Journal of Computer Science
https://dergipark.org.tr/en/pub/bbd

ISSN,e-ISSN: 2548-1304
Volume:IDAP-2022, pp:211-218, 2022
https://doi.org/ 10.53070/bbd.1172803
Research Paper

IPS Sistemlerde Yapay Zekânın Son Beş Yıldaki Gelişimi

The Development ff Artıfıcıal Intellıgence in IPS Systems in The Last Five Years

Muharrem Tuncay GENÇOĞLU[*1], Esra BAHADIR[2]
[1]Teknik Bilimler MYO, Fırat Üniversitesi, Elazığ, Türkiye
[2]Siber Güvenlik Bölümü, Ahmet Yesevi Üniversitesi TÜRTEP, Ankara, Türkiye
(mtgencoglu@gmail.com)

Received:Sep.08,2022 Accepted:Sep.16,2022 Published:Oct.10,2022

Özetçe— Günümüzde siber güvenliğin temel taşlarından olan IPS (Saldırı Önleme Sistemleri) 2017 yılından günümüze kadar geleneksel insan kontrollü savunma stratejisinden sıyrılıp, NGIPS (Yeni Nesil Saldırı Önleme Sistemleri) olarak da bilinen yapay zekâ ve makine öğrenimi entegrasyonlu yeni bir savunma stratejisine dönüşmüştür. Yapay zekaya entegre bu yeni IPS çözümleri yıllar içerisinde farklı algoritmalar ve teknikler ile saldırı önlemede kullanılmıştır. Bu çalışmada yapay zekaya entegre sistemler hakkında bilgi verilmiş ve son beş yıl içerisindeki gelişimi IPS çözümleri genelinde ve Fortinet IPS çözümü özelinde incelenmiştir. IPS çözümlerindeki bu yapay zekâ ile savunma, yine yapay zekâ ile yapılan saldırılar neticesinde doğru orantılı olarak gelişmiştir. IPS çözümlerinde makine öğrenimi üç temel teknikte kullanır. Bunlar, veri toplama, özellik seçimi ve model oluşturmadır. Model oluşturma yöntemi ile sınıflandırılan veriler yapay zekâ algoritmaları ile olumlu ya da olumsuz olarak değerlendirilip müdahale edilir. Geleneksel yöntemler yani yapay zekâ öncesi yöntemler bu algılamalarda yetersiz kalmıştır. Gelişen siber saldırılar ve her geçen gün keşfedilen yeni açıklıkların insan sınırlarının üzerinde olması sebebi ile IPS sistemlerde yapay zekânın var olması ve geliştirilmesi zorunlu hale gelmiştir.
Bu çalışmanın IPS'lerde yapay zekâ gelişiminin, siber savunmadaki önemi ile ilgili farkındalık yaratacağı değerlendirilmektedir.
Anahtar Kelimeler: IPS, yapay zeka, makine öğrenmesi, siber güvenlik.

Abstract— Today, IPS (Intrusion Prevention Systems), which is one of the cornerstones of cyber security, has been getting rid of the traditional human-controlled defense strategy since 2017 and has been implementing a new defense strategy with artificial intelligence and machine learning integration, also known as NGIPS (Next Generation Intrusion Prevention Systems). These new IPS solutions integrated with artificial intelligence have been used in attack prevention with different algorithms and techniques over the years. In this study, information about these systems integrated into artificial intelligence is given and its development in the last five years is examined in general IPS solutions and fortinet IPS Fortinet. Defense with this artificial intelligence in IPS solutions has developed in direct proportion as a result of attacks made with artificial intelligence. Machine learning in IPS solutions uses three basic techniques. These are data collection, feature selection, and model building. Finally, artificial intelligence algorithms evaluate the data classified by the modeling method and intervene positively or negatively. Traditional methods, that is, pre-artificial intelligence methods were insufficient in these perceptions. The existence and development of artificial intelligence in IPS systems have become mandatory due to the developing cyber attacks and the fact that new vulnerabilities discovered day by day are beyond human limits.
It is evaluated that this study will create awareness about the importance of artificial intelligence development in IPS in cyber defense.
Keywords: IPS, machine learning, cyber security, artificial intelligence.

1. Giriş

Geleneksel güvenlik duvarını kullandığımızda, saldırganlar verileri taklit ederek güvenlik duvarını aşabilir veya güvenlik duvarında arka kapı bulabilir. Bu sebeple güvenlik duvarı, ağ içindeki saldırıyı engelleyemez. Güvenlik duvarı, yetenek sınırları nedeniyle saldırıyı gerçek zamanlı olarak kontrol etme yeteneğine sahip değildir. Saldırı Önleme Sistemleri, ağ ve/veya sistem etkinliğini izleyen, herhangi bir kötü amaçlı etkinlik olup olmadığını belirleyen ve buna anında yanıt veren bir sistem veya yazılım uygulaması olarak tanımlanır. Bilginin güç olduğunun bilinmesi prensibine dayanarak, bilgisayar korsanları yararlı bilgiler elde etmek için çeşitli saldırı biçimleri kullanır. Saldırıların çoğu, izinsiz giriş tespit teknikleri kullanılarak tespit edilebilir ve bunların önlenmesi, izinsiz girişler için bir engelleme etkisi yaratır. Son birkaç yılda sonsuz iletişim paradigmasının gelişmesi, yaygınlaşması ve ağa bağlı dijital cihazların sayısındaki büyük artış nedeniyle, bilgi ve iletişim teknolojisini sürdürmeye çalışan sistemlerde siber güvenlik konusunda önemli eksiklikler ortaya çıkmıştır. Saldırganların günlük olarak yeni saldırılar tespit edip ve oluşturmaları nedeniyle saldırıların Saldırı Tespit

