlar.[1]

Nasıl Çalışır: Bu çözümler, çeşitli bulut hizmetlerinden, sanal makinelerden ve konteynerlerden güvenlik günlüklerini ve ağ trafiğini toplamak, analiz etmek ve işlemek için bulut bilişimin ölçeklenebilirliğinden ve dağıtılmış yapısından yararlanır. Genellikle yerel görünürlük ve kontrol için bulut sağlayıcı API'leriyle doğrudan entegre olurlar.[1]

Neden Önemlidir: Bulut bilişimin yaygın olarak benimsenmesi (2025 yılına kadar kuruluşların %90'ının çoklu bulut ortamlarından yararlanması bekleniyor) ve bulut tabanlı hizmetlere artan bağımlılık, bu dinamik ve dağıtılmış ortamları koruyabilecek

güvenlik çözümlerini zorunlu kılmaktadır.[1] Geleneksel şirket içi IDS/IPS, bulut iş yüklerinin ölçeği ve geçici doğasıyla başa çıkmakta zorlanmaktadır.

2025'teki Potansiyel Etkileri ve Uygulama Alanları:

- **Ölçeklenebilirlik ve Esneklik:** Bulut tabanlı IDS/IPS, değişen veri hacimlerine ve ağ taleplerine kolayca uyum sağlayabilir, bu da onları büyüyen kuruluşlar ve dalgalanan iş yükleri için ideal hale getirir.[1]
- **Maliyet Etkinliği:** Şirket içi çözümlerle ilişkili önemli donanım yatırımı ve sürekli bakım maliyetlerini azaltır, tipik olarak abonelik tabanlı bir modelle çalışır.[1]
- **Bulut Ortamlarında Gelişmiş Görünürlük:** Buluta özgü çözümler, geleneksel araçların kaçırabileceği buluta özgü tehditlere, yanlış yapılandırmalara ve uyumluluk sorunlarına daha derinlemesine görünürlük sağlar.[29]
- **Uzaktan Çalışma Güvenliği:** Uzaktan çalışan işgücünü ve dağıtılmış ekipleri güvence altına almak için çok uygundur, kullanıcının konumundan bağımsız olarak tutarlı güvenlik politikaları sağlar.[29]
- **Pazar Büyümesi:** Bulut tabanlı IDS/IPS çözümlerinin, bulut güvenliğine olan talep nedeniyle 2025 yılına kadar uygulamaların %30'undan fazlasını oluşturması beklenmektedir.[6]

Güvenilir Kaynak: DataGuard.com [13]; DataInsightsMarket.com [1]; ArchiveMarketResearch.com [2]; GlobalGrowthInsights.com [6]; SentinelOne.com [29]; Splunk.com.[5]

3.3. Sıfır Güven Mimarileriyle Entegrasyon

Nedir: Sıfır Güven, "asla güvenme, her zaman doğrula" ilkesine dayanan bir güvenlik modelidir.[3] Tehditlerin ağ çevresinin hem içinden hem de dışından gelebileceğini varsayar. Bu nedenle, kaynaklara erişmeye çalışan her kullanıcı, cihaz ve uygulama, konumlarından bağımsız olarak sürekli olarak kimlik doğrulaması, yetkilendirme ve izlemeye tabi tutulmalıdır.[20]

Nasıl Çalışır: Sıfır Güven, en az ayrıcalıklı erişim (minimum gerekli izinlerin verilmesi), kullanıcı/cihaz aktivitesinin sürekli kimlik doğrulaması ve izlenmesi ve mikro segmentasyon (ağları daha küçük, izole edilmiş bölgelere ayırma) gibi ilkelere dayanır.[20] IDS/IPS, Sıfır Güven'in "sürekli izleme" yönünde kritik bir rol oynar.

Neden Önemlidir: Geleneksel çevre tabanlı güvenlik modelleri, özellikle uzaktan çalışmanın ve bulut benimsemesinin artmasıyla modern, sofistike tehditlere karşı artık etkili değildir.[3] Sıfır Güven, doğal güveni ortadan kaldırarak ve katı erişim kontrolleri uygulayarak bu temel kusuru giderir, siber riski önemli ölçüde azaltır.[31] Gartner, 2025

yılına kadar kuruluşların %60'ından fazlasının Sıfır Güven ilkelerini benimseyeceğini tahmin etmektedir.[3]

2025'teki Potansiyel Etkileri ve Uygulama Alanları:

