

Siber Savunmada Yapay Zeka: Güncel Uygulamalar ve Teknolojiler

Ahsen Beyza Özkul

1) Tehdit Tespiti ve Olay Yanıtı'nda Yapay Zeka

- **Twitter'in Anomali Tespit Aracı** Twitter, veri üzerinde alışılmadık desenleri tespit etmek için bir araç geliştirdi. Bu araç, ağ trafiği ve kullanıcı aktiviteleri gibi şeyleri gerçek zamanlı olarak izler ve makine öğrenimi kullanarak garip davranışları hızlıca tespit eder ve uyarı verir.

twitter/ AnomalyDetection



Anomaly Detection with R



9

Contributors



62

Issues



4k

Stars



777

Forks



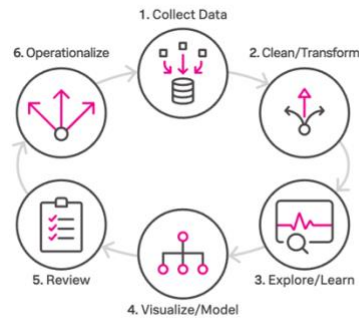
- **Splunk'ın Makine Öğrenimi Araç Seti** Splunk, sistem günlükleri ve operasyonlarda anomali tespiti için makine öğrenimi kullanan bir dizi araç sunar. Bu araçlar, IT dünyasında genellikle alışılmadık aktiviteleri belirleyip büyük sorunlara dönüşmeden önce uyarı gönderir.

Splunk Machine Learning Toolkit (MLTK)

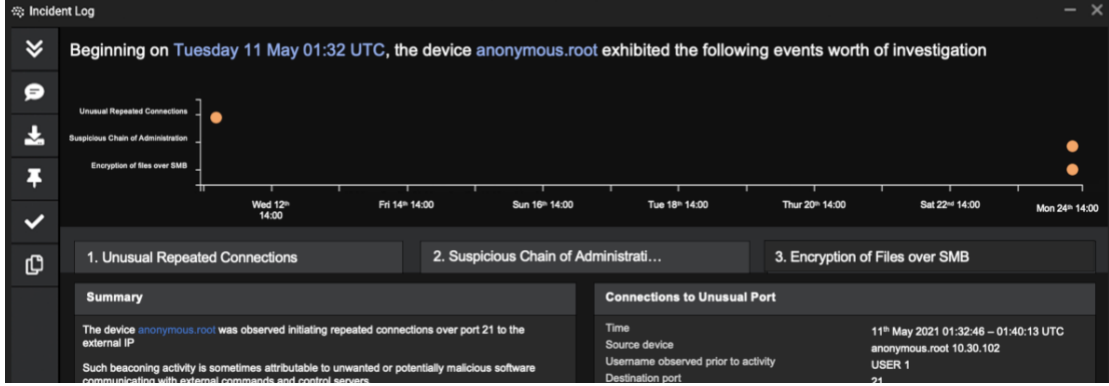
The MLTK is available to all Splunk Cloud or Splunk Enterprise customers and extends the value of the Splunk platform by enabling users to easily apply machine learning to their data.

- **Guide investigations** by using machine learning to discover hidden meaningful patterns in your data
- **Investigate** your expanding data universe and avoid costly downtime
- **Analyze and monitor** at machine speed with purpose-built machine learning algorithms
- **Automate** action with trained models for alerts in real time