Sistemleri (IDS) tarafından doğru bir şekilde tespit edilmesi ve uygun yanıtların verilmesi gerekir bu da IPS'lerin birincil amacıdır ve savunmada çok önemli bir rol oynamaktadır.

Sonuç olarak, IDS ve IPS sistemlerinde YZ kullanımı zorunlu hale gelmiştir. Daha önce geliştiriciler, saldırı düzeni hakkında önceden bilgi sahibi olmadan anormal trafiği normal trafikten ayırt etmek için farklı makine öğrenimi algoritmaları kullanılıyordu. Makine öğrenimi üzerine yapılan kapsamlı araştırmalarda, son zamanlarda insan beynini taklit etmekte büyük bir atılım yaptığı ortaya çıkmıştır. Ayrıca yapay zekâ sistemlerine karşı özel olarak tasarlanmış saldırıların etkili olduğu da kanıtlanmıştır. Bu da yapay zekâ saldırılarını yine yapay zekâ savunması ile bertaraf etmeyi zorunlu kılmıştır.

Normalde, bir insanın kapasitesi, meydana gelen tüm izinsiz girişleri tespit etmek ve önlemek konusunda sınırlıdır ancak bir makine bunu yapabilir. Dolayısıyla YZ bu teknik sorunu çözmede çok önemli bir faktördür.

Sistemlere yönelik gerçekleştirilen siber saldırıların çoğu kritik önem arz eden kurum ve kuruluşlara yansımaktadır. Bu saldırılar sonucunda gerek maddi, gerekse itibar kayıpları oluşmaktadır. Bu çalışmada IPS'in insan güdümlü performansındaki eksiklikleri, genel güvenlik açıklıkları ve IPS sistemlere yapay zekanın entegre edilmesi ile kat ettiği ilerleme incelenecektir. Ayrıca IPS' in yapay zekâ ile son beş yıl içerisinde gerçekleşen siber saldırılara süreç boyunca nasıl bir gelişim ve değişim ile cevap verdiği ele alınacaktır. Literatür incelemesi sonucunda elde edilen bilgi ve belgeler çerçevesinde "yapay zekâ / makine öğrenmesinin IPS'de ve siber güvenlikte ne kadar başarılı olduğu?" sorusunun cevabı aranacaktır.

Bu araştırmada IPS sistemlerin yapay zekâ öncesi ve yapay zekâ ile son beş yıl içerisindeki gelişimi incelenecek ve ikisi arasında kıyaslama yapılacaktır. IPS'de yapay zekânın kendi kendine öğrenme, insandan bağımsız olaylara müdahale etme ve yeni savunma teknikleri geliştirme özelliklerinin son beş yılda geldiği nokta ve önümüzdeki yıllarda bu entegrasyonun geleceği öngörülebilir noktalar değerlendirilecektir.

Siber güvenliğin bel kemiğini oluşturan IPS ve IDS'lerin önemi her geçen gün daha fazla artmaktadır. Bu sistemler, siber saldırılara karşı hayati bir tespit, savunma ve geri püskürtme sunmaktadırlar. Ancak saldırganların da sürekli yeni ataklar geliştirmeleri ve bunları yapay zekâ destekli yapmaları, IPS sistemlerde yapay zekâyı zorunlu hale getirmiştir. Özellikle EKS'lere yönelik gerçekleştirilen siber saldırıların insanlara ve çevreye verdiği zararlar düşünüldüğünde, IPS sistemlerde makine öğrenmesini insanlığın geleceği açısından daha önemli hale getirmiştir. Bu çalışmanın IPS'de yapay zekânın, siber güvenlik kapsamında geldiği ve gelebileceği yerler ile siber güvenliğin gelişiminde yapay zekânın rolü hakkında farkındalık yaratacağı değerlendirilmektedir.

Bu bağlamda çalışmanın bundan sonraki kısmında ikinci bölümde IPS sistemlerde yapay zekâ konusuna değinilecek, üçüncü bölümde 2018-2022 raporlarının analizi yapılacak ve son olarak dördüncü bölümde çalışmanın sonuçları değerlendirilerek önerilerde bulunulacaktır.