- **Gelişmiş Tehdit Tespiti:** IDS/IPS, özellikle davranışsal analitik ve yapay zeka ile, Sıfır Güven çerçevesinde sürekli izlemeye katkıda bulunur, belirlenen politikaları ihlal eden veya bir ihlali gösteren anormallikleri ve şüpheli davranışları tanımlar.[20]
- **Sınırlı Yanal Hareket:** Ağları segmentlere ayırarak (mikro segmentasyon) ve erişimi sürekli doğrulayarak, IDS/IPS, ilk bir ihlal meydana gelse bile saldırganların ağ içinde yanal olarak hareket etmesini tespit etmeye ve önlemeye yardımcı olabilir.[20]
- **Ayrıntılı Erişim Kontrolü:** IDS/IPS uyarıları, şüpheli aktivite tespit edildiğinde erişimi kısıtlayarak en az ayrıcalık ilkesini pekiştiren erişim politikalarında dinamik ayarlamalar hakkında bilgi sağlayabilir.[20]
- **Proaktif Güvenlik Durumu:** Sıfır Güven'in "ihlalleri varsay" ilkesi, IDS/IPS'in hızlı tespit ve yanıt rolüyle uyumlu olup, güvenlik olaylarının etkisini en aza indirir.[31]

Güvenilir Kaynak: FluidAttacks.com [31]; Faddom.com [20]; SPS.WFU.edu [3]; SentinelOne.com.[29]

3.4. Gelişmiş Tespit İçin Siber Tehdit İstihbaratından (CTI) Yararlanma

Nedir: Siber Tehdit İstihbaratı (CTI), mevcut veya ortaya çıkan siber tehditler hakkında organize edilmiş, analiz edilmiş ve eyleme dönüştürülebilir bilgilerdir. Ham verileri, kuruluşların tehdit aktörlerinin motivasyonlarını, taktiklerini, tekniklerini ve prosedürlerini (TTP'ler) anlamalarına yardımcı olan ve proaktif savunmayı mümkün kılan bilgilere dönüştürür.[7]

Nasıl Çalışır: CTI platformları, çeşitli kaynaklardan (açık kaynak, ticari beslemeler, karanlık ağ, IDS/IPS verileri dahil dahili günlükler) veri toplar ve birleştirir. Bu ham veriler daha sonra kalıpları tanımlamak, tehditleri bağlamsallaştırmak ve eyleme dönüştürülebilir bilgiler üretmek için makine öğrenimi ve gelişmiş analitik kullanılarak analiz edilir.[7] Bu bilgiler uyarılar olarak yayılır veya doğrudan IDS/IPS gibi güvenlik sistemlerine entegre edilir.

Neden Önemlidir: Siber saldırıların artan karmaşıklığı ve hacmi, istihbarat odaklı savunmaları zorunlu kılmaktadır.[1] CTI, saldırıları tahmin etmek, güvenlik açıklarını önceliklendirmek ve bilinçli güvenlik kararları almak için öngörü sağlar ve reaktif yanıtlardan öteye geçer.[7] Uyarıları bağlamsallaştırarak yanlış pozitifleri azaltmaya yardımcı olur.[32]

2025'teki Potansiyel Etkileri ve Uygulama Alanları:

- **Gelişmiş IDS/IPS Doğruluğu:** Güncel IOC'leri (Saldırı Göstergeleri) ve TTP'leri IDS/IPS'e besleyerek, CTI, bilinen ve ortaya çıkan tehditleri daha yüksek hassasiyetle tespit etme yeteneklerini artırır, yanlış negatifleri ve yanlış pozitifleri azaltır.[7]
- **Proaktif Savunma Yapılandırması:** CTI, güvenlik ekiplerinin saldırıların meydana gelmesini beklemeden, beklenen tehditlere dayalı olarak IDS/IPS kurallarını ve politikalarını proaktif olarak yapılandırmasını sağlar.[7]
- **Daha Hızlı Olay Yanıtı:** Eyleme dönüştürülebilir CTI, olaylara daha hızlı tespit ve yanıt verilmesini sağlayarak saldırganların ağlarda geçirdiği süreyi en aza indirir ve genel etkiyi azaltır.[7]
- **Genişletilmiş Tehdit İstihbaratı (XTI):** 2025 yılında CTI, IoT cihazları, Operasyonel Teknoloji (OT) ve tedarik zincirleri dahil olmak üzere daha geniş bir ekosistemden elde edilen bilgileri entegre eden XTI'ye dönüşmektedir ve tehdit ortamına bütünsel bir bakış açısı sunmaktadır.[7]

Güvenilir Kaynak: Exabeam.com [32]; Cyble.com.[7]

3.5. IoT Ortamlarının Güvenliğini Sağlamada IDS/IPS'in Rolü

Nedir: IoT (Nesnelerin İnterneti) cihazları, sensörler ve yazılımlarla gömülü, internet üzerinden veri bağlayan ve alışverişi yapan fiziksel nesnelerdir. IoT ortamlarının güvenliğini sağlamak, bu çeşitli cihazları, veri iletimlerini ve ağlarını siber tehditlerden korumayı içerir.[33]

Nasıl Çalışır: IDS/IPS, yetkisiz erişim girişimleri, olağandışı veri akışları veya botnet katılımı belirtileri gibi şüpheli aktiviteler için IoT cihazları tarafından üretilen ağ trafiğini izlemek üzere dağıtılır. Bilinen IoT güvenlik açıkları için imza tabanlı tespiti veya normal IoT cihazı davranışından sapmaları belirlemek için anomali tabanlı tespiti uygulayabilirler.[22]