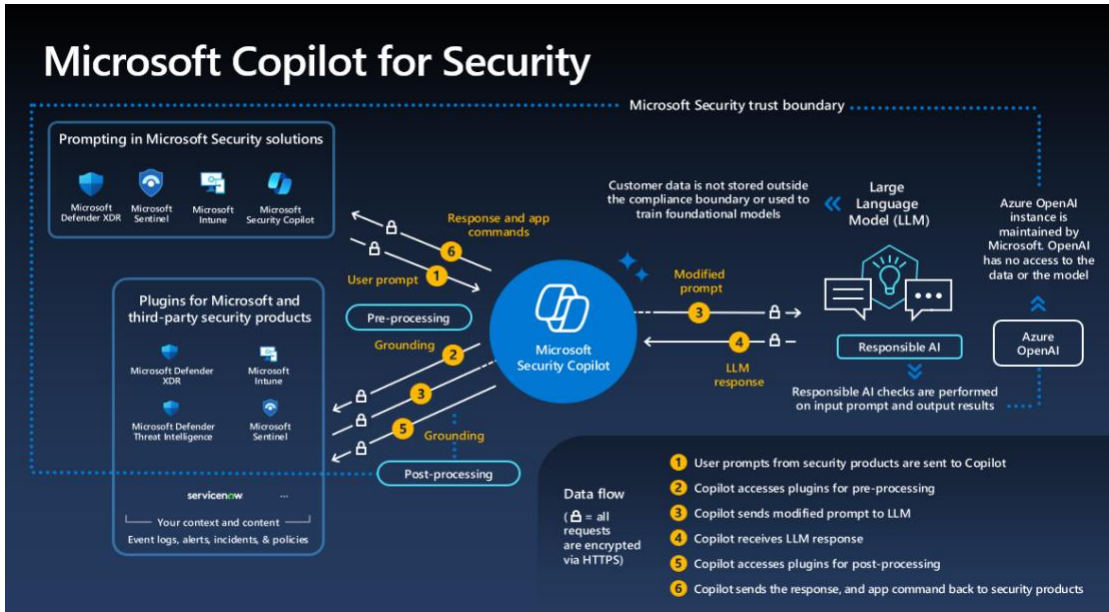
Machine Learning Process



- **Darktrace AI ile Olay Yanıtı** Darktrace, siber tehditlere otomatik olarak yanıt veren bir yapay zeka kullanır. Bir saldırı gerçekleştiğinde, Darktrace etkilenmiş sistem parçalarını izole eder, böylece güvenlik ekibiniz sorunun yayılmaması için odaklanabilir ve sorunu çözmeye yönelik çalışabilir.



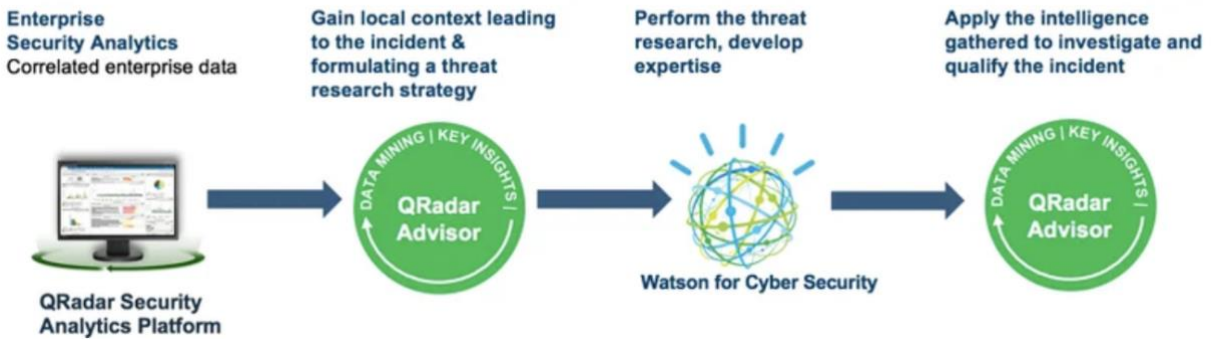
- **Microsoft Security Copilot ile Olay Yanıtı** Microsoft Security Copilot, siber saldırılarla başa çıkma sürecini otomatikleştirir. Olaylara hızlıca yanıt verebilir, problemi izole edebilir, gerekli bilgileri sağlayabilir ve sistemleri normale döndürebilir. Bu, güvenlik ekiplerinin zaman ve enerjisini korur.
- **Microsoft Security Copilot** Microsoft Security Copilot, ağı sürekli tarayarak alışılmadık aktiviteleri ve potansiyel tehditleri tespit eden bir yapay zeka aracıdır. Bu sayede şirketlerin verilerini korumak daha kolay hale gelir, insan gözetimine olan bağımlılık azalır.