2. IPS Sistemlerde Yapay Zekâ

Günümüzde IDS ve IPS'de kullanılan tekniklerin çoğu, bilgisayar ağlarına yapılan siber saldırıların dinamik ve karmaşık doğasıyla başa çıkamamaktadır. Güvenlik duvarları, erişim kontrol mekanizmaları ve şifrelemeler gibi geleneksel izinsiz giriş tespit ve önleme teknikleri, ağları ve sistemleri DDOS gibi giderek daha karmaşık hale gelen saldırılardan tam olarak koruma konusunda çeşitli sınırlamalara sahiptir.

Tablo 1. Belirli tehditlerde kullanılan makine öğrenme tekniklerinden bazıları

Ağ tehditlerine göre sınıflandırma	**Mevcut çözümler**	**Makine öğrenim teknikleri**
1. ICMP Fırtınaları	Dos saldırılarıyla aynı	K-araç kümelemesinin kullanımı
2. Ping	ICMP'yi devre dışı bırakın ve IP adresini değiştirin	Karar ağacı algoritması ile çözme
3. IP parçalanması	Telefon hattını temizleme ve Ethernet kablosunun kontrolü	Bulanık mantık, sorunun ciddiyetine bağlı olarak kullanılabilir

Tablo 1'de de görüldüğü gibi bilgisayarları ve ağları etkileyebilecek sürekli değişen tehdit ortamını ele almak için çeşitli makine öğrenimi tekniklerini verimli bir şekilde kullanmak; daha yüksek algılama oranları, daha düşük yanlış pozitifler ve zorlu saldırılara daha iyi uyum sağlama ile sonuçlanabilir. (Das, Nene, 2017).

IPS sistemler yapay zekâyı kullanırken 3 temel adım izlerler: Veri toplama, özellik seçimi ve model oluşturma.

2.1. Veri Toplama

Makine öğrenmesi aslında bir veri bilimidir ve veri toplama olmadan ilk adım gerçekleştirilemez. Makine öğrenimi, veriler üzerinde sınıflandırma görevlerini yerine getirmektedir. Yapay zekânın, belirli özelliklere göre (bir şeyin kötü amaçlı olup olmadığı gibi) tanımlama yapması, eldeki verileri farklı sınıflara ayırması ve doğru bir sınıflandırma yapması için öncelikle sınıflandırmaya çalıştığı öğeler hakkında mümkün olduğunca çok veri toplaması ve analiz etmesi gerekir. Veriler toplandıktan sonra, aykırı değerleri tespit etmek ve veri içindeki gizli grupları daha iyi anlamak için aykırılık tespiti ve kümeleme gibi teknikler kullanılabilir böylece sınıflandırma için yalnızca en uygun verilerin kullanılması sağlanır.

2.2. Özellik Seçimi

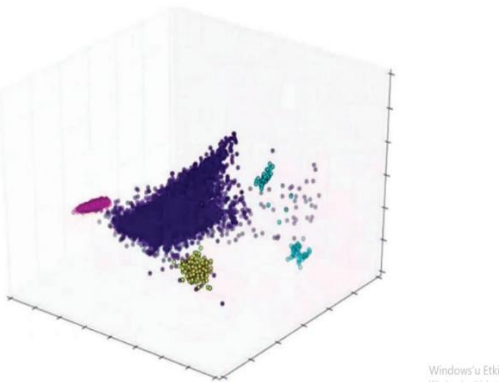
Veriler toplanıp temizlendikten sonraki adım, iyi huylu ve kötü niyetli verileri ayırt etmek için kullanılan istatistiksel modelin temelini oluşturacak özellikleri izole etmek ve ölçmektir. Makine öğrenimi algoritmaları, bir web sayfasını kötü veya iyi niyetli olarak ölçerken ve kategorilere ayırırken kelimeleri (yani alfabetik dizeleri), dilsel olmayan verileri (ZX gibi Hint-Avrupa dillerinde görünmeyen karakter çiftlerini) sayar. Ayrıca yapay zekâ algoritmaları web sayfasında farklı karakter sınıflarının görünme sıklığını da ölçer: rakamlar, onaltılık karakterler, noktalama işaretleri, büyük ve küçük harfler, boşluk ve yazdırılamayan karakterler. Ek olarak, çeşitli karakter sınıfları arasındaki geçişler de değerlendirilir. Örnek olarak, büyük harfin ardından küçük harfin ne sıklıkta geldiği veya arka arkaya iki boşluğun ne zaman ve nerelerde kullanıldığının ayrıştırılması, durumları söylenilebilir.

Şekil 1. Makine öğrenimi IPS'de nasıl uygulanır? (Micro,. 2017).

2.3. Model Oluşturma

Seçilen özelliklerle, süreçteki bir sonraki adım, iyi niyetli ve kötü niyetli verileri sınıflandırmak için genelleştirilebilir bir model oluşturmayı içerir.