Neden Önemlidir: IoT cihazlarının patlayıcı büyümesi (2025 yılına kadar 75 milyar cihaz bekleniyor), kuruluşlar için saldırı yüzeyini önemli ölçüde genişletmektedir.[7] Birçok IoT cihazı, sınırlı hesaplama kaynakları, gömülü kimlik bilgileri, seyrek güncellemeler ve güvensiz iletişim kanalları nedeniyle doğal güvenlik zayıflıklarına sahiptir.[33] Bu güvenlik açıkları, DoS, kaba kuvvet ve sıfır gün gibi saldırılar için onları birincil hedef haline getirir ve kritik sistemlere ağ geçidi olarak hizmet edebilirler.[33]

2025'teki Potansiyel Etkileri ve Uygulama Alanları:

- **IoT'ye Özgü Saldırıların Tespiti:** IDS/IPS, bağlantı noktası taraması, botnet

saldırıları ve IoT cihazlarından kaynaklanan veya bunları hedef alan DoS saldırılarını tespit edebilir.[22]

- **Ağ Segmentasyonu Uygulaması:** IDS/IPS, segmentlere ayrılmış IoT ağları ile kritik BT ağları arasındaki trafiği izleyebilir, bir IoT cihazının tehlikeye girmesi durumunda mikro segmentasyon politikalarını uygulamaya ve yanal hareketi sınırlamaya yardımcı olabilir.[34]
- **IoT Davranışı İçin Anomali Tespiti:** IoT cihazlarının genellikle tahmin edilebilir davranışları göz önüne alındığında, anomali tabanlı IDS/IPS, hassas finansal verilere erişmeye çalışan akıllı bir yazıcı gibi olağandışı aktiviteleri işaretlemede özellikle etkilidir.[34]
- **Zorluklar:** IoT cihazlarının, iletişim protokollerinin (Zigbee, Z-Wave, Bluetooth LE, WiFi), işletim sistemlerinin ve güncelleme yeteneklerinin çeşitliliği, tutarlı IDS/IPS dağıtımını ve yönetimini karmaşıklaştırmaktadır.[34] Birçok IoT cihazındaki sınırlı işlem gücü de, doğrudan cihaz üzerinde sağlam güvenlik özelliklerinin uygulanmasını kısıtlamaktadır.[33]

Güvenilir Kaynak: AMU.APUS.edu [22]; StationX.net [33]; Xobee.com [34]; Cyble.com.[7]

3.6. Birleşik Güvenlik Operasyonları İçin SIEM ve SOAR ile Sinerji

Nedir:

- **SIEM (Güvenlik Bilgileri ve Olay Yönetimi):** Bir kuruluşun ağ altyapısındaki çeşitli kaynaklardan (IDS/IPS, güvenlik duvarları, sunucular, uygulamalar dahil) günlük verilerini ve güvenlik olaylarını birleştiren, merkezileştiren ve analiz eden bir teknolojidir. Güvenlik duruşuna birleşik, gerçek zamanlı bir bakış açısı sunar ve geçmiş analizi sağlar.[5]
- **SOAR (Güvenlik Orkestrasyonu, Otomasyonu ve Yanıtı):** Önceden tanımlanmış "oyun kitapları" veya iş akışları uygulayarak güvenlik olaylarına yanıtı otomatikleştiren bir platformdur. Olay yanıtını kolaylaştırmak, manuel çabayı azaltmak ve azaltmayı hızlandırmak için SIEM ve diğer güvenlik araçlarıyla entegre olur.[5]

Nasıl Çalışır: IDS/IPS, tespit edilen izinsiz girişler veya şüpheli aktiviteler hakkında SIEM platformlarına uyarılar ve günlük verileri besleyerek kritik veri kaynakları olarak hareket eder. SIEM daha sonra bu olayları diğer kaynaklardan gelen verilerle ilişkilendirerek daha zengin bir bağlam sağlar, karmaşık saldırı kalıplarını tanımlar ve uyarıları önceliklendirir. SOAR platformları, SIEM'den gelen bu yüksek öncelikli uyarıları alır ve önceden tanımlanmış yanıt eylemlerini otomatik olarak tetikler.[5]

Neden Önemlidir: 2025 yılında, siber tehditlerin hacmi ve karmaşıklığı, izole edilmiş

güvenlik araçlarından daha fazlasını gerektirmektedir. SIEM ve SOAR, küresel siber güvenlik beceri açığını telafi ederek [5], ezici miktardaki güvenlik verisini yönetmek, uyarı yorgunluğunu azaltmak ve tehditlere hızlı, tutarlı yanıtlar vermek için gerekli otomasyonu ve orkestrasyonu sağlar.