- **SentinelOne'in Singularity Platformu** SentinelOne'in Singularity platformu, güvenlik ekiplerinin tüm ağda tehditleri aramasına yardımcı olur. Sistemdeki tüm verileri bir araya getirir ve tehditleri hızlıca bulup çözmeye yönelik net bir görünüm sağlar.



- **IBM QRadar ve Watson ile Siber Güvenlik** IBM QRadar güvenlik sistemi, Watson'ın yapay zekasını kullanarak güvenlik verilerini otomatik olarak analiz eder. Bu sayede güvenlik ekipleri potansiyel tehditleri hızlıca tespit edip yanıt verebilir, zaman ve çaba tasarrufu sağlar.

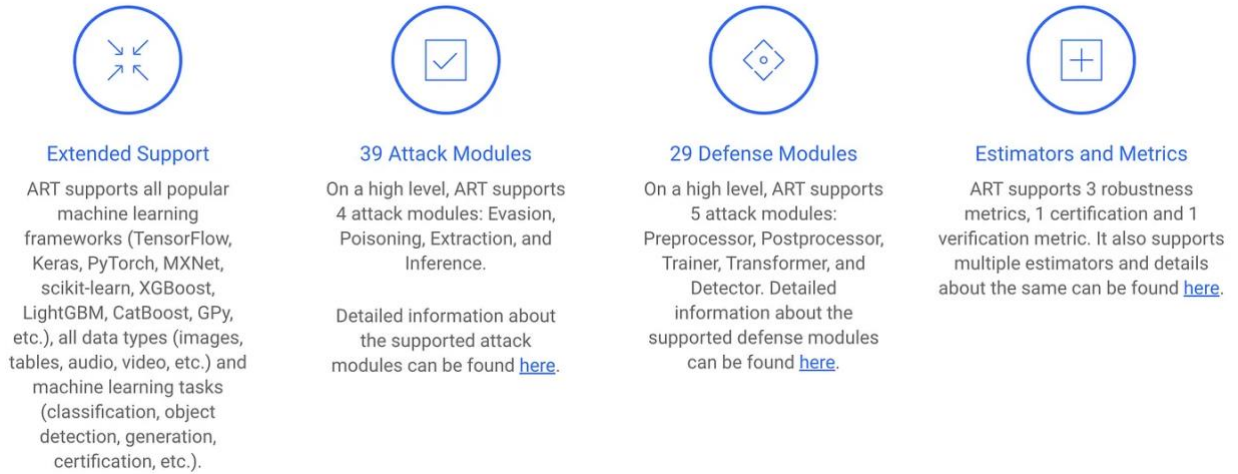


- **AWS GuardDuty** AWS GuardDuty, AWS hizmetlerinden gelen verileri izleyip analiz eder, alışılmadık aktiviteleri tespit eder. Anormal API çağrıları veya yetkisiz erişim girişimleri gibi potansiyel güvenlik ihlallerini belirler, tehdit tespitini geliştirir.