İlk olarak, seçilen özelliklere pozitif veya negatif değer verilir. Küçük harften büyük harfe geçişler, büyük harften boşluğa geçişler, rakamların ve dilsel olmayan verilerin kullanımı gibi özellikler pozitif olarak değerlendirilir. Bu durum, verilerin kötü amaçlı bir içeriği belirtme olasılıkları daha yüksek demektir. En popüler sitelerde ortak olan özelliklere negatif bir ağırlık atanır. Her özelliğin sayıları, ilgili ağırlık katsayıları ile çarpılır ve daha sonra bir araya getirilerek nihai bir puan üretilir. Skor pozitifse, içerik kötü amaçlı olarak sınıflandırılacaktır.



Şekil 2. Kötü ve iyi niyetli site ayrıştırmalarının 3D ile modellenmesi (Micro, 2017)

Şekil 2'de de görüldüğü gibi sistem, toplanan bu verileri n boyutlu uzaydan üç boyutlu alana almak için özelliklerdeki gereksiz bilgileri kaldırarak anlaşılması kolay bir 3D görselleştirme oluşturan ve temel bileşen analizi olarak bilinen bir süreç kullanır.

3. Yapay Zekâ İle Entegre IPS Çözümlerinin Siber Tehditlere Karşı Etkilerinin 2018-2022 Raporlarına Göre Değerlendirilmesi

Tablo 2. EPRI siber güvenlik yol haritası raporu (EPRI, 2020).

Major Past Accomplishments	2019	2020	Future
POWER DELIVERY CYBER SECURITY ANNUAL RESEARCH PORTFOLIO (P183)			
• ISOC Guidebook • Guidelines for planning an ISOC • Guidelines for integrating control center systems into an ISOC • Guidelines for integrating the substation and field domain into an ISOC • IDS/IPS guidelines for power deliver systems • ITAF framework and utility testing	• ISOC Guidebook update • Utilizing artificial intelligence and machine-learning for incident management • Data analytics guidelines for incident management • Review and update the National Electric Sector Cyber security Organization Resource (NESCOR) failure scenarios	• ISOC Guidebook update • Utilizing artificial intelligence and machine-learning for incident management • Data analytics for incident management; utilizing use cases and determining trends for machine-learning	Artificial intelligence for predictive analysis

EPRI (Electiric Power Research Enstitute) 2020 Raporuna göre; dünyada 2019 yılından itibaren tüm siber güvenlik alanlarında yapay zekâ ve makine öğrenimi kullanımı başlamış ve 2020 sonrasında yüksek oranda yapay zekâya bağlı bir siber güvenlik ortamı öngörülmüştür.

3.1. CyberEdge Group Research Lab'ın son 3 yıla ait siber tehdit savunma raporu

2020 Raporu	2021 Raporu	2022 Raporu
Rekor düzeylerde başarılı siber saldırılar gerçekleşti: beş kuruluştan dördü en az bir başarılı siber saldırı yaşadı ve üçte birinden fazlası altı veya daha fazla saldırıya uğradı.	Kuruluşların %86'sı geçen yıl başarılı bir siber saldırıya uğradı.	Kuruluşların %85'i geçen yıl başarılı bir siber saldırıdan zarar gördü. Fidye yazılımı kurbanlarının rekor düzeyde %63'ü geçen yıl fidye ödeyerek siber suçluları saldırılarını artırmaya teşvik etti.
API ağ geçitleri, veritabanı güvenlik duvarları ve WAF'ler, yüklü uygulama/veri güvenliği ürünleri listesinin başında gelmektedir.	COVID-19 salgını, kuruluşların yarısında yeni BT güvenlik yatırımlarının büyük ölçüde yeniden öncelik verilmesine neden oldu.	Kuruluşların %64'ü API güvenliğini benimsedi.
	Kuruluşların %69'u geçen yıl fidye yazılımı tarafından ele geçirildi.	Kuruluşların %84'ü kalifiye BT güvenlik personeli eksikliği yaşıyor;
	Fidye yazılımı kurbanlarının %57'si geçen yıl fidye ödeyerek	

Kuruluşların %85'i makine öğrenimi ve yapay zeka içeren IPS, IDS ve Firewall tercih ettiklerini belirtti.

Güvenlik uygulamalarının ve hizmetlerinin üçte birinden fazlası (%35,7) artık bulut aracılığıyla sağlanıyor.

siber suçluları saldırılarını artırmaya teşvik etti.

Kötü amaçlı yazılım, fidye yazılımı ve hedef odaklı kimlik avı en çok korkulan tehditlerdendir.

Düşük çalışan farkındalığı ve kalifiye personel eksikliği, BT güvenliğinin başarısını engelliyor.

Beş kuruluştan dördü, makine öğrenimi (MÖ) ve yapay zekâ (YZ) teknolojisine sahip IPS, IDS ve Firewall tercih ediyor.

Buluttan sağlanan BT güvenlik uygulamaları ve hizmetlerinin yüzdesi, kısmen pandeminin neden olduğu büyük bir artışla %36'dan %41'e yükseldi.

BT güvenlik yöneticileri, analistler ve mimarlar en az tedarikte.

