Savunma ve Güvenlik Araştırmaları Dergisi, 1(1): 75-96 (2024)

Basılı/Printed ISSN: **3023-5278**

SAVUNMA VE GÜVENLİK ARAŞTIRMALARI DERGİSİ

The Journal of Defence and Security Research

https://dergipark.org.tr/tr/pub/saga

Siber Tehdit İstihbaratında Yapay Zeka ve Makine Öğrenmesi

Artificial Intelligence and Machine Learning in Cyber Threat Intelligence

Beyza ÖZDEMİR[1,*]

[1] *Millî Savunma Üniversitesi, Alparslan Savunma Bilimleri ve Millî Güvenlik Enstitüsü, İstihbarat Çalışmaları Programı, 06654, Çankaya/ANKARA*

Makale Bilgisi

Araştırma makalesi
Başvuru: 22.01.2024
Düzeltme: 01.03.2024
Kabul: 19.03.2024

Keywords

Cyber Threat Intelligence
Threat Analysis
Artificial Intelligence
Machine Learning

Anahtar Kelimeler

Siber Tehdit İstihbaratı
Tehdit Analizi
Yapay Zeka
Makine Öğrenmesi

Özet

Siber tehditler giderek karmaşık bir hal almaktadır. Bu tehditlerin hedefi olabilecek kurumların daha etkin savunma gerçekleştirme çabaları siber tehdit istihbaratının önemini artırmaktadır. Geleneksel yöntemlerin kullanımı ile siber tehdit istihbaratı, siber tehditlerin anlaşılması ve bu tehditlere karşı önlemlerin alınmasını sağlamaktadır. Yapay zeka ve makine öğrenmesi ile siber tehdit istihbaratının verimliliğini ve etkinliğini artırabilecek çalışmalar gerçekleştirilmektedir. Bu çalışmalar, büyük miktarda veriyi hızlı ve verimli bir şekilde analiz ederek, tehditlerin daha hızlı ve doğru bir şekilde tespit edilmesini ve anlamlandırılmasına yardımcı olmayı amaçlamaktadır. Bu noktadan hareketle bu çalışmada, yapay zeka ve makine öğrenmesinin siber tehdit istihbaratına faydaları ve nasıl uygulanabileceği incelenmektedir. Çalışma kapsamında, yapay zeka ve makine öğrenmesinin siber tehdit istihbaratının farklı aşamalarında nasıl kullanılabileceğinin açıklaması ve geliştirilmiş platformlar ile dünya çapında etki göstermiş saldırılara karşı gerçekleştirilen başarılı savunmalara örnekler sunulmaktadır.

Abstract

Cyber threats are becoming increasingly sophisticated. Efforts by corporations that may be the target of these threats to carry out more effective defense increase the importance of cyber threat intelligence. Using traditional methods, cyber threat intelligence provides understanding of cyber threats and taking precautions against these threats. Studies are carried out to increase the efficiency and effectiveness of cyber threat intelligence with artificial intelligence and machine learning. These studies aim to help detect and make sense of threats more quickly and accurately by analyzing large amounts of data quickly and efficiently. Starting from this point, the study examines the benefits of artificial intelligence and machine learning in cyber threat intelligence and how they can be applied. Within the scope of the study, an explanation of how artificial intelligence and machine learning can be used at different stages of cyber threat intelligence and examples of successful defenses against attacks that have a worldwide impact with developed platforms are presented.

* Beyza ÖZDEMİR, beyzazdmr05@gmail.com

1. GİRİŞ

Günümüz dünyasında gelişmekte olan dijital ekosistem, siber saldırı tehditlerinin gittikçe karmaşık bir hal almasına yol açmaktadır. Birçok farklı kültür ve alandan kurumlara ve kuruluşlara hatta ileri seviyelerde devletlere yönlendirilebilen bu tehditler ile baş edebilmek ve önlem alabilmek için devletlerin, kurumların ve kuruluşların siber güvenlik sistem ve stratejilerini güçlendirmeleri gerekmektedir. Siber Tehdit İstihbaratı (Cyber Threat Intelligence, CTI) bu aşamada kritik bir öneme sahiptir.

Siber tehdit istihbaratı, siber tehditlerin anlaşılabilmesi ve bu tehditlere uygun önlemlerin alınabilmesi için yapılan tehdit tanımlamasına fayda sağlamakla birlikte devletler, kurumlar ve kuruluşlar için hayati önem arz eden ağdaki sistemlerin tehditlere karşı nasıl korunduğu ve korunması gerektiği hakkında bilgi vermeyi amaçlamaktadır (Lee, 2023, s.21). Siber tehdit istihbaratı, ağdaki cihazlara karşı oluşan tehditler ile ilgili bilgilerin toplanması, analiz edilmesinin süreci ve sonucudur (Lee, 2023, s.5).

Tehdit analizi, bir sisteme ve sistemin işlediği bilgilere yönelik potansiyel güvenlik ve gizlilik tehditlerini tanımlamaya, analiz etmeye ve önceliklendirmeye yardımcı olan etkinlikleri içermektedir (Tuma, Calikli, ve Scandariato, 2018). Siber tehdit analizi Açık Kaynak İstihbaratı (Open Source Intelligence, OSINT), ağ trafik analizleri, güvenlik firmalarının raporları, saldırı tespit sistemleri, siber tehdit istihbaratı ve daha birçok farklı veri kaynağını içerebilmektedir. Siber tehdit istihbaratı, verilerin kaynaklardan toplanması, işlenmesi ve analiz edilmesi için çeşitli yöntem ve metodolojileri bir araya getirir. Bu kaynaklardan elde edilen büyük ölçeklerdeki veri, siber tehdit istihbaratı analistleri tarafından analiz edilmektedir. Ancak günümüzde verinin fazla ama niteliksiz veya güvenilir olmaması sebebiyle analistler elde edilen büyük ölçekteki verileri analiz etmeleri esnasında sorun yaşayabilmektedirler.

Yapay zeka (Artificial Intelligence, AI), sorunu önceden tahmin etmek ve harekete geçmek için milyonlarca veriyi hızlı bir şekilde analiz edebilmektedir. Bu özelliği ile yapay zeka, sürekli olarak gelişen çeşitli siber saldırı tehditlerine karşı korunmak için analitik zekayı kullanabilen bir aracı olarak karşımıza çıkmaktadır (Kaur, Gabrijelčič ve Klobučar, 2023). Yapay zekanın alt kümelerinden biri olan Makine Öğrenmesi (Machine Learning, ML) ile makineler verilere bağlı olarak öğrenen ve performans geliştiren sistemler oluşturmaya odaklanmaktadırlar (Oracle Türkiye, 2014). Yapay zeka ve makine öğrenmesi, büyük miktarda veri sağlamakla birlikte bu verilerin akıllıca analiz edilebilmesini mümkün kılmaktadırlar (Anonim, 2018). Yapay zeka, hedeflere ulaşmak için veri inovasyonu ve fiziksel zekayı birlikte kullanarak varsayımları kabul etme, farklı örnekleri görme, seçimler yapma ve bunlar sonucunda gerçeğe ulaşarak derinlemesine düşünebilme kapasitesinin kullanılmasını sağlayabilmektedir (Jain 2021, s.101). Makinelerin insanlar gibi hatta daha hızlı bir şekilde çalışması yapay zeka ile sağlanabilmektedir (Rathore, Singh ve García-Díaz, 2020).

Siber saldırı tehditlerinin sahip olduğu ve günümüzde artarak devam eden organize ve ısrarcı tehdit aktörleri, paramiliter teknikler, karmaşık ve çoğu zaman askeri tarzda taktiksel yapısı, tehdit analistleri tarafından siber tehditlerin, yöntemlerin ve hedeflerin anlaşılmasını zorlaştırmaktadır.

Bu çalışmanın hipotezi; yapay zeka ve makine öğrenmesinin siber tehdit istihbaratı üretimi sürecindeki başarının artırılmasına, siber tehdit analizlerinin daha hızlı ve doğru bir biçimde gerçekleştirilmesine yardımcı olma potansiyeline sahiptirler. Bu çalışma içerisinde yapay zeka ve makine öğrenmesinin siber tehdit istihbaratı etkinliklerini nasıl geliştirilebileceği ve tehdit analizinin siber tehdit istihbaratı uygulamalarına nasıl entegre edilmesi gerektiği örnek olaylar ile incelenmektedir.

Dört bölümden oluşan bu çalışmada öncellikle yapay zeka ve makine öğrenmesinin siber tehdit istihbaratı ve analizinde kullanımını araştıran literatürdeki çalışmalar incelenmektedir. İkinci olarak Siber tehdit istihbaratının türleri ve siber tehdit istihbarat çarkı üzerinde durulmuş ve ardından üçüncü bölümde yapay zeka ve makine öğrenmesinin siber tehdit istihbaratı türlerine ve istihbarat çarkına uygulanması ele alınarak popüler yapay zeka ve makine öğrenmesi tabanlı siber tehdit analizi yapan platformlar incelenmiştir. Dördüncü bölümde örnek olaylar ile yapay zeka ve makine öğrenmesi tabanlı uygulamaların siber tehdit istihbaratındaki başarıları ele alınmış ve son olarak değerlendirmeler sonuç kısmında incelenmiştir. Çalışma yapay zeka ve makine öğrenmesi tabanlı platformların kurumlar tarafından kullanımına odaklanması sebebiyle buna benzer yapıya sahip uygulamaların tehdit aktörleri tarafından kurumlara yönlendirilmesini inceleme dışında bırakmaktadır.