2) Güvenlik Açığı Yönetimi ve Güvenlik Artırımı'nda Yapay Zeka

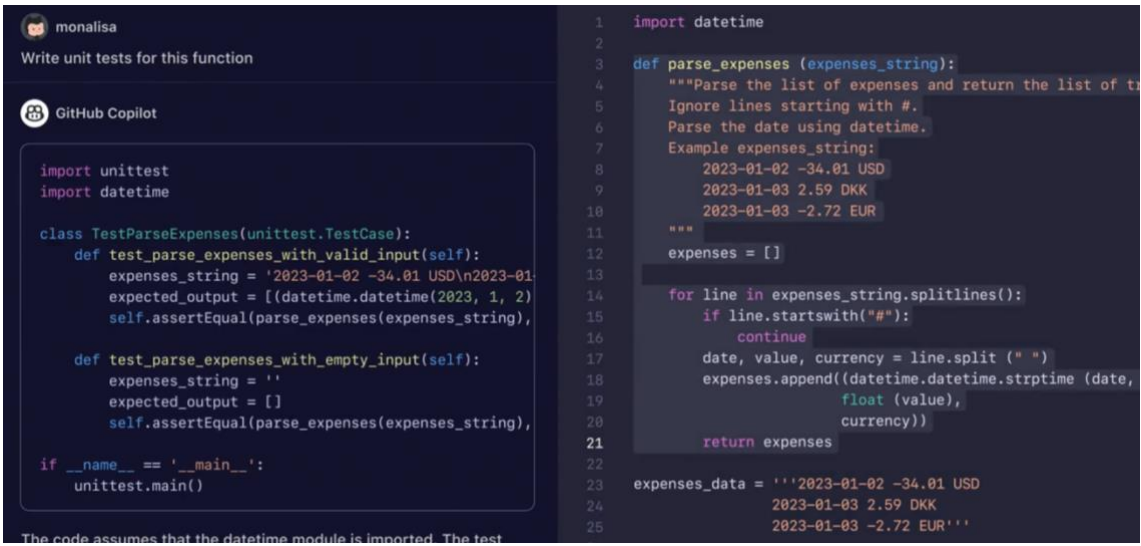
- **IBM Adversarial Robustness Toolbox (ART)** IBM'in ART, AI sistemlerini saldırılardan korumak için tasarlanmış bir araç kitidir. Veri zehirlenmesi veya AI zayıflıklarını hedef alan siber saldırılara karşı savunma sağlar.



- **TensorFlow Privacy** TensorFlow Privacy, TensorFlow platformunun bir uzantısıdır ve AI modellerinin gizlilik korumalarıyla eğitilmesini sağlar. Bu, AI sistemlerinin saldırırganlar tarafından sömürülebilir veya manipüle edilebilir olmasını azaltır.
- **OWASP ZAP ve Makine Öğrenimi** OWASP ZAP, web uygulamalarında güvenlik açıklarını test eden bir araçtır. Makine öğrenimi eklenerek, SQL enjeksiyonları

veya çapraz site betikleme (XSS) gibi sorunları otomatikleştirerek bulma konusunda daha etkili hale gelir.

- **HackerOne ve AI Destekli Tarama** HackerOne, güvenlik araştırmacılarının yazılım hatalarını bulduğu bir platformdur. AI kullanarak güvenlik açıklarını bulma sürecini otomatikleştirir, uygulamalardaki zayıflıkları daha hızlı ve kolay bir şekilde keşfeder.
- **GitHub Copilot ve CodeQL** GitHub Copilot, geliştiricilere kod yazmada yardımcı olan bir AI aracıdır. CodeQL ile kullanıldığında, yazılan kodda güvenlik sorunlarını da tarar, sorunları erken aşamada yakalayarak büyük problemlere dönüşmelerini önler.



The screenshot shows the GitHub Copilot interface. On the left, a prompt says "Write unit tests for this function". Below it, the GitHub Copilot logo is visible. The main area displays Python code for unit tests. The code imports unittest and datetime, then defines a class TestParseExpenses with two test methods: test_parse_expenses_with_valid_input and test_parse_expenses_with_empty_input. The valid input test uses a string with three expense entries. The empty input test uses an empty string. The code also includes a main block to run the tests. On the right, the function being tested is shown: parse_expenses, which takes a string of expense entries and returns a list of tuples containing the date, value, and currency. The function uses datetime.strptime to parse the date and float to parse the value.

```
import unittest
import datetime

class TestParseExpenses(unittest.TestCase):
    def test_parse_expenses_with_valid_input(self):
        expenses_string = '2023-01-02 -34.01 USD\n2023-01-03 2.59 DKK\n2023-01-03 -2.72 EUR'
        expected_output = [(datetime.datetime(2023, 1, 2), -34.01, 'USD'), (datetime.datetime(2023, 1, 3), 2.59, 'DKK'), (datetime.datetime(2023, 1, 3), -2.72, 'EUR')]
        self.assertEqual(parse_expenses(expenses_string), expected_output)

    def test_parse_expenses_with_empty_input(self):
        expenses_string = ''
        expected_output = []
        self.assertEqual(parse_expenses(expenses_string), expected_output)

if __name__ == '__main__':
    unittest.main()
```

```
import datetime

def parse_expenses (expenses_string):
    """Parse the list of expenses and return the list of tuples.
    Ignore lines starting with #.
    Parse the date using datetime.
    Example expenses_string:
    2023-01-02 -34.01 USD
    2023-01-03 2.59 DKK
    2023-01-03 -2.72 EUR
    """
    expenses = []

    for line in expenses_string.splitlines():
        if line.startswith("#"):
            continue
        date, value, currency = line.split(" ")
        expenses.append((datetime.datetime.strptime (date, "%Y-%m-%d"), float (value), currency))

    return expenses

expenses_data = '''2023-01-02 -34.01 USD
2023-01-03 2.59 DKK
2023-01-03 -2.72 EUR'''
```