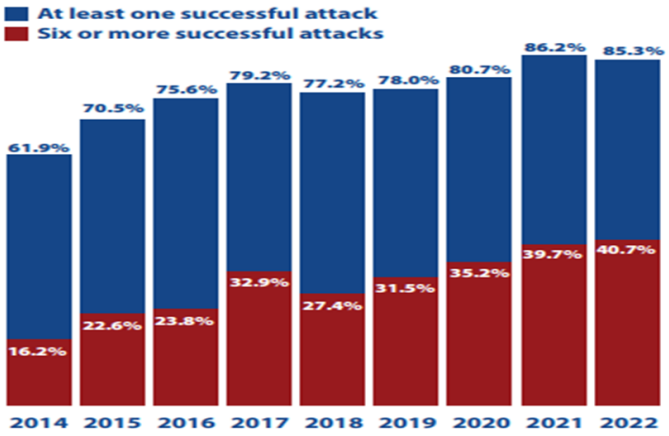
Tipik kurumsal BT güvenlik bütçesi bu yıl yaklaşık %5 arttı.

Güvenlik uygulamalarının ve hizmetlerinin %41'i bulut aracılığıyla sağlanmaya başlandı.

Dört kuruluştan üçü SD-WAN, sıfır güven ağ erişimi (ZTNA) ve güvenli erişim hizmeti kenarı (SASE) uyguladı veya yakında uygulayacak.

Kuruluşların %90'ı makine öğrenimi ve yapay zekâ içeren IPS, IDS ve Firewall tercih ettiklerini belirtti.

CyberEdge Group Research Lab'ın Son 3 Yıla Ait Siber Tehdit Savunma Raporu'na göre: 2022 yılında kuruluşların %90'ının makine öğrenimi ve yapay zekâ içeren IPS, IDS ve Firewall tercih etmelerine rağmen; aynı kuruluşların %85'i geçen yıl başarılı bir siber saldırıdan zarar görmüştür. Bu zararın ve saldırıların sebebi; özellikle 2020, 2021 ve 2022 yıllarında Covid19 salgını sebebi ile kişi ve kurumların çoğunun iş ve işlemlerini bilgisayarlar üzerinden online olarak yapmasıdır ancak kurum personelleri ve şahısların siber okur yazarlık ve bilgi güvenliği hakkında yeterli olmaması özellikle phishing (oltalama) ve diğer sosyal mühendislik bazlı saldırılarda siber saldırganlara cazip bir ortam hazırlamış oldu. Şekil 3 'de de görüldüğü gibi son beş yıldaki tüm siber saldırılar, şiddetini son üç yıl içerisinde ciddi oranda arttırmıştır. Yapay zekâ her ne kadar IPS'in etkinliğini arttırsa da, saldırganlar da Zero Day, Ddos ve bir çok siber saldırıda yapay zekâ kullanmaya başlamışlardır.



Şekil 3. Cyberedge 2022 Raporu (Cyberedge, 2022).

Şekil 3' de de görüldüğü üzere; Cyberedge 2022 Raporunda, veri güvenliğini tehlikeye atan en az bir ve altı ya da daha fazla başarılı atağın yıllara göre yüzdelik grafiği verilmiştir.

Bu rapor, siber ataklar yapay zekâ ile kuvvetlendikçe, siber savunmanın da yapay zekâ ile kuvvetlenmesinin zorunlu hale geldiğini göstermektedir. Dark trace CEO'su Nicole Eagen, siber güvenliğin geleceğinin yapay zekâya karşı yapay zekâ olduğunu söylemiştir.

Campemini Araştırma Enstitüsü 2020 Siber Güvenlik Raporuna Göre;

- Yapılan araştırmalarda, işletmelerin %61'i, günümüzde yapay zekâ teknolojilerini kullanmadan ihlal girişimlerini tespit edememekte ve önleyememektedirler.
- Cisco'nun yapay zekâlı IPS çözümü 2018'de müşterileri adına yedi trilyon tehdidi engellemiştir.

- Uç nokta cihazlarının çoğalması ve 2021 yılına kadar 25 milyarın üzerine çıkması beklenen yapay zekâ tabanlı IPS çözümlerine yatırım yapmak için uç nokta güvenliği 3. en yüksek önceliktedir.
- 2017 yılından 2020 yılına kadar YZ ile tehditleri ve ihlalleri tespit etmek için geçen toplam süre %12'ye kadar azalmıştır. Bekleme süresi ise (tehdit aktörlerinin tespit edilmeden kalma süresi) YZ kullanımıyla %11 azalmıştır. Bekleme süresinin tespiti, tehdit kalıplarını gösteren anormallikleri sürekli olarak tarayarak yapılır.
- Capgemini, bilgisayar korsanlığı kuruluşlarının 'spur phishing' tweetleri (hedeflenen kullanıcıları kandırarak hassas bilgileri paylaşmaları için onlara gönderilen kişiselleştirilmiş tweetler) göndermek için algoritmaları başarıyla kullandığını tespit etti. YZ, tweetleri bir insandan altı kat daha hızlı ve iki kat daha başarılı bir şekilde gönderebilir ve bunu benzer şekilde tespit etmektedir. (Tolido, Frank, Delabarre, Cherian, 2020).