2. YAPAY ZEKA VE İSTİHBARAT

Yapay zeka endüstriye ve günlük hayata yenilik getirmektedir. Günlük hayatın birçok yerinde yapay zeka sohbet robotları, müşteri hizmetleri, biyometri tanıma sistemleri gibi farklı formlarda karşımıza çıkmaktadır. Teknoloji ve endüstride yer edinmiş önemli şirketler uygulamalarına yapay zekayı adapte etmektedir. Yapay zekanın metodolojisi olan makine öğrenmesi ise spesifik sorunları çözümlemek için büyük veri setlerindeki örüntüleri tanımlamada en verimli yoldur. Bu noktadan yola çıkılarak günümüzde kurumlar, kuruluşlar ve devletler için ciddi bir risk oluşturan siber tehditlerin önceden tespiti için çalışan siber tehdit istihbaratının etkinliğini artırma potansiyeli dahilinde yapay zeka ve makine öğrenmesi araç olarak görülebilir.

Dutta ve Kant (2020) çeşitli kaynaklardan eyleme dönüştürülebilir siber tehdit istihbaratını elde etmek için makine öğrenimi destekli bir mimari önermişlerdir. Çeşitli kaynaklardan toplanan veri ile veri setleri oluşturulmuştur. Bu veri setleri güvenlik açığı, zayıflık veya kötü amaçlı yazılımla ilgili duyarlılık için -1 ve iyi huylu gönderilerle ilgili duyarlılık için 0 olarak etiketlenerek ön işleme aşamasından geçirilmiştir. Son olarak veri seti makine öğrenmesi tabanlı sınıflandırma uygulamasında işlenmiştir. Yapay zeka ve makine öğreniminin siber tehdit istihbaratına entegrasyonunun, tehdit hesaplama süresini düşürdüğü görülmüştür. Güven (2023), veri ihlali ve veri sızıntısı olarak tespit edilen kaynakları

tarayarak elde ettiği verileri analiz ederek kural tabanlı ve yapay zeka destekli bir sızıntı verisi işleme modeli geliştirmiştir.

Mittu ve Lawless (2015), yaptıkları incelemelerle birlikte bilgi sistemlerine ve bulut bilişim platformlarına zarar vermeyi amaçlayan Gelişmiş Kalıcı Tehditleri (Advanced Persistence Threats, APT) tespit etmek için yapay zeka ve makine öğrenimini kullanımına örnek bir yol önermişlerdir. Wang (2021), yapay zekanın alt dallarından olan Doğal Dil İşleme'yi (Natural Language Processing, NLP) kullanarak, bankacılık sektöründeki şirketlerin PCI/DSS endüstri standardına uyabilmesi için finansal işlem sürecinde siber tehditleri tanımlayabilen bir yaklaşım geliştirmiştir.

Dilmaghani ve diğerleri (2019), yapay zeka ve makine öğrenmesi iş akışında büyük verilerin yol açtığı gizlilik hususlarını ve güvenlik sorunlarını ihlal eden mevcut tehditlere genel bir bakış sunmaktadır. Kamrull ve diğerleri (2019), siber tehdit tespiti uygulamalarına yapay zekanın eklenmesiyle IDPS sistemlerinin tespit oranının artırılabileceğini ve makine öğrenmesi tekniklerinin adaptasyonu ile APT'nin farklı aşamalarını tespit eden senaryolar incelemiştir. Ancak siber tehdit tespitinde yapay zekanın uygulanmasının başka riskleri de beraberinde getirebileceğinin üzerinde durulmuştur.

Literatürde olumlu sonuçlara ulaşılmış araştırmalar olmasına rağmen unutulmamalıdır ki makine öğrenmesi tabanlı modeller de gerçek siber tehditleri her zaman tespit edememekte veya stabil bir durumu kötü niyetli bir tehdit olarak yanlış sınıflandırabilmektedirler. Arp ve diğerleri (2020), makine öğrenimi modellerinin performansını düşüren ve modelleri kullanım durumları için potansiyel olarak uygunsuz hale getiren 10 ince tuzağı incelemektedir. Barreno ve diğerleri (2010) ise makine öğrenmesi tabanlı bir sistemin yanlış sınıflandırmasının, tehdit aktörlerinin radarına girmesi ile nasıl daha kötüye gidebileceğinin üzerinde durmaktadır. Ulaşılan olumsuz sonuçlara çözüm olarak makine öğrenmesinin yanlış sınıflandırması, yapay zeka ile birlikte kullanımında çözümlenebilmektedir.

3. SİBER TEHDİT İSTİHBARATI (CTI)

Literatürde siber tehdit istihbaratının farklı prosedür ve bakış açılarına sahip yapısı dolayısıyla çok sayıda tanımlaması bulunmaktadır. Siber tehdit istihbaratı, her seviyedeki karar vericilere iletilebilecek şekilde kurumların veya kuruluşların siber uzaydaki ve bir ölçüde de fiziksel alandaki faaliyetlerine ilişkin bilgilerin sistematik olarak toplanmasına, mevcut ve ortaya çıkan tehditler hakkında durumsal farkındalığın korunmasına yardımcı olmak için analiz edilmesi ve dağıtılmasıdır (FIRST, 2018). Siber tehdit istihbaratı, siber alandaki zararlı bir olayı hafifletmek için yeterli anlayışı sağlayan, tehditler ve tehdit aktörleri hakkında bilgidir (Bank of England, 2016).

Tehdit analistleri kötü amaçlı bir yazılımın tekniklerini ve davranışlarını analiz etmek için Güvenlik İhlali Göstergelerini (Indicators of Compromise, IoCs) kullanmaktadırlar. Siber tehdit istihbaratında, bir IoC, potansiyel olarak tehlikeye atılmış bir sistemi belirlemek için kullanılabilen bir bilgi parçası olarak tanımlanmaktadır (Harrington 2013). Bu bilgi basit bir URL adresinden karmaşık bir dizi taktik, teknik ve prosedüre kadar değişebilir. IoC'ler, teknolojik altyapılardaki kötü niyetli faaliyetlerin tespitini hızlı

bir şekilde mümkün kılarak siber tehdit istihbaratının anahtarı haline gelmektedirler. Sistem yöneticileri, IoC'ler yardımı ile tehdit aktörleri tarafından gerçekleştirilmiş olması mümkün izinsiz ağa giriş denemelerini veya diğer kötü amaçlı etkinlikleri tespit edebilmektedirler. Ayrıca IoC'ler, bir kuruluşun olaylara müdahale stratejilerini geliştirmek için de siber tehdit istihbaratı sağlayabilmektedir (Trend Micro Incorporated, 2023).

Siber alandaki saldırılar, tehdit aktörlerinin yöntemlerini ve saldırı düzenini tanımlayan önemli tehdit bilgilerini içermektedirler. Tehdit aktörleri becerilerini tutarlı bir şekilde geliştirebilmekle birlikte hali hazırda kullandıkları yöntemlere sadık kalmak eğilimindedirler. Tehdit aktörlerinin uyguladığı bu yöntemlere Taktik, Teknik ve Prosedürler (Tactics, Techniques & Procedures, TTPs) adı verilmektedir. TTP'ler, bir tehdit aktörünün istenen hedefe ulaşmak için nasıl bir girişimde bulunduğunun bilgisidir (Lee, 2023). 'Taktik', tehdit aktörünün davranış ve stratejilerinin spesifik açıklamasını ifade etmektedir. Düşmanın belirli bir hedefe ulaşmak için kullandığı bir dizi davranış ve eylemi içermektedir. 'Teknikler', tehdit aktörü tarafından gerçekleştirilen eylemlerin ayrıntılı bir tanımını ifade etmektedir. Bunlar, bir taktik eylemin nasıl gerçekleştirilebileceğini açıklayan kılavuzlar ve ara yöntemlerdir. 'Prosedürler' ise tehdit aktörünün belirli bir tekniği uygulamak için kullandığı sıralı talimatları ifade etmektedir. Bir tehdit aktörünün hedeflerine başarılı bir şekilde ulaşmasını sağlayan özel faaliyetlere ilişkin ayrıntılı açıklamaları içermektedir. (Strom vd., 2020; Raza, 2023).

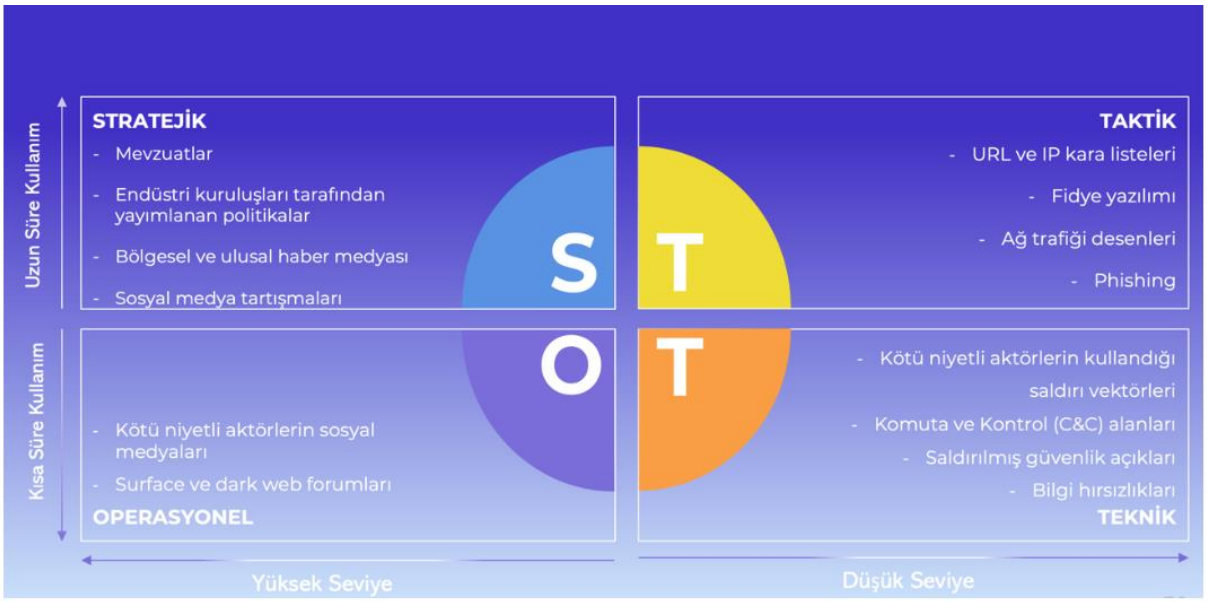
TTP'deki taktik ve teknikler, tehdit aktörünün hedefine ulaşan bir saldırı gerçekleştirebilmesi için gerekli olan çerçeve iken prosedürler, tehdit aktörünün tekniği uygulama detaylarıdır. TTP'ler, tehdit aktörüne özgü ve kimlik tespitinde kullanılabilecek bir tür parmak izi oluşturmaktadırlar. Buna göre TTP'ler, tehdit aktörüyle ilişkili faaliyet kalıplarının oluşturulmasına, saldırının arkasındaki tehdit aktörünün ve saldırıdaki spesifik prosedür ve tekniklerin belirlenmesi yardımcı olmak için kullanılabilmektedir. TTP'ler arasındaki ilişkilerin erken tespiti, siber tehdit aktörlerinin ve bunların saldırı vektörlerinin teşhisi için etkili bir strateji oluşturulmasına yardımcı olabilmektedirler.