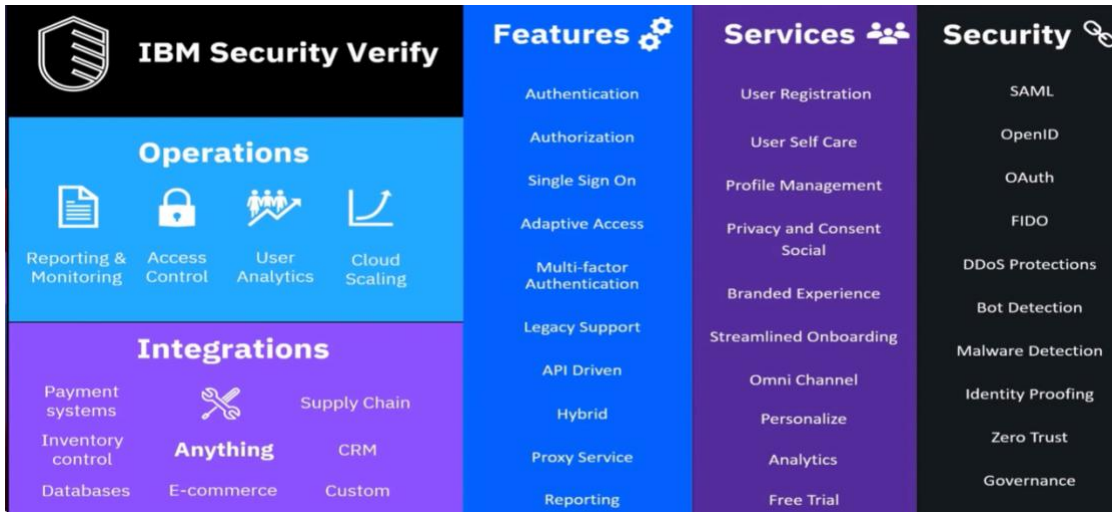
- **SonarQube ve AI Eklentileri** SonarQube, kod kalitesi ve güvenliğini kontrol eden bir araçtır. AI eklentileri ile, güvenlik açıklarını bulmada daha etkili olur ve yanlış alarm sayısını azaltır, böylece geliştiricilerin gerçek sorunları daha kolay çözmelerini sağlar.
- **IBM Guardium ve Yaman Yönetimi** IBM Guardium, verilerinizi güvence altına almak için AI kullanır, hem yerel hem de bulut ortamlarında güvenlik açıklarını bulur ve düzeltir. Yeni tehditlere uyum sağlar ve verilerinizi korumak için gerekli yamaları zamanında uygular.
- **Tenable'in Exposure AI** Tenable'in Exposure AI, sisteminizdeki zayıf noktaları tespit eder ve bunları hackerlar tarafından kullanılmadan önce düzeltir. AI kullanarak, zayıflıkları tarar, hangi açıkların daha kritik olduğunu önceliklendirir ve hızlıca yamalar, sisteminizin daha güvenli olmasını sağlar.



- **Zscaler Veri Koruma** Zscaler Veri Koruma, hassas bilgileri korumak için AI kullanır, belgeleri, e-postaları ve görüntüleri tarar. Verileri sınıflandırır, yetkisiz erişimleri tespit eder ve veri ihlallerini önler, hassas bilgilerinizi yönetmeyi ve korumayı kolaylaştırır.

Kimlik ve Erişim Yönetimi'nde Yapay Zeka

- **IBM Verify** IBM Verify, kimlik ve erişim yönetimini geliştirmek için AI kullanır, kullanıcı davranışlarını analiz eder ve kimlik doğrulama gereksinimlerini ayarlar. Anomalileri tespit edebilir ve otomatik olarak çok faktörlü kimlik doğrulama uygular, güvenliği artırırken kullanıcı erişim yönetimini basitleştirir.