2025'teki Potansiyel Etkileri ve Uygulama Alanları:

- **Gelişmiş Görünürlük ve Bağlam:** SIEM, farklı günlükleri merkezileştirerek, IDS/IPS'in tek başına sunamayacağı ağ aktivitesine bütünsel bir bakış açısı sağlar. Bu, güvenlik analistlerinin kötü niyetli aktörleri daha etkili bir şekilde tespit etmelerini ve tehditlere odaklanmalarını kolaylaştırır.[5]
- **Daha Hızlı ve Daha Verimli Olay Yanıtı:** SOAR, rutin görevleri otomatikleştirerek güvenlik ekiplerinin karmaşık sorunlara odaklanmasını sağlar. Bu, yanıt sürelerini önemli ölçüde azaltır ve ihlallerin hızla kontrol altına alınmasına ve hasarın en aza indirilmesine yardımcı olur.[5]
- **Azaltılmış Uyarı Yorgunluğu:** SIEM çözümleri, birden fazla olayı ilişkilendirerek ve risk tabanlı uyarılar uygulayarak yanlış pozitifleri azaltmaya yardımcı olur ve analistlerin gerçek tehditlere odaklanmasını sağlar.[5]
- **Uyumluluk ve Adli Bilişim:** SIEM'den gelen merkezileştirilmiş günlükler, adli soruşturmalar ve düzenleyici uyumluluk gereksinimlerini karşılamak için paha biçilmezdir.[5]
- **Zorluklar:** SIEM/SOAR'ın doğru şekilde uygulanması karmaşıktır, veri normalizasyonu, kapsamlı toplama kapsamı, etkili günlük analizi ve bakım ile yetenekli personel için önemli kaynaklar gerektirir.[27] Yanlış yapılandırma, meşru hizmetleri kesintiye uğratan otomatik yanıtlara yol açabilir.[27]

Güvenilir Kaynak: Otorio.com [9]; Cyber.gov.au [27]; Splunk.com.[5]

Tablo 3: 2025 ve Sonrası İçin IDS/IPS'teki Temel Eğilimler

Eğilim	Açıklama (2-3 Cümle)	2025'teki Etki/Uygulama Alanı	Ana Referans
Yapay Zeka ve Makine Öğreniminin Yükselişi	AI/ML, ağ trafiğini ve sistem verilerini analiz ederek normal davranış profilleri oluşturur, anormallikleri tespit eder ve tehditleri	Sıfır gün ve APT tespitinde büyük gelişme, otomatik olay yanıtı, uyarı yorgunluğunun azalması ve proaktif tehdit avcılığı.	[12]

	tahmin eder. Geleneksel imza tabanlı sistemlerin sınırlamalarını aşarak sıfır gün saldırılarını tespit etmede ve yanlış pozitifleri azaltmada kritik öneme sahiptir.		
Bulut Tabanlı IDS/IPS Çözümlerine Geçiş	Bu çözümler, bulut üzerinden sunulur ve bulut, hibrit ve çoklu bulut ortamlarındaki trafiği izler ve korur. Ölçeklenebilirlik, esneklik ve maliyet etkinliği sunarak geleneksel şirket içi sistemlerin zorluklarını giderir.	Ölçeklenebilirlik ve esneklik, maliyet etkinliği, bulut ortamlarında gelişmiş görünürlük ve uzaktan çalışma güvenliği için ideal.	6
Sıfır Güven Mimarileriyle Entegrasyon	"Asla güvenme, her zaman doğrula" ilkesine dayanan bir güvenlik modelidir. IDS/IPS, sürekli kimlik doğrulaması, en az ayrıcalıklı erişim ve mikro segmentasyon yoluyla sürekli izlemeye katkıda bulunur.	Gelişmiş tehdit tespiti, yanal hareketin sınırlanması, ayrıntılı erişim kontrolü ve proaktif güvenlik duruşu.	31
Siber Tehdit İstihbaratından (CTI) Yararlanma	CTI, mevcut veya ortaya çıkan tehditler hakkında eyleme dönüştürülebilir bilgiler sağlar. IDS/IPS'e güncel saldırı göstergeleri ve TTP'ler besleyerek tespit doğruluğunu artırır ve proaktif savunma	Gelişmiş IDS/IPS doğruluğu, proaktif savunma yapılandırması, daha hızlı olay yanıtı ve genişletilmiş tehdit istihbaratı (XTI) kapsamı.	7

	yapılandırmasını sağlar.		
IoT Ortamlarının Güvenliğini Sağlamadaki Rolü	IoT cihazlarının ağ trafiğini izleyerek yetkisiz erişim, olağandışı veri akışları veya botnet katılımı gibi şüpheli aktiviteleri tespit eder. Özellikle anomali tabanlı tespit, IoT davranışındaki sapmaları belirlemede etkilidir.	IoT'ye özgü saldırıların tespiti, ağ segmentasyonu uygulaması ve IoT davranışı için anomali tespiti.	[34]
SIEM ve SOAR ile Sinerji	SIEM, çeşitli kaynaklardan gelen günlük verilerini toplar ve analiz ederken, SOAR olay yanıtını otomatikleştirir. IDS/IPS, SIEM için kritik bir veri kaynağı görevi görür ve SOAR, SIEM'den gelen uyarıları temel alarak otomatik yanıtları tetikler.	Gelişmiş görünürlük ve bağlam, daha hızlı ve verimli olay yanıtı, azaltılmış uyarı yorgunluğu ve uyumluluk/adli bilişim desteği.	[27]

---

4. 2025'te Dayanıklı Bir Ağ Güvenliği Duruşu İçin Öneriler

Bu bölüm, kuruluşların IDS/IPS stratejilerini optimize etmeleri ve 2025 ve sonrasında sağlam bir ağ güvenliği duruşu oluşturmaları için eyleme dönüştürülebilir öneriler sunmaktadır.