Siber saldırılar belirli bir süreç içerisinde gerçekleşmektedir. Saldırı sürecinde saldırgan tarafından belirlenen hedeflere ulaşılabilmesi için bir dizi farklı adımın başarı ile gerçekleştirilmesi gerekir, planlanmış bu adımlar Siber Ölüm Zinciri (Cyber Kill Chain) olarak adlandırılmaktadır. Siber Ölüm Zinciri ifadesi, Lockheed Martin şirketi tarafından 2011 yılında geliştirilen Cyber Kill Chain® çerçevesinin, siber saldırı faaliyetlerinin tanımlanması ve önlenmesine yönelik Intelligence Driven Defense® modelinin bir parçasıdır. Model ile bir saldırganın kötü niyetli bir siber operasyonu tamamlamak için ilerlemesi gereken adımlar ortaya koyulmuştur. Siber Ölüm Zinciri modeli sırasıyla Keşif (Reconnaissance), Silahlanma (Weaponization), İletme (Delivery), Sömürme (Exploitation), Yükleme (Installation), Komuta ve Kontrol (Command and Control- C2), Eylem (Actions on Objectives) olmak üzere 7 aşamadan oluşmaktadır. Siber Ölüm Zincirindeki bu farklı aşamalar incelendiğinde, tehdit aktörünün önceki davranışını belirlemek için saldırının keşfedildiği noktadan

başlayarak Siber Ölüm Zinciri üzerinde geriye doğru ilerlenmelidir. Ayrıca bu sayede tehdit analistleri siber saldırı ve tehdit aktörünü ilişkilendirebilir.

3.1 Siber Tehdit İstihbaratı Türleri

Siber tehdit istihbaratı, tehdit aktörlerinin düzenlemiş olduğu saldırılara karşı elde ettikleri istihbatı incelerken farklı ölçeklerde seviyelere ayrılabilmektedir. Şekil 1'de görüleceği üzere siber tehdit istihbaratı kendi içerisinde taktik, teknik, operasyonel ve stratejik olmak üzere dört temel seviyeye ayrılmaktadır.



Şekil 1: Siber Tehdit İstihbaratı Seviyeleri İçerik Örnekleri.

Şekil 1'de siber tehdit istihbaratının kullanım süreleri ve kıymetlendirilen bilgilerin değerine göre seviyenlendirilmesi gösterilerek her seviye için içerik örnekleri verilmiştir. Bu alt başlığın devamında siber tehdit istihbaratı seviyeleri ayrı ayrı incelenmektedir.

3.1.1 Taktik Siber Tehdit İstihbaratı

Taktik siber tehdit istihbaratı, bir ağa ve ağdaki cihazlara sızmaya çalışan kötü niyetli tehdit aktörlerinin saldırı taktikleri ve amaçları gibi çeşitli noktalara odaklanılarak anlık veya yakın gelecekteki olaylar üzerinden önlemler alınmasını içermektedir. Geçmişte gerçekleştirilmiş saldırılardan ve IoC'lerden yola çıkılarak tehdit hakkında bilgi sahibi olunabilmektedir. Taktik siber tehdit istihbaratı, kurum veya kuruluşun siber alanda proaktif bir duruş sergilemesine, tehdit tespitinin kolaylaştırılmasıyla birlikte bir saldırı esnasında ve sonra sürecin profesyonel yürütülmesine katkı sağlar (Montasari vd., 2021, s.54).

3.1.2 Teknik Siber Tehdit İstihbaratı

Tehdit aktörü tarafından gerçekleştirilmiş eylemlerden yola çıkılarak tehdit aktörünün kullandığı TTP'lere odaklanmaktadır. Bu sayede siber tehdit istihbaratı, analistlerin ne tür anomalileri takip

etmeleri gerektiğinin belirlenmesine fayda sağlar (Montasari vd., 2021, s.54). Ancak hassas iş sektörlerinde siber alanın korunmasında teknik siber tehdit istihbaratında yetersiz kalınabilmektedir.

Finansal sektör kuruluşlarının siber tehdit istihbaratını, siber güvenlik programlarının önemli bir bileşeni olarak benimsemeleri ve uygulamaları gerektiği Bank of England tarafından 2016'da yayınlanan CBEST raporunda da yer almıştır. Rapor, "Maturity" modellerinin kuruluşlara uygun yapılandırılması ve kuruluşlarda siber tehdit istihbaratı güvenliğinin geleneksel güvenlikten farklı olduğu farkındalığının oluşturulması gerektiğini savunmaktadır. Rapora göre siber tehdit istihbaratı için bir çerçeve ve süreç oluşturulması ve siber tehdit istihbaratının siber güvenlik disiplinlerine entegrasyonu TTP'lerin analiz sürecine fayda sağlayabilir.

3.1.3 Operasyonel Siber Tehdit İstihbaratı

Kuruluşlara yönlendirilen siber saldırıların spesifik olarak özelliklerinin belirlenmesinde ve geleceğe yönelik olası siber tehditlerin incelenmesinde operasyonel siber tehdit istihbaratı kullanılmaktadır. Operasyonel siber tehdit istihbaratı, siber tehdit analistlerinin ağda önceden kontrol sağlamalarına ve saldırıları engellemelerine şans yaratır ve bu birçok açıdan güvenliğin altın standardıdır (Dinu, 2023). Operasyonel siber tehdit istihbaratında siber tehdit analistleri tarafından doğru adımların izlenmesi ile son kullanıcı olan karar alıcılara veya istihbarat kullanıcılarına iletilebilecek belirli bir olayı destekleyen veya karar verme sürecine yardımcı olabilen istihbarat üretimi sağlanır. Kısa ve orta gelecekteki tehditlere ve saldırılara yönelik istihbarat üretilir. Bu noktada hitap ettiği zaman açısından operasyonel siber tehdit istihbaratının, taktik siber tehdit istihbaratından farklılaşmasının temel sebebi tehdit aktörlerinin araçlarının değişmesi fakat TTP'lerinin değişmemesidir (Montasari vd., 2021).

3.1.4 Stratejik Siber Tehdit İstihbaratı

Stratejik siber tehdit istihbaratı, karar vericilerin kuruluşlarına yönelik siber tehditler ile oluşan riskleri yüksek seviyede ve spesifik olarak anlamalarını sağlar (Kurt Baker, 2023; Lee, 2023). Buradaki temel zorluk stratejik siber tehdit istihbaratının uzun vadeli bir geleceğe hitap etmesi dolayısıyla tehdit aktörünün yanlış anlaşılması halinde siber tehdit analistleri tarafından hazırlanıp karar vericiye iletilen hatalı bir stratejik istihbarat raporu ile karar verme süreci olumsuz etkilenmekte ve kurumlar tehditlere karşı savunmasız kalabilmektedir. Fakat doğru adımların izlenmesi ile stratejik siber tehdit istihbaratı kurumlara durumsal farkındalık sağlamakla birlikte karar vericilerin etkili savunma adımları oluşturmalarına, stratejik öncelikleri belirlemelerine ve bunlarla uyumlu siber güvenlik yatırımları yapmalarına olanak sağlamaktadır (Montasari vd., 2021).

3.2 İstihbarat Çarkı

İstihbarat çarkı verilerin toplanarak istihbarata dönüştürülmesi ve elde edilen istihbaratın yayılması sürecini ifade etmektedir. Siber tehdit istihbaratı için Şekil 2'de gösterilmekte olan "Amerikan Müşterek İstihbarat Çarkı (Döngüsü)" kullanılmaktadır.

Şekil 2: Amerikan Müşterek İstihbarat Çarkı.