3.2. NGIPS (Yeni Nesil IPS) Çözümlerinden Fortinet IPS'in Analizi

2017'den günümüze Gartner ve NSS Labs'ın en çok önerilenlerinden olan Fortinet, IPS sistemlerde yapay zekânın son beş yıldaki gelişimi araştırma konumuzdaki zaman sınırlılığı ile örtüşmektedir. Fortinet, 2018 yılında makine öğrenmesi ve yapay zekâyı sistemlerine dâhil etti. Ayrıca yeni tehditleri belirlemek için 2017 yılından günümüze büyük hacimli tehdit verilerini hızlı ve doğru bir şekilde işleyebilen otomatik bir makine öğrenimi sistemini oluşturmaya başladı. Sürekli gelişmekte olan ve beş yılı aşkın bir süredir denetimli öğrenme teknikleri kullanılarak eğitilen FortinetGuard YZ, haftada milyonlarca tehdit örneğini analiz etmektedir. Örnekler, her örneğin benzersiz kötü niyetli ve temiz özelliklerini tanımlayan beş milyardan fazla işleme düğümü tarafından işlenir. FortinetGuard YZ, gelişmiş algoritmalar kullanarak proaktif olarak yeni bir örneğin bir tehdit oluşturup oluşturmadığını belirler ve tüm Fortinet Security Fabric genelinde savunma imzalarını güncelleyen tehdit istihbaratı üretir.

3.3. Son beş yılda Fortinet NGIPS' in yapay zekâ ile gelişimi

Makine öğrenimi özelliğinin anormallik algılama modeli, web sunucularınıza geçen HTTP ve/veya HTTPS oturumlarının URL'lerini, parametrelerini ve HTTP yöntemini gözlemler. Anormal trafiği tespit etmek için matematiksel modeller oluşturur. Bir isteğin meşru olup olmadığını veya olası bir kötü niyetli saldırı girişimi olup olmadığını öğrenmek için aşağıdaki görevleri gerçekleştirir:

- İzin verilen erişimin matematiksel bir modelini oluşturmak için URL parametreleri gibi girdileri yakalar ve toplar.
- Trafiğin HTTP yöntemini gözlemler.
- Anormallikleri önceden eğitilmiş tehdit modelleriyle eşleştirir.
- Saldırıları algılar.

Fortinet, kötü niyetli saldırıları tespit etmek için iki makine öğrenimi katmanı kullanır. İlk katman, Gizli Markov Modelini (HMM) kullanır ve uygulamaya erişimi izler. Her parametrenin ve HTTP yönteminin arkasında matematiksel bir model oluşturmak için veri toplar. Veri toplama işlemi tamamlandığında, bir anormallik olup olmadığını belirlemek için modele yönelik her talebi doğrular.

İlk makine öğrenimi katmanı, anormallik olarak bir isteği tetiklediğinde, Fortinet bunun gerçek bir saldırı mı yoksa göz ardı edilmesi gereken iyi huylu bir anormallik mi olduğunu doğrulamak için ikinci makine öğrenimi katmanını kullanır. Bunu yapmak için önceden oluşturulmuş eğitimli tehdit modelleri içerir. Her biri, SQL enjeksiyon, siteler arası komut dosyası oluşturma vb. gibi belirli bir saldırı kategorisini temsil eder. Her tehdit modeli, binlerce saldırı örneğinin analizine dayalı olarak önceden eğitilmiştir. Tehdit modelleri, Fortinet Güvenlik Hizmeti kullanılarak sürekli olarak güncellenir. Yeni saldırı türleri yayınlandığında, FortiGuard yapay zekâ ekibi yeni tehditleri analiz eder ve ilgili tehdit modelini yeniden eğitir. Yeni tehdit modeli daha sonra imzaların güncellenmesine benzer bir şekilde tüm müşteri kurulumlarına gönderilir.

Yapay zekâ tabanlı makine öğrenimi bot algılama modeli, mevcut imza ve eşik tabanlı kuralları tamamlar. Bazen algılanamayan karmaşık botları algılar. Bot algılama modeli, kullanıcı davranışlarını on üç boyutta gözlemler; örneğin, kullanıcı tarafından kaç kez HTTP isteği başlatıldığı, isteğin yasadışı HTTP sürümleri kullanıp kullanmadığı, JSON/XML kaynaklarını alıp almadığı vb.