4.1. Stratejik Dağıtım ve Hibrit Yaklaşımlar

Öneri: Kuruluşların, ağ çevrelerinde ve kritik dahili segmentlerde NIDS/NIPS'in güçlü yönlerini hassas ana bilgisayarlarda ve uç noktalarda HIDS/HIPS'in yetenekleriyle birleştiren hibrit bir IDS/IPS dağıtım modelini uygulamaları kritik öneme sahiptir. Ayrıca, imza tabanlı, anomali tabanlı ve AI/ML destekli davranışsal analizi entegre eden hibrit

bir tespit metodolojisi benimsenmelidir.

Gerekçe: Siber tehdit ortamının çeşitliliği ve sürekli evrimi göz önüne alındığında, tek bir IDS/IPS türü veya tespit yöntemi yeterli değildir.[12] NIDS/NIPS geniş ağ görünürlüğü sağlarken, HIDS/HIPS ayrıntılı ana bilgisayar düzeyinde bilgiler sunar.[22] Bilinen tehditler için imza tabanlı tespiti, sıfır gün saldırıları için yapay zeka destekli anomali tespitiyle birleştirmek, kapsamlı kapsama ve uyarlanabilirlik sağlar.[12]

2025'teki Etki: Bu katmanlı yaklaşım (derinlemesine savunma), tespit noktalarını ve yöntemlerini artırarak başarılı ihlal olasılığını önemli ölçüde azaltan yedeklilik ve dayanıklılık sağlar. Kuruluşların tüm dijital ayak izlerinde hem bilinen hem de yeni tehditleri tespit etmelerine olanak tanır.[20] Güvenlik stratejisinde "ya/ya da" zihniyetinden "hem/hem de" zihniyetine geçiş, modern güvenlik ortamında hayati önem taşımaktadır. IDS ve IPS arasındaki tarihsel ayrım ve imza ile anomali tespiti arasındaki tartışma giderek eskimektedir.[8] Modern güvenlik, bu yeteneklerin birleşmesini zorunlu kılmaktadır. Pazar eğilimleri, entegre çözümlere [2] ve hibrit tespit modellerine [12] doğru bir kaymayı göstermektedir. Bu, kuruluşların güvenlik araçları veya yöntemleri arasında seçim yapmaktan vazgeçmesi gerektiği anlamına gelir. Bunun yerine, farklı güvenlik katmanlarının ve tespit tekniklerinin sinerjik, uyarlanabilir bir savunma oluşturmak için nasıl birleştirilebileceği ve entegre edilebileceğine odaklanılmalıdır. Bu, IDS/IPS'in bağımsız ürünler değil, daha geniş, birbirine bağlı bir güvenlik ekosisteminin ayrılmaz bileşenleri olduğu bütünsel bir güvenlik mimarisi gerektirir.

4.2. Sürekli Optimizasyon ve Ayarlama

Öneri: IDS/IPS kurallarının, temel çizgilerinin ve uyarılarının sürekli ayarlanması ve optimizasyonu için özel bir görev gücü oluşturulmalı veya yönetilen güvenlik hizmetlerinden (MSSP) yararlanılmalıdır. Bu, imza veritabanlarının düzenli güncellemelerini, ağ değişikliklerine uyum sağlamak için anomali tespit temel çizgilerinin iyileştirilmesini ve yanlış pozitiflerin aktif olarak azaltılmasını içerir.

Gerekçe: IDS/IPS "kur ve unut" araçları değildir; etkinlikleri sürekli bakım ve ayarlama olmadan hızla azalır.[5] Yanlış pozitifler, uyarı yorgunluğuna ve kaynak israfına yol açarken, güncel olmayan imzalar yeni tehditleri kaçırır.[9] Anomali tespiti için temel çizgiler, meşru ağ evrimini yansıtacak şekilde sürekli olarak güncellenmelidir.[12]

2025'teki Etki: Proaktif ayarlama, IDS/IPS'in gelişen tehditlere karşı son derece doğru ve ilgili kalmasını sağlayarak, uyarı yorgunluğundan kaynaklanan operasyonel yükü en aza indirir ve gerçek tehditlerin tespitini en üst düzeye çıkarır. Bu, daha verimli güvenlik

operasyonları ve daha güçlü bir savunma duruşu anlamına gelir.