Şekil 2'de görüldüğü üzere istihbarat çarkı, planlama ve yönetme, toplama, verilerin işlenmesi, analiz ve üretim, dağıtım ve entegrasyon, geri bildirim ve değerlendirme olmak üzere birbiriyle ilişkili altı aşamadan oluşmaktadır. Siber tehdit istihbaratı faaliyetleri gerçekleştirilmesi sürecinde bu aşamalar arasında gidip gelmeler, bazı aşamaların çıkarılması veya adımların paralel ilerletilmesi son kullanıcının gereksinimlerini karşılayan bir istihbarat ürünü sunmaya odaklanılarak düzenlenebilmektedir. Döngüde sürece bağlı olarak işlenen her adımın tamamı boyunca ve orijinal soruların etkili bir şekilde ele alınmasını sağlamak amacıyla eş zamanlı olarak değerlendirme ve geri bildirim süreçlerinin de gerçekleştirilmesi gerekmektedir. Döngü içerisindeki aşamalar ayrı ayrı adımlar olarak değil, örtüşen adımların bir sürekliliği olarak düşünülmelidir (Lee, 2023). Altı aşamalı bu istihbarat çarkını, geleneksel istihbarat çarkından farklı kılan özelliği değerlendirme ve geri bildirim aşamalarının süreç içerisindeki varlığıdır.

3.2.1 Planlama ve Yönetme

Siber tehdit istihbaratı üretiminin istihbarat çarkındaki ilk adımı "Planlama ve Yönetme" aşaması, son kullanıcıya özgü belirlenmesi gereken sınırlar, istihbarat gereksinimleri ve istihbarat öncelikleri ile birlikte yanıtlanması gereken soruları net bir şekilde ifade edilmelidir. Bu aşamada genellikle "ne, nerede, neden, nasıl, kim ve ne zaman" gibi ana istihbarat sorularının türevlerini ortaya çıkarmaktadır (Development, Concepts and Doctrine Centre, UK Ministry of Defence, 2011). Ayrıca bu aşamada son kullanıcıya ve onun isteğine bağlı olarak teslim edilmesi gereken istihbaratın hangi formatta, zamanda ve türde (stratejik, operasyonel, teknik, taktik) olması gerektiği açık bir şekilde belirlenmeli ve ileri aşamalar için ifade edilmelidir. Bu aşamanın önemli bir yönü, ürünün tamamını kimin tüketeceğini ve

bundan yararlanacağını anlamak olmalıdır. Bu aşamada istihbarat tüketicisi ile istihbarat üreticisi arasında güçlü bir iletişim olması gerekmektedir.

3.2.2 Toplama

Siber tehdit istihbarat çarkındaki bir sonraki adım ham verilerin toplanıp uygun formatta diğer adımlara iletilmesini içeren "Toplama" aşamasıdır. Bu aşamada toplanan verilerin ilk adımda belirlenen sınır ve gereklilikleri karşılaması gerekmektedir. Siber tehdit istihbaratı verileri, organizasyon içi ağdan, güvenlik sistemlerinden, güvenilir siber güvenlik şirketlerinden, açık kaynaklardan, APT gruplarının belirlenmiş TTP'lerinden, tehdit aktörlerinin iletişimlerinden ve daha birçok farklı iç ve dış kaynaklardan edinilebilmektedir. Bu veri kaynakları aracılığıyla IoC'ler analiz edilebilir (Montasari vd., 2021).

Doğru verinin elde edileceğe kaynağa ulaşma aşamasında hangi kaynaklardan istenen bilginin edinilebileceği ve zaman uyumu sağlanabileceği konularında dikkatli planlama yapılması gerekmektedir. Endüstri kurumlarının üyeleri veya istihbarat ortakları gibi güvenilir veri kaynakları değerli veri kaynaklarıdır. Ayrıca süreç içerisinde siber tehdit aktörlerinin motivasyonları değişkenlik gösterebilmektedir. Bazı tehdit aktörleri dikkat çekmek için eylemlerini medyada duyurabilmektedir.

3.2.3 Verinin İşlenmesi

"Verinin İşlenmesi" adımı, siber tehdit istihbarat çarkında ham verilerden istihbarata ulaşmayı ifade etmektedir. Bir önceki aşamada birden fazla kaynaktan toplanan ham verinin analistler tarafından kullanılabilir ve anlaşılabilir bir forma dönüştürülmesini içermektedir. Bu ham verilerin, istihbarat üretimine uygun formlara dönüştürülmesi çevirileri, şifre çözmeyi ve veri azaltmayı içerebilmektedir

3.2.4 Analiz ve Üretim

Siber tehdit istihbarat çarkının bir sonraki aşaması işlenmiş verilerin anlamlandırılarak istihbarata dönüştürüldüğü "Analiz ve Üretim" adımıdır. Bu aşamada işlenmiş veri ve son kullanıcı ihtiyaçları çerçevesinde siber tehdit analistinin sentezleme ve analiz becerileriyle istihbarat elde edilmektedir. Analistler, analizlerine getirebilecekleri açık veya bilinçaltı önyargılarının farkında olarak kendi tarafsızlıklarını sağlamalı ve yeni bilgi veya istihbarat elde edildikçe analizlerini yeniden işlemelidirler (Lee, 2023). Ek olarak bu aşamada, kaynakların ve toplanan materyallerin güvenilirliğini değerlendirmek ve öngörücü ve eyleme geçirilebilir olması gereken doğru ve tarafsız değerlendirmeleri sağlamak için çeşitli kelime öbekleri, Admiralty Kodu, Trafik Işığı Protokolü (Traffic Light Protocol, TLP) gibi çeşitli yaklaşımların uygulanması gerekmektedir.

Bu aşamanın amacı olası güvenlik tehditlerini araştırmak ve ilgili hedef kitleyi Planlama ve Yönlendirme aşamasında tanımlanan istihbarat gereksinimlerini karşılayacak bir formatta bilgilendirmektir (Recorded Future, 2020).

3.2.5 Dağıtım ve Entegrasyon

"Dağıtım ve Entegrasyon" aşaması siber tehdit istihbarat çarkında temel anlamıyla üretilen istihbaratın, istihbarat üreticisinden istihbarat tüketicisine aktarılması sürecidir. Dağıtım, ham veya tamamlanmış istihbaratın, sürecin başlangıcından itibaren devam eden istihbarat gereksinimlerini başlatan politika yapıcılara dağıtılmasıdır (Groce, 2016).

Siber tehdit istihbaratının eyleme geçirilebilmesi için doğru hedef kitleye doğru zamanda ulaştırılması gerekmektedir. Bir siber tehdit istihbarat döngüsü adımı ile diğeri arasında sürekliliğin sağlanabilmesi için dağıtım aşamasının izlenebilir olması gerekmektedir. Bunu başarmanın yollarından biri, siber tehdit istihbarat döngüsünün her aşamasını takip etmek için tüketicilerin diğer güvenlik sistemleriyle entegrasyonunu sağlayan sistemleri kullanmaktır. Geri bildirim alarak ve mevcut istihbarat gerekliliklerini iyileştirerek veya yenilerini oluşturarak siber tehdit istihbarat döngüsü yeniden başlatılabilmektedir.

3.2.6 Değerlendirme ve Geri Bildirim

Siber tehdit istihbarat döngüsünün son aşaması "Değerlendirme ve Geri Bildirim" aşamasıdır. Bu son adımda, son kullanıcı olan karar vericilerin veya istihbarat tüketicilerinin istihbarat üreticilerine gereksinimlerinin karşılanıp karşılanmadığı ve süreçte herhangi bir düzenleme veya iyileştirmeye ihtiyaç olup olmadığı konusunda geri bildirim vermesini içermektedir. Ayrıca gereksinimlerde yapılacak herhangi bir revizyonun bu adım içerisinde yayınlanması gerekmektedir.

4. SİBER TEHDİT İSTİHBARATINDA YAPAY ZEKA VE MAKİNE ÖĞRENMESİ

Yapay zeka ve makine öğrenmesi, siber tehdit istihbaratı uygulamalarını önemli ölçüde iyileştirebilecek umut verici iki araştırma alanıdır. Yapay zeka ve makine öğrenmesi tabanlı tehdit analizi uygulamaları, bir ağ üzerinde anormali tespitini geleneksel yöntemlerle gerçekleştiren uygulamalara göre daha etkili bir şekilde gerçekleştirebilmektedirler. Artan gelişme hızı ve daha etkili önlemlere duyulan ihtiyaç nedeniyle, yapay zeka ve makine öğrenmesi, sayıları giderek artan siber tehditler ve saldırılar ile başa çıkma sorununa bir çözüm olarak karşımıza çıkmaktadır.

Yapay zeka, insan zekasını simüle etmek ve genişletmek için teorileri, yöntemleri, teknikleri ve uygulama sistemlerini araştıran ve geliştiren, bilgisayar bilimlerinin hızla büyüyen bir dalıdır (Li, 2018). Yapay zeka aynı zamanda bilgisayar programları aracılığıyla öğrenme, çıkarım, algılama ve dil anlama yeteneklerini uygulayan bir teknolojidir. Yapay zekanın uygulanmasına yönelik birçok yaklaşım vardır. Bu yaklaşımlarla birlikte yükselişe geçen yapay zekanın birden fazla sektöre ve alana sürekli nüfuz etme ve çapraz entegrasyon eğilimi ortaya çıkmaktadır (Zeng, 2022).

Yapay zekanın alt dallarından biri olan makine öğrenmesi, çevredeki ortamdan öğrenerek insan zekasını taklit etmek için tasarlanmış, gelişen bir hesaplamalı algoritma türüdür. Makine öğrenimi algoritması, belirli bir sonucu üretmek için tam anlamıyla programlanmadan istenen görevi gerçekleştirmek için

girdi verilerini kullanan bir hesaplama sürecidir. (El Naqa & Murphy, 2015). Makine öğrenimi, eldeki göreve yönelik çözümü optimize etmek için çevredeki ortamdan öğrenebilen bilgisayar algoritmaları sunmaktadır. Yapay zeka, olasılık ve istatistik, bilgisayar bilimi, bilgi teorisi ve bilişsel nöropsikoloji gibi çeşitli alanlardaki uzmanlıklara dayanmaktadır.