Kaynaklar

- IBM. (t.y.). *Tehdit tespiti ve yanıt*. Erişim adresi: <https://www.ibm.com/services/threat-detection-response>
- IBM. (t.y.). *Guardium*. Erişim adresi: <https://www.ibm.com/guardium>
- IBM. (t.y.). *Watsonx yönetimi*. Erişim adresi: <https://www.ibm.com/products/watsonx-governance>
- Watkins, O. (2024, 19 Nisan). *Siber güvenlikte AI kullanımı için 4 vaka*. Red Hat. Erişim adresi: <https://www.redhat.com/en/blog/4-use-cases-ai-cyber-security>
- Goss, A. (2024, 13 Mayıs). *Siber güvenlikte AI örnekleri*. Station X. Erişim adresi: <https://www.station.net/examples-of-ai-in-cyber-security/>
- Shutenko, V. (2024, 8 Ağustos). *Siber güvenlikte AI*. TechMagic. Erişim adresi: <https://www.techmagic.co/blog/ai-in-cybersecurity/>
- (t.y.). *Siber güvenlik projelerinde yapay zeka*. Network Simulation Tools. Erişim adresi: <https://networksimulationtools.com/artificial-intelligence-in-cyber-security-projects/>
- Daivi. (2024, 19 Mart). *Siber güvenlik makine öğrenimi projeleri*. ProjectPro. Erişim adresi: <https://www.projectpro.io/article/cybersecurity-machine-learning-projects/631>
- Caniszczyk. (t.y.). *AnomalyDetection*. GitHub. Erişim adresi: <https://github.com/twitter/AnomalyDetection>
- Fier, J., & Kenyon Grant, S. (t.y.). *Splunk makine öğrenimi aracı*. Splunk. Erişim adresi: https://www.splunk.com/en_us/resources/splunk-machine-learning-toolkit.html
- Darktrace. (2022, 12 Nisan). *Darktrace'in Siber AI Analisti, ABD federal hükümetine olay raporlamalarını nasıl hızlandırır*. Erişim adresi: <https://darktrace.com/blog/how-darktraces-cyber-ai-analyst-accelerates-reporting-incidents-to-the-us-federal-government>
- Microsoft. (2024, 18 Temmuz). *Microsoft güvenlik yardımcı pilotu*. Erişim adresi: <https://learn.microsoft.com/en-us/copilot/security/microsoft-security-copilot>
- (t.y.). *Singularity platformu*. Kidan. Erişim adresi: <https://kidan.co/partners/singularity-platform/>
- (t.y.). *IBM'in QRadar danışmanı ile Watson'un çalışma aşamaları*. ResearchGate. Erişim adresi: https://www.researchgate.net/figure/Stages-involved-in-the-working-of-IBMs-QRadar-advisor-with-Watson-64_fig3_373712758
- Amazon Web Services. (t.y.). *Amazon GuardDuty artık Amazon EKS çalışma zamanı izlemeyi destekliyor*. Erişim adresi: <https://aws.amazon.com/tr/blogs/aws/amazon-guardduty-now-supports-amazon-eks-runtime-monitoring/>
- Hajra, A. (2023, 4 Mayıs). *IBM ART karşıt saldırganlık testi bir film öneri sistemi için*. Medium. Erişim adresi: <https://medium.com/@asmitahajra/ibm-art-adversarial-robustness-check-for-a-movie-recommendation-system-649ba46e9e8a>
- (t.y.). *Copilot*. GitHub. Erişim adresi: <https://github.com/features/copilot>
- (t.y.). *Maruziyet yönetimi: Tenable One nedir?* E-SPIN. Erişim adresi: <https://www.e-spincorp.com/exposure-management-what-is-tenable-one/>

- (t.y.). *IBM Verify incelemeleri*. TrustRadius. Eriřim adresi:
<https://www.trustradius.com/products/ibm-verify/reviews?qs=pros-and-cons#comparisons>