Güvenilir Kaynak: Otorio.com [9]; DataGuard.com [13]; SecurityMetrics.com [28]; InfosecInstitute.com [30]; Owasp.org [18]; Ubiquity.ACM.org [19]; NIST.gov [15]; FidelisSecurity.com [23]; Cyber.gov.au [27]; Splunk.com.[5]

4.3. Gelişmiş Analitik ve Otomasyona Yatırım

Öneri: Yapay zeka/makine öğrenimi destekli IDS/IPS çözümlerinin benimsenmesine öncelik verilmeli ve bunlar SIEM ve SOAR platformlarıyla entegre edilmelidir. Bu yatırım, daha derin tehdit bilgileri için gelişmiş analitikten ve hızlandırılmış yanıt için otomasyondan yararlanmaya odaklanmalıdır.

Gerekçe: Yapay zeka/makine öğrenimi, geleneksel yöntemleri atlayan yeni ve sofistike tehditleri tespit etmek için vazgeçilmezdir.[12] IDS/IPS'i SIEM ile entegre etmek, tüm BT ekosisteminden gelen güvenlik olaylarının merkezileştirilmiş görünürlüğünü ve korelasyonunu sağlar.[5] SOAR, tekrarlayan olay yanıtı görevlerini otomatikleştirerek insan hatasını azaltır ve modern siber saldırıların hızı göz önüne alındığında kritik olan gerçek zamanlıya yakın azaltmayı sağlar.[5]

2025'teki Etki: Bu yaklaşım, güvenlik operasyonlarını reaktiften proaktife ve son derece verimli hale dönüştürür. Kuruluşların karmaşık saldırı kalıplarını tanımlamasına, tehditlere saniyeler içinde yanıt vermesine ve insan analistlerini stratejik görevler için serbest bırakmasına olanak tanıyarak genel dijital dayanıklılığı önemli ölçüde artırır.[5]

Güvenilir Kaynak: AI Multiple [16]; ResearchGate [12]; ControlAudits.com [25]; Cyber.gov.au [27]; Splunk.com.[5]

4.4. Siber Güvenlik Becerisi Açığının Giderilmesi

Öneri: Mevcut güvenlik personelinin gelişmiş IDS/IPS teknolojileri, AI/ML ve entegre güvenlik platformları (SIEM/SOAR) konusunda eğitilmesi ve becerilerinin geliştirilmesi için aktif olarak yatırım yapılmalıdır. Önemli kaynak kısıtlamalarıyla karşı karşıya olan kuruluşlar için, saygın Yönetilen Güvenlik Hizmeti Sağlayıcıları (MSSP) ile ortaklık yapılması düşünülmelidir.

Gerekçe: Küresel siber güvenlik beceri açığı, milyonlarca pozisyonun doldurulamamasıyla birlikte büyük bir zorluktur.[1] Nitelikli profesyoneller, doğru uygulama, sürekli ayarlama ve etkili olay yanıtı için kritik öneme sahiptir.[1] AI/ML ve SOAR aracılığıyla otomasyon, insan analistleri üzerindeki yükü azaltarak bu açığı telafi etmeye yardımcı olabilir.[5] MSSP'ler, şirket içi işe alım ihtiyacı olmadan özel uzmanlığa

erişim sağlayabilir.[6]

2025'teki Etki: Beceri açığının kapatılması, gelişmiş IDS/IPS ve entegre güvenlik çözümlerinin etkili bir şekilde dağıtılmasını, yönetilmesini ve kullanılmasını sağlar. Bu, güvenlik yatırımlarından elde edilen getiriyi en üst düzeye çıkarır ve kuruluşun karmaşık tehditlere yanıt verme yeteneğini güçlendirerek teknolojinin kullanılmayan bir gider haline gelmesini önler.[27]

Güvenilir Kaynak: DataInsightsMarket.com [1]; ArchiveMarketResearch.com [2]; GlobalGrowthInsights.com [6]; Cyble.com [7]; Cyber.gov.au [27]; Splunk.com.[5]

4.5. Proaktif Tehdit Avcılığı ve Olay Yanıtını Teşvik Etme

Öneri: Güvenlik duruşu, tamamen reaktif olmaktan proaktif tehdit avcılığını vurgulayan bir yaklaşıma kaydırılmalıdır. IDS/IPS uyarılarını, CTI'yi ve otomatik SOAR oyun kitaplarını içeren kapsamlı olay yanıt planları geliştirilmeli ve düzenli olarak test edilmelidir.

Gerekçe: Geleneksel IDS öncelikli olarak reaktiftir, tehditleri ağa girdikten sonra tespit eder.[9] APT'ler ve sıfır günler gibi modern tehditler, önemli hasara neden olmadan önce güvenlik açıklarını ve kötü niyetli aktiviteleri tanımlamak için proaktif önlemler gerektirir.[2] Tehdit avcılığı, IDS/IPS'in hemen işaretlemeyebileceği gizli tehditleri aktif olarak arar.[7] IDS/IPS verileri ve CTI tarafından bilgilendirilen sağlam olay yanıt planları, kaçınılmaz ihlallerin etkisini en aza indirmek için kritik öneme sahiptir.[28]

2025'teki Etki: Proaktif tehdit avcılığı, iyi prova edilmiş olay yanıtıyla birleştiğinde, kuruluşların saldırı yaşam döngüsünün daha erken aşamalarında tehditleri tespit etmesini ve etkisiz hale getirmesini sağlayarak, kalma süresini ve potansiyel hasarı azaltır. Bu stratejik değişim, genel güvenlik olgunluğunu ve iş sürekliliğini artırır.