Yapay zeka ve makine öğrenmesi, siber tehdit istihbaratı alanında büyük bir potansiyele sahiptir. Bu noktada yapay zeka ve makine öğrenmesinin siber tehdit istihbaratına entegrasyonu ile süreç içerisindeki farklı adım ve seviyelerde performans iyileştirmeleri gözlemlenebilir.

4.1 Siber Tehdit İstihbaratına Yapay Zeka ve Makine Öğrenmesinin Uygulanması

Yapay zeka ve makine öğrenmesi istihbarat türlerinin geliştirilmesi sürecine birçok farklı fayda sağlayabilir. Kısa, orta ve uzun vadedeki süreçlerdeki değişiklikler ile kurum siber tehdit istihbaratı üretimi ve tehditlere karşı savunmada daha stabil bir duruş sergileyebilir.

Stratejik siber tehdit istihbaratı boyutundan bakıldığında karmaşık veri kümelerinin makine öğrenmesi yardımıyla analiz edilerek anlam çıkarılmasıyla karar alıcıların tehdit kökenini daha iyi anlayarak hedef belirlemelerine ve kurumların uzun vadede proaktif savunma stratejileri planlamalarına yardımcı olabilir. Ayrıca yapay zeka yardımı ile organizasyon içerindeki zayıf noktaların tahmini sağlanarak savunma stratejileri güçlendirilebilir ve en kritik alanlara odaklanılarak güvenlik yatırımları optimize edilebilir.

Operasyonel siber tehdit istihbaratı bağlamında yapay zeka ve makine öğrenmesi normal ağ ve sistem davranışlarını öğrenerek anomalilerin tespit edilmesini sağlayabilir. Ayrıca makine öğrenmesi ile kullanıcı davranışları ve varlık ilişkileri modellenerek tehdit analistlerinin iç tehditleri ve yetkisiz erişimleri belirlemeleri ve kurum içerisindeki potansiyel riskleri düşürmelerini sağlanabilir.

Taktik siber tehdit istihbaratında gerçekleşen anlık durumlar için yapay zeka ve makine öğrenmesi yardımıyla büyük veri setlerinin hızlı analizi ile anormal aktiviteler eş zamanlı tespit edilebilir. Ayrıca bu şekilde dinamik risk değerlendirmesi gerçekleştirilebilir. Bunun yanı sıra makine öğrenmesi ile teknik siber tehdit istihbaratı çerçevesinde tehdit aktörlerinin TTP'leri üzerinden analizler ve ilişkilendirmeler yapılarak benzerlik modelleri oluşturulabilir.

4.2 İstihbarat Çarkına Yapay Zeka ve Makine Öğrenmesinin Entegrasyonu

Yapay zeka ve makine öğrenmesi, siber tehdit istihbarat çarkının tüm aşamalarında kullanılabilecek güçlü araçlardır.

- *Verilerin Toplanması ve İşlenmesi:* İstihbarat çarkının ikinci ve üçüncü aşamalarında gerçekleştirilen ham verinin toplanıp işlenmesi adımları yapay zeka ve makine öğrenmesi ile otomatikleştirilerek kolaylaştırılabilir. Özellikle büyük boyutlardaki veri kümeleri ile ilgilenen kuruluşların daha hızlı ve doğru bir toplama ve işleme süreci gerçekleştirmelerine yardımcı

olabilir. Kuruluşlar, siber tehdit istihbaratını spesifik bağlamında, veri toplama ve işlemeyi otomatikleştirmek, mevcut güvenlik çözümleriyle birleştirmek, ayrık kaynaklardan yapılandırılmamış verileri alarak tehdit aktörlerinin uzlaşma ve işleyiş tarzlarına ilişkin bağlam ekleyerek farklı yerlerden gelen bilgileri birbirine bağlamak için yapay zeka ve makine öğrenimi yöntemlerinden faydalanabilir.

Örneğin kurumlar, yapay zeka ve makine öğrenmesi yardımıyla kendilerine yönlendirilebilecek olası siber saldırılar için dark web ve diğer birçok açık kaynak üzerinden otomatik olarak siber tehdit istihbaratı verilerini toplayabilirler. Özellikle sosyal medyadan toplanan veriler makine öğrenmesi modelleri yardımıyla duygu ve ton analizine tabi tutularak işlenebilir. Kurumlar elde ettikleri bu bilgileri yapay zeka ve makine öğrenmesi yardımıyla birbirleri ile ilişkilendirerek kendilerine yönelik olası saldırıları tespit edebilirler.

- *Öznitelik Çıkarımı ve Analiz:* İstihbarat çarkının dördüncü aşamasında yer verilen analiz ve istihbaratın üretimi adımında yapay zeka ve makine öğrenmesi veriler üzerinden öznitelik çıkarımı gerçekleştirerek, siber tehdit istihbaratının anlaşılması için gereken spesifik özellikleri belirleyebilir. Hızla değişim gösteren siber alanda oldukça kısa süreler içerisinde değişen tehdit modelleri makine öğrenmesi ile tanıtılarak yeni tehdit türlerinin keşfi ve makinenin sürekli öğrenimi sağlanabilir.

  Örnek olarak bankacılık sektöründeki şirketlere yönelik gerçekleştirilen fidye saldırıları ile müşterilerin kişisel bilgilerinin çalınması amaçlanabilmektedir. Şirketlerin siber güvenlik ekipleri, saldırıları araştırmak için manuel yöntemler kullanarak vakit kaybetmek yerine yapay zeka ve makine öğrenmesi ile süreci hızlandırabilirler. Yapay zeka ile saldırı örnekleri hızlı bir şekilde analiz edilerek yeni varyantalar otomatik olarak tanımlanır ve siber tehdit istihbarat raporları otomatik olarak oluşturulabilir. Makine öğrenmesi ile ise saldırıların arkasındaki altyapı, saldırganların taktikleri belirlenerek ve siber saldırıların olası hedef ve etkilerini tahmin etmek için kullanılabilir. Bu şekilde yapay zeka ve makine öğrenmesi ile daha hızlı bir şekilde gelecekteki saldırıların daha iyi tahmin edilerek önlenmesi, operasyonların optimizasyonsunu ve kaynakların daha etkin kullanımı sağlanabilir.

- *Siber Tehdit İstihbaratının Dağıtılması:* Beşinci adım olarak istihbarat çarkında yer alan istihbaratın dağıtımı ve entegrasyonu sürecinde siber tehdit istihbaratı üreticileri ve tüketicileri için kullanıcı dostu ara yüze sahip yapay zeka ve makine öğrenmesi yardımıyla siber tehditleri otomatik olarak önceliklendirip güncelleyebilen bir platform oluşturarak üretilen istihbarat güvenli bir şekilde dağıtılabilir.

  Örneğin siber güvenlik şirketleri, farklı kaynaklardan elde ettikleri siber tehdit istihbaratını, geliştirdikleri yapay zeka tabanlı bir uygulama yardımıyla güvenli ve kolay arayüz ile müşterilerine dağıtabilirler. Makine öğrenmesi ile siber tehdit türüne, ilgi seviyesine ve kaynağa

bağlı olarak otomatik sınıflandırma ve öncelliklendirme yapılarak uygulama üzerinden siber tehdit istihbaratı üretici ve tüketicilerine yönlendirme sağlanabilir.

- *Değerlendirme ve Geri Bildirim:* İstihbarat çarkının son aşaması olarak görülmekle birlikte her adımda icra edilen değerlendirme ve geri bildirim sürecinde yapay zeka ve makine öğrenmesi tabanlı gerçekleştirilen tehdit tespitinin süreci hızlandırması ile anlık tehdit tespiti yapılarak gerçek zamanlı geri bildirim ve değerlendirmeler gerçekleştirilebilir.

  Örnek olarak siber güvenlik ekipleri yapay zeka tabanlı gerçek zamanlı geri bildirim sağlayan bir sistem geliştirerek gerçek zamanlı değerlendirme ve iyileştirme yapabilirler. Özellikle Siber tehdit istihbarat gösterge panolarından gelen geri bildirimler ile siber tehdit istihbaratı etkinliklerini optimize etmek için veri odaklı geri bildirimler sağlanabilir. Bu sayede siber güvenlik ekipleri siber tehditlere karşı daha hızlı ve etkili etkinlikler gerçekleştirebilirler.