Sistemlerde yapay zekâ kullanılmadan önce botları algılamaya yönelik geleneksel mekanizmalarda bot algılama modeli, anormal kullanıcı davranışlarını algılamak için uygun bir eşik üzerinde deneme yapmayı zorunlu kılardı. Örneğin, bir kullanıcı tarafından başlatılan HTTP isteklerinin kaç kez anormal olarak kabul edilmesi gerektiğinin bilinememesi bu tarz bir saldırıda kayıplara yol açar. Yapay zekâ kullanılmayan bir IPS ile farklı eşik değerleri üzerinde deneme yapmak ve normal trafik için saldırı günlüğü raporlanana kadar, saldırı günlüğünü sürekli olarak kontrol etmek gerekebilir. Yapay zekâ tabanlı bot algılama modelini kullanmak IPS'de büyük kazanç sağlamıştır. Fortinet, kullanıcılarının trafik profillerini kendi kendine öğrenen bot algılama modelini oluşturmak için SVM (Destek Vektör Makinesi) algoritmasını kullanır. Yeni bir istemciden gelen trafik aktığında,

normal istemcilerinkiyle karşılaştırılır. Eşleşmezlerse, bot algılama modeli yeni istemciyi bir anormallik olarak sınıflandırır. Normal istemcilerin trafik profilleri önemli ölçüde değiştiğinde (uygulamanın işlevleri değiştiğinde ya da kullanıcılar uygulamayı ziyaret ettiklerinde farklı davranırlarsa), FortiWeb değişikliklere uyum sağlamak için bot algılama modelini otomatik olarak yeniler. Trafik, yapay zekâ ile 13 boyuttan kapsamlı bir şekilde değerlendirilir. Algılama doğruluğu arttırılmaya ve yanlış pozitif oranı azaltılmaya çalışılır.

Tablo 3. NSS Labs Fortinet NGIPS grup testi (NSS,.2020)

Product	2011/12	2013	2014	2015	2016	2017	2018	2019
NGFW	Neutral	Recommended	Recommended		Recommended	Recommended	Recommended	Recommended
Data Center Security Gateway						Recommended	Recommended	Recommended
Data Center IPS			Neutral		Recommended		Recommended	
NGIPS				Recommended	Retested & Passed	Recommended	Recommended	Recommended
Breach Detection			Recommended	Recommended	Recommended	Recommended	Recommended	
Breach Prevention						Recommended		Recommended
Web Application Firewall			Recommended			Recommended		
Adv. Endpoint Protection						Recommended	Recommended	Recommended
DDoS					Neutral			
SD-WAN							Recommended	Recommended

2017 yılında yapay zekâ ve makine öğrenmesi ile buluşan Fortinet NGIPS'in NSS Labs grup testlerindeki derecelendirmelerinin 9 yıllık özetine bakıldığında, tutarlı bir iyileştirme ve büyüyen bir "Önerilen" derecelendirme listesi görülmektedir(Tablo 3). Bu durum Fortinet'in yapay zekâ başarısı olarak da adlandırılmaktadır.

4. Sonuç

Bu çalışmada son beş yıl içerisinde yapay zekânın IPS sistemlerdeki gelişimi ele alınmış, örnek IPS çözümü olarak Fortinet NGIPS incelenmiş ve hakkında bilgiler verilmiştir.

Araştırma sonucunda görülmüştür ki; geleneksel IPS yöntemlerinin gelişen saldırlar karşısında yetersiz kalması, saldırıların hem çok özel hem de genel olarak karmaşık hale gelmesi, insan algı ve kapasitesine ek bir kuvvet olarak makine öğrenmesini zorunlu kılmıştır.

IPS sistemlerin genelinde ve Fortinet özelinde incelenen raporlarda YZ'nın saldırı önlemede ciddi yol kat ettiği ancak siber suçluların da daha karmaşık yöntemler ve teknikleri aynı makine öğrenimi ve yapay zekâ yöntemleri ile kullandığı görülmüştür. Bunun nedeni, YZ araştırmalarının herkese açık olması ve YZ'nın saldırganlar tarafından akıllı ve sürekli öğrenen açıklar oluşturmak için de kullanılabilmesidir. Günümüzde YZ saldırıları ve buna karşı savunma olarak YZ destekli IPS'ler savunma/saldırı grafiklerinde eşit oranda etkinlik göstermektedirler.

Cyberedge Research Lab 2022 raporuna göre; kuruluşların %84'ü kalifiye BT güvenlik personeli eksikliği yaşıyor; BT güvenlik yöneticileri, analistler ve mimarlar en az tedarik edilen çalışanlardır. Devam eden uzman güvenlik personeli eksikliği göz önüne alındığında, YZ otomasyonu IPS'de özellikle önem arz etmektedir. Bu, kuruluşların ek kalifiye personel bulma konusunda endişelenmeden güvenlik yatırımlarını geliştirmelerine ve operasyonlarını iyileştirmelerine de olanak tanıyacaktır. Siber suçlular yapay zekâ ile daha karmaşık yöntemler ve teknikler kullandıkça, her yıl binlerce yeni güvenlik açığı keşfedilip ve rapor edilmektedir. İşletmeler her gün karşılaştıkları çok sayıda yeni güvenlik açığını yönetmekte zorlanıyorlar ve geleneksel sistemleri bu yüksek riskli tehditleri gerçek zamanlı olarak engelleyemiyorlar. Bu durum IPS sistemlerde yapay zekânın tercihini arz/talep olarak da desteklemektedir ve halen insan ihtiyacı devam etse de yapay zekânın kendi kendine öğrenmesi geliştikçe bu ihtiyaç en aza düşecektir ancak insanın sistemden tamamen çıkartılması söz konu değildir.