Güvenilir Kaynak: Otorio.com [9]; ArchiveMarketResearch.com [2]; Cyble.com [7]; ControlAudits.com [25]; Berkeley.edu [35]; SecurityMetrics.com [28]; FluidAttacks.com.[31]

---

5. Sonuç

2025 yılında ve sonrasında ağ güvenliği dedektörleri (IDS/IPS), sağlam bir ağ güvenliği stratejisinin vazgeçilmez bileşenleri olarak kritik ve evrimleşen bir rol oynamaktadır. Analizler, tek başına IDS/IPS çözümlerinin, günümüzün sofistike ve dinamik tehdit ortamına karşı giderek yetersiz kaldığını göstermektedir.

Ağ güvenliğinin geleceği, özellikle IDS/IPS bağlamında, entegre, uyarlanabilir ve

istihbarat odaklı bir yaklaşımda yatmaktadır. Bu yaklaşım şunları içermektedir:

- Üstün tehdit tespiti ve azaltılmış yanlış pozitifler için gelişmiş yapay zeka ve makine öğreniminden yararlanmak.
- Ölçeklenebilirlik ve esneklik için bulut tabanlı çözümleri benimsemek.
- Sürekli doğrulama ve en az ayrıcalık için Sıfır Güven mimarileriyle sorunsuz entegrasyon sağlamak.
- Proaktif savunmaları bilgilendirmek için Siber Tehdit İstihbaratını kullanmak.
- Nesnelerin İnterneti (IoT) cihazlarının yaygınlaşmasının ortaya çıkardığı benzersiz güvenlik zorluklarını ele almak.
- Birleşik görünürlük ve otomatik yanıt için SIEM ve SOAR'ın gücünden faydalanmak.

Bu teknolojik gelişmelerin, yetenekli insan uzmanlığı ve proaktif güvenlik uygulamalarıyla stratejik olarak birleştirilmesiyle, kuruluşlar yalnızca saldırıları tespit etmek ve önlemekle kalmayıp, aynı zamanda ortaya çıkan tehditlere uyum sağlayan, dijital çağda kritik varlıkların gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlayan dayanıklı bir ağ güvenliği duruşu inşa edebilirler.

Alıntılanan çalışmalar

1. Intrusion Detection System & Intrusion Prevention System (IDS & IPS) Market Expansion: Growth Outlook 2025-2033, erişim tarihi Haziran 10, 2025, https://www.datainsightsmarket.com/reports/intrusion-detection-system-intrusion-prevention-system-ids-ips-1952826
2. Intrusion Detection and Prevention Systems (IPS) Software 2025-2033 Trends: Unveiling Growth Opportunities and Competitor Dynamics, erişim tarihi Haziran 10, 2025, https://www.archivemarketresearch.com/reports/intrusion-detection-and-prevention-systems-ips-software-558785
3. 5 Cybersecurity Trends to Watch in 2025, erişim tarihi Haziran 10, 2025, https://sps.wfu.edu/articles/top-cybersecurity-trends/
4. Top Cybersecurity Trends in 2025: 9 Trends to Watch | Splunk, erişim tarihi Haziran 10, 2025, https://www.splunk.com/en_us/blog/learn/cybersecurity-trends.html
5. SIEM: Security Information & Event Management Explained | Splunk, erişim tarihi Haziran 10, 2025, https://www.splunk.com/en_us/blog/learn/siem-security-information-event-management.html
6. Intrusion Detection System/Intrusion Prevention System (IDS/IPS ..., erişim tarihi Haziran 10, 2025, https://www.globalgrowthinsights.com/market-reports/intrusion-detection-system-intrusion-prevention-system-ids-ips-market-107682
7. Everything You Need To Know About Cyber Threat Intelligence, erişim tarihi Haziran 10, 2025, https://cyble.com/knowledge-hub/cyber-threat-intelligence-2025/