4.3 Yapay Zeka ve Makine Öğrenmesi Tabanlı Siber Tehdit Analizi Yapan Platformlar

Yapay zeka ve makine öğrenmesi tabanlı siber tehdit analizi yapan birçok platform bulunmaktadır. Bu platformlar, büyük veri kümelerini analiz ederek anomalileri tespit etmeye ve siber tehditleri önceden belirlemeye odaklanmaktadır. Kullanımı kıyasla daha popüler olan platformlar:

- *DeepArmor:* SparkCognition tarafından geliştirilmiş hem istemci tarafı kullanıcıların, bulutta barındırılan yönetim konsolunu hem de küresel bulut hizmetlerini içeren Hizmet Olarak Yazılım (Software as a Service, SaaS) tabanlı bir koruma platformudur. DeepArmor, bir işlemin, dosyanın veya bellek içi etkinliğin anormal veya kötü niyetli olup olmadığını analiz etmek ve tahmin etmek için geliştirilmiş makine öğrenimi modellerinin ve yapay zekanın gücünden yararlanmaktadır (SparkCognition Inc, 2018).
- *Cyber AI Analyst:* Darktrace tarafından geliştirilmiş Cyber AI Analyst, siber güvenlik ekiplerini güçlendirmek ve tehdit araştırmasını optimize etmek için oluşturulmuştur. Darktrace tarafından üretilen bir diğer ürün olan Enterprise Immune System içerisinde ortaya çıkan her olay Cyber AI Analyst tarafından sürekli olarak incelenip otonom önceliklendirme ve raporlama için uzman insan düşünce süreçlerini taklit edilmektedir. Bu teknoloji ile birlikte tehdit analistlerin sezgisi ve yapay zekanın tutarlılığı, hızı ve ölçeklenebilirliği birleştirilmektedir. Cyber AI Analyst, anlamlandırma süresini ve yanıt verme süresini önemli ölçüde kısaltmaktadır (Darktrace Team, 2020).
- *Vectra AI:* Vectra AI içerisinde Vectra Threat Detection and Response, Vectra Attack Signal Intelligence ve Vectra Threat Intelligence platformlarını bulundurmaktadır. Vectra Threat Detection and Response platformu ile siber tehditleri gerçek zamanlı olarak tespit ederek bunlara cevap vermek için yapay zeka ve makine öğrenimini kullanan yüksek riskli tehditleri belirleme ve önceliklendirme için ağ trafiğinin sürekli izlenmesine ve analiz edilmesine olanak sağlayan bir platformdur. Ayrıca platform, gelişmiş kalıcı tehditlere ve hedefli saldırılara karşı

ek bir savunma katmanı sağlayarak güvenlik duvarları ve antivirüs yazılımı gibi geleneksel güvenlik önlemlerini tamamlamak üzere tasarlanmıştır. Şirket içinde, bulutta veya hibrit bir çözüm olarak ve çok çeşitli güvenlik teknolojileriyle entegre edilerek kullanılabilmektedir (InfoSEC, 2019). Vectra Attack Signal Intelligence, kuruluşlara potansiyel siber tehditler hakkında gerçek zamanlı bilgi sağlar. Son olarak Vectra Threat Intelligence platformu ise kuruluşlara mevcut ve gelecekteki siber tehditler hakkında bilgi ve analizler sağlamaktadır.

- *Cylance AI:* BlackBerry tarafından geliştirilmiş olan Cylance AI, daha iyi güvenlik sonuçları sunmak amacıyla modern altyapı, eski cihazlar, yalıtılmış uç noktalar ve aradaki her şey için kapsamlı koruma sunmaktadır. Yapay zeka ve makine öğrenmesini kullanarak siber tehdit tespiti ve olası saldırıların engellenmesi sağlanmaktadır. Cylance AI, ağ, uç nokta, bulut ve kimlik verilerinden gelen verileri analiz ederek, bilinen ve bilinmeyen tehditleri tespit etmektedir. Yapay zeka ve makine öğrenimini kullanarak, normal davranıştan sapmaları tespit ederek tehditlerin olası etkilerini tahmin etmektedir (BlackBerry Limited, t.y.).
- *QRadar SIEM:* IBM'in Güvenlik Bilgi ve Olay Yönetimi (Security Information and Event Management, SIEM) çözümüdür. QRadar SIEM, açık standartları kullanarak çok sayıda dış veri kaynağını (mevcut bulut, SaaS, e-posta, kimlik, diğer veri güvenliği sistemleri) entegre ederek net ve eyleme geçirilebilir önerileri hızlı bir şekilde kullanıcıya döndürebilmek için yapay zeka destekli uyarı önceliklendirme ve korelasyon uygulaması ile tek bir yönetim noktasından tehdit tespiti yapan bulutta yerel bir çözümdür. QRadar SIEM, uyarıları otomatik olarak siber tehdit istihbaratıyla birleştirerek ve bunları MITRE ATT&CK çerçevesiyle eşleştirip önerilen uygulamaları gerçekleştirmektedir (IBM, t.y.).

İncelenen bu platformların daha iyi karşılaştırılabilmesi adına Tablo 1'de temel işlev, yapay zeka ve makine öğrenmesi kullanımı, platformun hitap ettiği hedef kitle, API desteği, entegrasyonlar, destekleyen platformlar, fiyatlandırma gibi belirli parametreler doğrultusunda ele alınmıştır.

	DeepArmor	Cyber AI Analyst	Vectra AI	Cylance AI	QRadar SIEM
Temel İşlev	Siber tehdit tespiti ve engellemesi	Siber tehditleri analiz etme ve istihbarat üretme	Siber tehdit tespiti ve engellemesi	Siber tehdit tespiti ve engellemesi	Siber güvenlik olaylarını yönetme
Yapay Zeka Kullanımı	- Derin öğrenme - Makine öğrenmesi - Davranış analizi	- Risk değerlendirmesi - Makine öğrenmesi - Davranış analizi	- Derin öğrenme - Makine öğrenmesi - Davranış analizi	- Derin öğrenme - Makine öğrenmesi - Davranış analizi	- Korelasyon - Makine öğrenmesi - Anormallik tespiti
Makine Öğrenmesi Kullanımı	- Anormallik tespiti - Tehdit avı - Davranış analizi	- Tehdit avı - Davranış analizi - Risk değerlendirme	- Anormallik tespiti - Tehdit avı - Davranış analizi	- Anormallik tespiti - Tehdit avı - Davranış analizi	- Korelasyon - Anormallik tespiti - Tehdit avı
Hedef Kitle	Küçük-orta ölçekli işletmeler ve girişimler için siber tehdit tespiti	Şirketler için otonom siber tehdit tespiti	SaaS, bulut ve şirket içi dağıtımlarını korumak için yapay zeka siber güvenlik platformu isteyen güvenlik merkezleri veya bilgi teknolojileri yöneticileri	Siber güvenlik ve korunma yazılımı çözümü arayan kullanıcılar ve şirketler	Güçlü bir SIEM çözümü arayan siber güvenlik ekipleri
API Desteği	Yok	Yok	Var	Yok	Yok
Destekleyen Platformlar	SaaS/Web	SaaS/Web	SaaS/Web	- Windows - Mac - Linux - SaaS/Web - iPhone&iPad - Android	- Windows - Mac - SaaS/Web - Şirket içi sunucular
Üretici Şirket	SparkCognition	Darktrace	Vectra	BlackBerry	IBM
Entegrasyonlar	Yok	40'dan fazla entegre edilebilir teknoloji	30'dan fazla entegre edilebilir teknoloji	30'dan fazla entegre edilebilir teknoloji	90'dan fazla entegre edilebilir teknoloji
Müşteri Desteği	- Çevrimiçi destek - Telefon destek hattı	- Çevrimiçi destek - Telefon destek hattı	- Çevrimiçi destek - Telefon destek hattı - Canlı destek	Çevrimiçi destek	Çevrimiçi destek
Eğitim Paketi	Doküman	Doküman	- Doküman - Webinar - Canlı eğitim	Doküman	Doküman
Fiyatlandırma	Abonelik	Abonelik (Bedava deneme sürümü)	Abonelik	Abonelik (Bedava deneme sürümü)	Hem abonelik hem lisans (SaaS için sadece abonelik seçeneği)

Tablo 1: Yapay Zeka ve Makine Öğrenmesi Tabanlı Siber Tehdit Analizi Platformların Karşılaştırılması.

5. ÖRNEK OLAY İNCELEMELERİ

5.1 Ricoh Group

Ricoh Grubu, 2017 yılında WannaCry fidye yazılımı saldırısına maruz kaldıktan sonra dahili ağlarında hızla artan uyarılar ve görünürlük eksikliği sorunlarıyla karşı karşıya kalmıştır. CSIRT (Computer Security Incident Response Team) ekibi, gelişmiş ağ görünürlüğü ve tehdit tespitine olan ihtiyacın altını çizerek, günlükleri analiz etme ve saldırının sistemleri üzerindeki etkisini anlama konusunda zorluk yaşamıştır (Vectra, 2023).

Ricoh Grubu, araştırmaları sonucunda yapay zeka odaklı bir tehdit algılama ve yanıt platformu olan Vectra'yı uygulamaya koymuştur. Vectra, gerçek zamanlı izleme yetenekleri, kural oluşturmaya gerek kalmadan öncelikli uyarılar ve gelişmiş raporlama yetenekleri sağlamıştır. Platform sayesinde CSIRT ekibinin kurum genelindeki verileri yakalayıp analiz etmesine yardımcı olarak dahili ağ görünürlüğü sorununun üstesinden gelinmiştir (Vectra, 2023a)

Vectra ile iş birliği sonucunda Ricoh Grubu, tehditlerin erken belirtilerini tespit etme konusunda proaktif bir yaklaşım kazanmış ve bu da daha etkili karşı önlemlerin alınmasını sağlamıştır. Platform, yetkisiz erişim ve sanal bilgisayarlar da dahil olmak üzere gizli faaliyetleri ortaya çıkarmış ve şirketin bireysel sözleşmeler için bulut hizmetlerinin kullanımına karşı politikalar uygulamasını sağlamıştır. Vectra'nın kontrol panelinin netliği ve verimliliği, yapay zeka destekli tehdit tespitiyle birlikte, Ricoh Grup mevcut ve gelecekteki siber tehditlere karşı dirençli hale getirilmiştir (Vectra, 2023a).

5.2 PowerPepper

Kiralık hack grubu DeathStalker tarafından yürütülen PowerPepper, hassas iş bilgilerini çalmayı amaçlayan, uzaktan gönderilen kabuk komutlarını yürütebilen bir Windows bellek içi PowerShell arka kapısıdır. Kötü amaçlı bir Microsoft Word belgesi yoluyla gönderilen PowerPepper, fare hareketlerini engellemek, istemcinin medya erişim kontrol adreslerini filtrelemek ve tespit edilen antivirüs ürünlerine göre yürütme akışını uyarlamak gibi tekniklerle tespit edilmekten kurtulmaya çalışmaktadır (Barikat Siber Güvenlik, 2020). İlk raporlara göre PowerPepper, özellikle küçük ve orta ölçekli kuruluşlara odaklanarak Avrupa, Asya ve Amerika'daki ana bilgisayarları hedef almıştır (Lakshmanan, 2020).