Sonuç olarak yapay zekânın IPS üzerinde son beş yıldaki gelişimi aynı uygulamayı kullanan saldırganların tetiklemesi ile oldukça hızlı gelişmiştir. Siber güvenlik arenası her yönden genişleyecektir. Daha fazla veri, daha fazla cihaz, daha fazla saldırı vektörü, daha fazla siber fiziksel tehdit ve bunlara karşı kendini sürekli yenileyen

savunma sistemleri olacaktır. 2022 yılının ilk çeyreğinde başarılı siber saldırılar ve başarılı siber savunmalar eşit miktardadır. Bu da bize IPS sistemlerde hala eksiklikler olduğunu göstermektedir. Savaşların artık sistemler, veriler, kritik alt yapılar üzerinden yapıldığı ve siber savaş kavramının diğer savaş türleri arasında bir kategori olarak yer aldığı düşünülürse; özellikle siber güvenlikteki en zayıf halka olan insan faktörü üzerinde durulup, bilgi güvenliği ile ilgili eğitimlerinin planlanması ve siber saldırılara karşı etkili yanıt vermek için IPS'lerde kendi kendine öğrenmeyi, karar vermeyi, açıklıkları kapatmayı ve oluşabilecek zafiyetleri önceden tespit edip, bunlara müdahale edecek makine öğrenmesi için algoritmalar geliştirecek yazılımcı ve siber güvenlikçilere yatırım yapılması önem arz etmektedir. Bunun yanında çoğu saldırı önleme ve tespit sistemi yabancı menşeilidir, bu sistemlerin başarıları göz ardı edilemese de yerli ve milli IPS, IDS ve FW sistemlerimizin olması ülkemiz için çok önemlidir.

Kaynaklar

Borman, K. (2019). Data center ıntrusion prevention system test report. texas: nss laps.

Buduma, N., & Locascio, N. (2017). Fundamentals of deep learning: designing next-genaration. o'reilly media.

Costa, C. F. (2021). Artificial ıntelligence & cybersecurity: european union panorama. societa ıtaliana per ı'l organizzazione ınternazionale. pedralva.

Cyberedge. (2022). Cyberthreat defence report. newyork: cyberedge research labs.

Das, S., & Nene, M. J. (2017). A survey on types of machine learning techniques in ıntrusion prevention systems. ıeee wispnet 2017. ıeee.

ENISA. (2018). Cybersecurity culture guidelines: behavioural aspects of cybersecurity. enısa. doi:doı: 10.2824/324042

EPRI. (2020). Cyber security road map. california: eprı.

Fortinet. (2022). Investor presentation. amsterdam: fortinet labs.

Marinos, L., & Lourenco, M. B. (2020). Main incidents in the eu and worldwide enısa threat landscape. enısa.

Micro, T. (2017). Machine learning and ngıps. amerika birleşik devletleri.

Patel, A., Qassim, Q., & Wills, C. (2010, Aralık 8). Ids and ıps research. ınformation and computer security.

Qu, S., Li, X., Szurley, J., Kolter, J. Z., & Metze, F. (2019). Adversarial music: real worldaudio adversary against wake-word detection system. 2019. vancouver: neurıps.

Scarfone, K., & Mell, P. (2007). Guide to ıntrusion detection and prevention system. gaithersburg: nıst.

Shokri, R., Stronati, M., Song, C., & Shmatikov, V. (2017). Membership ınference attacksagainst machine learning models. güvenlik ve gizlilik sempozyumu (s. 3-18). ıeee.

Tolido, R., Frank, A., Delabarre, L., & Cherian, S. (2020). Reinventing cybersecurity withartificial ıntelligence: the new frontier in digital security. amsterdam: capgemini researchınstitute.

Aslan, F. (2022, Nisan 14). iskulubu.

https://iskulubu.com/manset/yapay-zekanin-en-onemli-5-avantaji-ve-dezavantaji/

Cimpanu, C. (2020, Ekim 17).

https://www.zdnet.com/article/first-death-reported-following-a-ransomware-attack-on-a-german-hospital/iisbf gelisim haber. (2021).

https://iisbf.gelisim.edu.tr/bolum/isletme-37/haber/stanford-universitesi-2021-yili yapay-zeka-raporu-yayimlandi

McElfresh, M. (2016).https://theconversation.com/cyberattack-on-ukraine-grid-heres-how-it-worked-and-perhaps-why-it-was-done-52802

Voss RF, Clarke J. (1986) Algorithmic Musical Composition, Silver Burdett Press, London.

Zabierowski W, Napieralski A (2003) Chords classification in tonal music. *Journal of Environment Studies* 10(5): 50-53.

Abiewskiro A, Moplskiiera Z. (2008) The Problem Of Grammar Choice For Verification. TCSET of the International Conference, House of Lviv Polytechnic National University, pp.19-23.

Healthwise Knowledgebase (1998) US Pharmacopeia, Rockville. http://www.healthwise.org. Accessed 21 Sept 1998