8. IPS Nedir? IPS vs. IDS Farkları - Bulutistan Blog, erişim tarihi Haziran 10, 2025, https://bulutistan.com/blog/ips-nedir/
9. Intrusion Detection Systems (IDS): Pros and Cons | OTORIO, erişim tarihi Haziran 10, 2025, https://www.otorio.com/blog/intrusion-detection-systems-ids/
10. IPS. vs. IDS vs. Firewall: What Are the Differences? - Palo Alto Networks, erişim tarihi Haziran 10, 2025, https://www.paloaltonetworks.com/cyberpedia/firewall-vs-ids-vs-ips
11. IDS vs. IPS: Definitions, Comparisons & Why You Need Both | Okta, erişim tarihi Haziran 10, 2025, https://www.okta.com/identity-101/ids-vs-ips/
12. (PDF) Comparison of Traditional vs. AI-Based Intrusion Detection ..., erişim tarihi Haziran 10, 2025, https://www.researchgate.net/publication/389717300_Comparison_of_Traditional_vs_AI-Based_Intrusion_Detection_and_Prevention_Systems_Efficiency_and_Accuracy
13. How intrusion detection systems help identify cyber threats in real-time - DataGuard, erişim tarihi Haziran 10, 2025, https://www.dataguard.com/blog/how-intrusion-detection-systems-help-identify-cyber-threats/
14. IPS (Saldırı Önleme Sistemi) Nedir? IPS vs. IDS Arasındaki Farklar - Uzman Posta, erişim tarihi Haziran 10, 2025, https://uzmanposta.com/blog/ips/
15. Intrusion Detection and Prevention Systems - National Institute of Standards and Technology, erişim tarihi Haziran 10, 2025, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=901146
16. AI IPS: 6 Real-life Use Cases & Leading Tools in 2025, erişim tarihi Haziran 10, 2025, https://research.aimultiple.com/ai-ips/
17. Top 10 Intrusion Detection and Prevention Systems (IDPS) for Real-Time Threat Monitoring in 2025 - CloudNuro.ai, erişim tarihi Haziran 10, 2025, https://www.cloudnuro.ai/blog/top-10-intrusion-detection-and-prevention-systems-idps-for-real-time-threat-monitoring-in-2025
18. Intrusion Detection - OWASP Foundation, erişim tarihi Haziran 10, 2025, https://owasp.org/www-community/controls/Intrusion_Detection
19. Intrusion prevention systems - ACM Ubiquity, erişim tarihi Haziran 10, 2025, https://ubiquity.acm.org/article.cfm?id=1071927
20. Network Security in 2025: Threats, Security Models and ... - Faddom, erişim tarihi Haziran 10, 2025, https://faddom.com/network-security-in-2025-threats-security-models-and-technologies/
21. IPS ve IDS Nedir ve Nasıl Çalışır? (IPS vs IDS) - ÇözümPark, erişim tarihi Haziran 10, 2025, https://www.cozumpark.com/ips-ve-idsin-ortak-yonleri-birbirleriyle-iliskileri-ips-ve-ids-nedir/
22. Intrusion Detection and Prevention Systems and Techniques - American Military University, erişim tarihi Haziran 10, 2025, https://www.amu.apus.edu/area-of-study/information-technology/resources/intrusion-detection-and-prevention-systems-and-techniques/

23. Signature Based vs Anomaly Based IDS | Fidelis Security, erişim tarihi Haziran 10, 2025, https://fidelissecurity.com/cybersecurity-101/learn/signature-based-vs-anomaly-based-ids/
24. Utilizing IDS and IPS to Improve Cybersecurity Monitoring Process, erişim tarihi Haziran 10, 2025, https://jcsra.thestap.com/archives/volume-2025-3/682abc34937e9af5efb39cb9
25. What Is the Future of Intrusion Detection and Prevention Systems? - Controlaudits.com, erişim tarihi Haziran 10, 2025, https://controlaudits.com/blog/what-is-the-future-of-intrusion-detection-and-prevention-systems/
26. IPS ve IDS Nedir? Nasıl Çalışır? - TurkNet Blog, erişim tarihi Haziran 10, 2025, https://www.turk.net/blog/ips-ve-ids-nedir-nasil-calisir/
27. Implementing SIEM and SOAR platforms: Practitioner guidance ..., erişim tarihi Haziran 10, 2025, https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-monitoring/implementing-siem-and-soar-platforms/implementing-siem-and-soar-platforms-practitioner-guidance
28. Auditor Tips: Set Up Your Intrusion Detection/Prevention System - Security Metrics, erişim tarihi Haziran 10, 2025, https://www.securitymetrics.com/blog/set-your-intrusion-detectionprevention-system
29. Top 5 Cloud Security Trends to Watch in 2025 - SentinelOne, erişim tarihi Haziran 10, 2025, https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-security-trends/
30. Intrusion detection software best practices - Infosec, erişim tarihi Haziran 10, 2025, https://www.infosecinstitute.com/resources/network-security-101/intrusion-detection-software-best-practices/
31. What is the zero trust security model? - Fluid Attacks, erişim tarihi Haziran 10, 2025, https://fluidattacks.com/cybersecurity-essentials/what-is-zero-trust-security-model
32. Best Insider Threat Management Software: Top 9 Solutions in 2025, erişim tarihi Haziran 10, 2025, https://www.exabeam.com/explainers/cyber-threat-intelligence/best-threat-intelligence-platforms-top-10-solutions-in-2025/
33. IoT Security Challenges (Most Critical Risk of 2025) - StationX, erişim tarihi Haziran 10, 2025, https://www.stationx.net/iot-security-challenges/
34. Critical Internet of Things Security Challenges Businesses Must ..., erişim tarihi Haziran 10, 2025, https://xobee.com/2025/04/critical-internet-of-things-security-challenges-businesses-must-address-in-2025/

35. Intrusion Detection Guideline - Information Security Office, erişim tarihi Haziran 10, 2025, https://security.berkeley.edu/intrusion-detection-guideline