Tehdit ortamının hızla gelişmesi ile DeathStalker gibi gruplar, kurumların en hassas verilerine erişebilmek için gelişmiş yeni yöntemler kullanmaktadır. Bu hassas veriler, uygun şekilde koruma altına alınmadıkları takdirde ciddi sonuçlanabilecek sorunların oluşmasına sebebiyet verebilmektedir. SparkCognition'ın DeepArmor platformu gibi siber güvenlik ürünleri oluşturmak için makine öğrenmesinin kullanımı ile kullanıcıların, DeathStalker gibi tehdit aktörlerinin önüne geçmesine ve kötü amaçlı yazılımların kurumu tehlikeye atmadan önce durdurulmasına olanak sağlamaktadır.

İmzalar, buluşsal yöntemler veya kurallara dayalı yaklaşımlar kullanmak yerine DeepArmor ürünü, dosya tabanlı ve bellek içi saldırıları önlemek için özel olarak yapay zekayı kullanarak PowerPepper

gibi yeni tehditlerin tespit edilmesini sağlamaktadır. SparkCognition, VirusTotal aracılığıyla IoC'leri çalıştırarak DeepArmor'un PowerPepper'ı tanımlama ve ona karşı savunma yeteneğini doğrulamayı başarmıştır. VirusTotal, bir PowerPepper dosyası üzerinde 66 makineden oluşan bir grubu test ederek, bugün itibariyle yalnızca 39 makinenin kötü amaçlı yazılımı tespit edebildiğini, geri kalanların ya dosyanın algılanmadan geçmesine izin verdiğini ya da dosyayı hiç işleyemediğini bulmuştur (SparkCognition, 2020).

Hedefleme yöntemi sadece PowerPepper'a özgü tasarlanmamalı, aynı zamanda küçük ve orta ölçekli işletmelerde dahi kuruluşlarını kapsamlı bir şekilde koruması için yapay zeka ve makine öğrenmesi tabanlı siber güvenlik çözümlerini kullanması gerekmektedir.

6. SONUÇ VE ÖNERİLER

Teknolojinin hızlı ilerleyişi, günlük yaşantının her alanında olduğu gibi siber alanda da kendini göstermektedir. Bu gelişimler doğrultusunda yeni siber tehditler ortaya çıkmaktadır. Bilinen tehdit yapısından farklı olarak daha karmaşık ve hedef odaklı ısrarcılığa sahip olan bu tehditler paramiliter teknikler ile hedeflerin siber alanda savunmasız bırakılmasını amaçlamaktadır. Tüm düzeyler ve çalışanlar siber tehditlerden etkilendikleri için, yakın gelecekte siber tehdit istihbaratının kuruluşların ve devletlerin operasyonlarına dahil edilmesinin giderek daha hayati hale geleceği öngörülmektedir (Montasari vd., 2021). Bu bağlamda kurumlar ve devletler siber savunma altyapılarını güçlendirme isteklerini siber tehdit istihbaratı ile karşılamaları gerekmektedir. Doğru bir şekilde uygulandığında siber tehdit istihbaratı, siber tehditlerin daha iyi anlaşılmasını kolaylaştırabilmekte, daha hızlı, daha hedef odaklı bir müdahaleye ve kaynak geliştirme ve tahsisine olanak sağlayabilir (Intel&Analysis Working Group, 2015).

Siber tehdit istihbaratı ile potansiyel risklerin belirlenmesi ve değerlendirmesi için açık ve kapalı platformlar da dahil olmak üzere çeşitli kaynaklardan veri toplanmaktadır. Toplanan verilerin istihbarat çarkı aşamalarından geçirilmesi ile adım adım olan ve olası tehditlere yönelik siber tehdit istihbaratı üretimi gerçekleşmektedir. Bu adımlar içerisinde amaç doğrultusunda farklı uygulamalar gerçekleştirilerek sonuç itibari ile tehdide yönelik bir istihbarata ulaşılmaktadır. Süreç içerisindeki bu faaliyetlerin, gittikçe karmaşık bir hal alan siber tehditlere karşı geliştirilmesi için arayışa geçilmiştir.

Yapay zeka, milyonlarca veri noktasını oldukça hızlı bir şekilde analiz ederek, olası sorunları önceden tahmin edip etkili çözümler üretme yeteneğine sahiptir. Yapay zeka, problem çözme, öğrenme ve karar verme gibi görevleri yerine getirebilen sistemler geliştirmeye odaklanmaktadır. Yapay zekanın alt dallarından biri olan makine öğrenmesi bilgisayarların deneyimden ve verilerden öğrenmesini sağlayan bir tekniktir. Makine öğrenmesi algoritmaları, büyük veri kümelerini analiz ederek örüntüleri ve ilişkileri bulabilmekte ve ayrıca bulduğu bu örüntü ve ilişkileri kullanarak tahminler ve öngörülerde bulunabilmektedir.

Yapay zeka ve makine öğrenmesi, diğer bilgisayar tabanlı bilgi sistemleri ile bütünleştirilerek bilgisayarların yeteneklerini, uygulanabilirliklerini ve becerilerini hızla artırmaktadır (Kebude, t.y.). Bu özelliği ile yapay zeka ve makine öğrenmesi her an günlük hayatta daha fazla ihtiyaç duyulan bir hal almakla birlikte siber tehdit istihbaratı uygulamalarını önemli ölçüde geliştirebilme ihtimaline sahip araştırma alanlarıdır. Yapay zeka, makinelerin verilerden öğrenmesini, kalıpların belirlemesini ve anomalilerin tanımasını sağlayarak siber güvenlik ortamındaki büyük ilerlemelere imkan sağlamaktadır. Makine öğrenimi algoritmalarının, olağandışı etkinlikleri ve potansiyel tehditleri tespit etmek için ağ trafiği, kullanıcı davranışı ve sistem günlükleri dahil olmak üzere çok büyük miktarda bilgiyi analiz ederek devamlılık gösteren öğrenme ve gelişme sürecine olanak tanımaktadır.

Siber tehdit istihbaratının daha efektif ve verimli kullanımı için yapay zeka ve makine öğrenmesi alanlarının siber tehdit istihbarat çarkı ve siber tehdit istihbarat türlerindeki faaliyetlerine, gerekliliklerine ve hedeflerine göre entegrasyon sağlanabilmektedir. Bu bağlamda yapay zeka ve makine öğrenmesi destekli güvenlik çözümleri, gerçek zamanlı tehdit tespiti, otomatik olay müdahalesi ve uyarlanabilir savunma mekanizmaları dahil olmak üzere çeşitli avantajları revize ederek sunabilmektedir. Bu anlık ve değişken yapı sebebiyle siber tehdit istihbaratı güvenlik çözümleri özelleştirilebilir olmalı ve belirli davranışsal faaliyetlere uyarlanabilen yapay zeka ve makine öğrenimi ile gelişmiş analitiklerle net ve eksiksiz bir araştırma sağlama kapasitesine sahip olmalıdır (Forcepoint, 2018).

Yapay zeka ve makine öğrenmesi destekli araçlar, büyük ölçekli veri analizini gerçekleştirebilmekte ve tehdit analistlerinin olan ve olası tehditlere hızla yanıt vermelerini sağlayabilmektedir. Ayrıca çeşitli kaynaklardan verilerin toplanmasını, işlenmesini ve analizini otomatik hale getirerek güvenlik ekiplerinin kritik noktaları yorumlamasını ve bunlara göre hareket etmeye odaklanmasını sağlamaktadır. Yapay zeka ve makine öğrenmesinin siber tehdit istihbaratı ile birleşimi sonucunda tahmine dayalı analize olanak tanınarak kuruluşların potansiyel siber saldırıları öngörmesi ve bunlara hazırlıklı olmasına imkan sağlanmaktadır. Ayrıca ortaya çıkan eğilimler ve güvenlik açıkları belirlenerek siber güvenlik savunmalarını güçlendirmek için proaktif önlemler alınabilmektedir.

Yapay zeka ve makine öğrenmesi, kuruluşların altyapılarında kapsamlı güvenlik açığı değerlendirmeleri gerçekleştirerek tehdit aktörlerinin yararlanabileceği zayıf noktaları belirlemektedir. Bu bağlamda güvenlik açığı yamalarının önceliklendirilmesine ve kritik varlıkların etkili bir şekilde korumasına olanak sağlamaktadır.

Kurumlar yapay zeka ve makine öğrenmesi tabanlı tehdit analizi platformları yardımıyla siber tehdit istihbaratı süreçlerine katkı sağlayabilmektedir. Günümüzde sektör fark etmeksizin büyük ölçekteki şirketler bu platformlardan yararlanmaktadır. Alanda bir platform üzerinden yapay zeka ve makine öğrenmesi tabanlı tehdit analizi imkanı sağlayan birçok farklı şirket vardır. Bu şirketler sağladıkları platformun içerikleri bakımından birbirinden ayrılabilmektedir. Kurumlar gereklilik, hedef ve şirket boyutlarına bağlı kalarak kendileri için en uygun desteği seçebilirler.

Platformların tabi tutuldukları testler ve siber saldırılara hedef olmuş şirketlere sağladıkları tehdit analizi desteği gösteriyor ki gittikçe askeri hale bürünen siber saldırılar ve tehditler yapay zeka ve makine öğrenmesi tabanlı siber tehdit analizi siber tehdit istihbaratı süreçlerinin geliştirilmesi ve başarı oranının artırılmasına fayda sağlamaktadır.

Özetle siber tehditlerin giderek daha istikrarlı ve gelişmiş bir yapıya evrilmiştir. Bu tehditlere karşı etkili bir şekilde mücadele edebilmek için kurumların, siber tehdit istihbaratını uygun bir şekilde kullanmalı gerekmektedir. Siber tehdit istihbaratı, potansiyel tehditleri belirleme, bunlara karşı hazırlıklı olma ve saldırıları hızlı bir şekilde tespit etmek için gerekli olan bilgileri sağlamaktadır. Yapay zeka ve makine öğrenmesi, siber tehdit istihbaratı için önemli bir teknolojidir. Bu teknolojinin kullanımı, kurumları siber saldırılara karşı daha hazırlıklı yapmaya ve saldırıların etkisini azaltmaya yardımcı olabilmektedir.

Yapay zeka ve alt dalı olan makine öğrenmesi, hızlı analiz özelliği ile problemleri önceden tahmin edip proaktif çözümler üretme, problem çözme, öğrenme ve karar verme gibi görevleri yerine getirebilen sistemler geliştirmeye odaklanmaktadırlar. Bu özellikleri sayesinde yapay zeka ve makine öğrenmesi, siber tehdit istihbaratını daha etkili ve verimli hale getirmede önemli bir rol oynamaktadır. Yapay zeka, makinelerin verilerden öğrenmesini, kalıpları belirlemesini ve anomalileri tanımasını sağlayarak siber güvenlik ortamındaki büyük ilerlemelere imkan sağlamaktadır. Makine öğrenimi algoritmaları, ağ trafiği, kullanıcı davranışı ve sistem günlükleri dahil olmak üzere çok büyük miktarda bilgiyi analiz ederek potansiyel tehditleri tespit edebilmektedir.

Yapay zeka ve makine öğrenmesi destekli siber tehdit analizi platformları, kurumlara gerçek zamanlı tehdit tespiti, otomatik olay müdahalesi, uyarlanabilir savunma mekanizmaları, tahmine dayalı analiz ve kapsamlı güvenlik açığı değerlendirmesi imkanları sunmaktadır. Bu platformların yeterlilikleri ve özellikleri örnek olaylar içerisinde incelenmiştir.

KAYNAKLAR

Bank of England. (2016). *CBEST Intelligence-Led Testing Understanding Cyber Threat Intelligence Operations Version 2.0*. CBEST. Erişim adresi: https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations.pdf

Barikat Siber Güvenlik. (2020). SOC Faaliyet Raporu—Kasım 2020. Barikat Siber Güvenlik. Erişim adresi: https://www.barikat.com.tr/blog/soc-faaliyet-raporu-kasim-2020

BlackBerry Limited. (t.y.). Cylance AI from BlackBerry. Erişim adresi: https://www.blackberry.com/us/en/products/cylance-endpoint-security/cylance-ai

Blake E. Strom, Andy Applebaum, Doug P. Miller, Kathryn C. Nickels, Adam G. Pennington, & Cody B. Thomas. (2020). *MITRE ATT&CKÒ: Design and Philosophy*. MITRE Corporation. Erişim adresi: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153-1176. https://doi.org/10.1109/COMST.2015.2494502

Cezarina Dinu. (2023). Operational Threat Intelligence (OTI): Definition, Lifecycle, Benefits. Heimdal Security Blog. Erişim adresi: https://heimdalsecurity.com/blog/operational-threat-intelligence/

Darktrace Team. (2020). *Darktrace Cyber AI Analyst*. Erişim adresi: https://em360tech.com/sites/default/files/2021-01/Darktrace%20Cyber%20AI%20Analyst.pdf

Development, Concepts and Doctrine Centre, UK Ministry of Defence. (2011). *Joint Doctrine Publication 2-00*. Erişim adresi: https://assets.publishing.service.gov.uk/media/653a4b0780884d0013f71bb0/JDP_2_00_Ed_4_web.pdf

El Naqa, I., & Murphy, M. J. (2015). What Is Machine Learning? Içinde I. El Naqa, R. Li, & M. J. Murphy (Ed.), *Machine Learning in Radiation Oncology* (ss. 3-11). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-18305-3_1

FIRST. (2018). Introduction to CTI as a General topic / Cyber Threat Intelligence SIG Curriculum. FIRST — Forum of Incident Response and Security Teams. Erişim adresi: https://www.first.org/global/sigs/cti/curriculum/cti-introduction

Forcepoint. (2018, Ağustos 11). What is Threat Intelligence? Forcepoint. Erişim adresi: https://www.forcepoint.com/cyber-edu/threat-intelligence

Groce, A. (2016). LibGuides: Intelligence Studies: Dissemination of Intelligence. Erişim adresi: https://usnwc.libguides.com/c.php?g=494120&p=3381610

Harrington, C. (2013). *Sharing Indicators of Compromise: An Overview of Standards and Formats*. Program adı: RSACONFERENCE2013. Erişim adresi: https://docs.huihoo.com/rsaconference/usa-2013/Sharing-Indicators-of-Compromise-An-Overview-of-Standards-and-Formats.pdf

IBM. (t.y.). IBM Security QRadar XDR. Erişim adresi: https://www.ibm.com/products/qradar-xdr

InfoSEC. (2019, Aralık 5). Vectra—InfoSEC. Erişim adresi: https://www.infosec.com.tr/vectra/

Intel&AnalysisWorkingGroup. (2015, Ekim 26). What is Cyber Threat Intelligence? CIS. Erişim adresi: https://www.cisecurity.org/blog/what-is-cyber-threat-intelligence/

Jain, J. (2021). Artificial Intelligence in the Cyber Security Environment. Içinde N. Bhargava, R. Bhargava, P. S. Rathore, & R. Agrawal (Ed.), *Artificial Intelligence and Data Mining Approaches in Security Frameworks* (1. bs, ss. 101-117). Wiley. https://doi.org/10.1002/9781119760429.ch6

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion, 97,* 101804. https://doi.org/10.1016/j.inffus.2023.101804

Kebude, A. (t.y.). *Yapay Zeka*. Ahmet Kebude.

Kurt Baker. (2023, Mart 23). What is Cyber Threat Intelligence? [Beginner's Guide]. Erişim adresi: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/

Lakshmanan, R. (2020). Hackers-For-Hire Group Develops New "PowerPepper" In-Memory Malware. The Hacker News. Erişim adresi: https://thehackernews.com/2020/12/hackers-for-hire-group-develops-new.html

Lee, J., Kim, J., Kim, I., & Han, K. (2019). Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles. *IEEE Access*, *7*, 165607-165626. https://doi.org/10.1109/ACCESS.2019.2953095

Lee, M. (2023). *Cyber threat intelligence*. Oxford, UK ; Hoboken, NJ, USA: Wiley.

Li, J. (2018). Cyber security meets artificial intelligence: A survey. *Frontiers of Information Technology & Electronic Engineering*, *19*(12), 1462-1474. https://doi.org/10.1631/FITEE.1800573

Montasari, R., Carroll, F., Macdonald, S., Jahankhani, H., Hosseinian-Far, A., & Daneshkhah, A. (2021). Application of Artificial Intelligence and Machine Learning in Producing Actionable Cyber Threat Intelligence. Içinde R. Montasari, H. Jahankhani, R. Hill, & S. Parkinson (Ed.), *Digital Forensic Investigation of Internet of Things (IoT) Devices* (ss. 47-64). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-60425-7_3

Oracle Türkiye. (2014). Makine Öğrenimi nedir? Erişim adresi: https://www.oracle.com/tr/artificial-intelligence/machine-learning/what-is-machine-learning/

Rathore, P., Singh, A. K., & García-Díaz, V. (2020). A Holistic Methodology for Improved RFID Network Lifetime by Advanced Cluster Head Selection using Dragonfly Algorithm. *International Journal of Interactive Multimedia and Artificial Intelligence*, *6*(2), 8. https://doi.org/10.9781/ijimai.2020.05.003

Raza, Muhammad. 2023. "What Are TTPs? Tactics, Techniques & Procedures Explained | Splunk". Erişim adresi: https://www.splunk.com/en_us/blog/learn/ttp-tactics-techniques-procedures.html

Recorded Future. (2020). What Is Threat Intelligence? | Recorded Future. Erişim adresi: https://www.recordedfuture.com/blog/threat-intelligence

SparkCognition. (2020). SparkCognition's DeepArmor® Cybersecurity Product Detects PowerPepper Malware. Erişim adresi: https://www.prnewswire.com/news-releases/sparkcognitions-deeparmor-cybersecurity-product-detects-powerpepper-malware-301188352.html

SparkCognition Inc. (2018). Deeparmor-platform-architecture.pdf. Erişim adresi: https://www.sparkcognition.com/wp-content/uploads/2019/12/deeparmor-platform-architecture.pdf

Trend Micro Incorporated. (2023). Indicators of compromise—Definition. Erişim adresi: https://www.trendmicro.com/vinfo/us/security/definition/indicators-of-compromise

Tuma, K., Calikli, G., & Scandariato, R. (2018). Threat analysis of software systems: A systematic literature review. *Journal of Systems and Software*, *144*, 275-294. https://doi.org/10.1016/j.jss.2018.06.073

Vectra. (2023). Ricoh Co. Ltd. Achieves real-time monitoring of 100,000 units to detect threats in advance. Erişim adresi: https://www.vectra.ai/resources/customer-stories/ricoh

Zeng, Y. (2022). AI Empowers Security Threats and Strategies for Cyber Attacks. *Procedia Computer Science*, *208*, 170-175. https://doi.org/10.1016/j.procs.2022.10.025