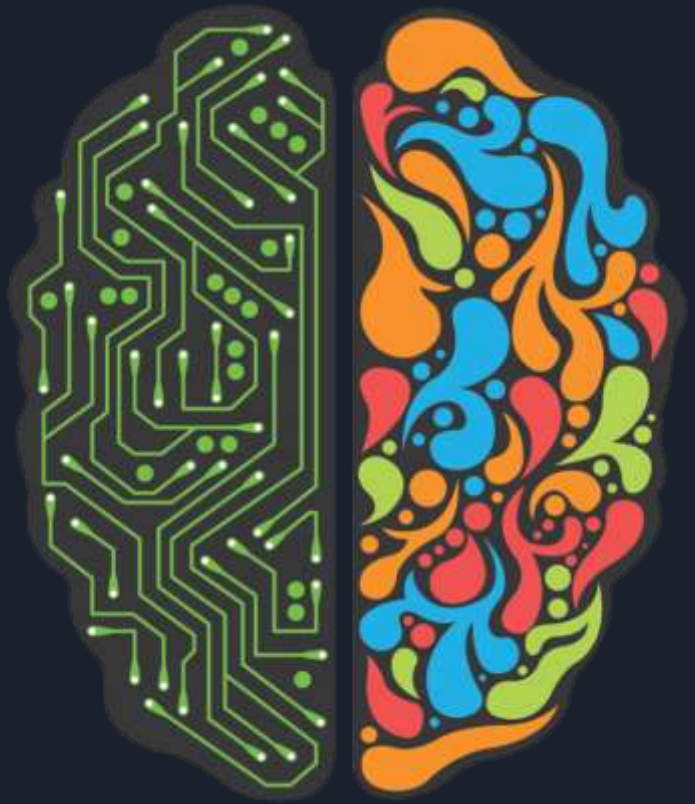
GRUP-1

Ağ Güvenliğinde Yapay Zeka Uygulamaları

Grup #1

Yapay Zeka Nedir?

Yapay zeka, en basit şekilde belirli görevleri yerine getirmek için insan zekasını taklit eden ve topladıkları bilgileri yineleyerek kendilerini geliştirebilen sistemler olarak tanımlanır.



Yapay Zeka Ve Siber Güvenlik

Günümüzde hızla gelişen siber saldırılar ve cihazların hızla çoğalmasıyla yapay zeka ve makine öğrenimi, siber suçluları takip etmeye, tehdit tespitini otomatikleştirmeye ve geleneksel yazılım odaklı tekniklerden daha etkili yanıt vermeye yardımcı olabilir.

Grup #1

Tehdit Tespiti Ve Analizi

- Davranışsal Analiz
- Gelişmiş Tehdit İstihbaratı
- Otomatik Tehdit Yanıtı

Yapay Zekanın Siber Güvenliğe Faydaları

- Verimlilik
- Maliyet
- Gerçek Zamanlı Tehdit algılama ve hızlı yanıt verebilme
- Bilinmeyen tehditleri tespit edebilme

Grup #1

Saldırılara Karşı Güvenceye Alınan Makine Öğrenimi

Makine Öğrenimi Nedir ?

Makine öğrenimi, yapay zeka alanında büyük bir ilerleme kaydeden bir disiplindir. Veri analizi, tahminleme ve desen tanıma gibi birçok alanda kullanılır.

Saldırılara Karşı Güvenceye Alınan Makine Öğrenimi Nedir?

Saldırılara karşı güvenceye alınan makine öğrenimi, makine öğrenimi modellerini saldırılara karşı korumak ve güçlendirmek için kullanılan bir dizi teknik ve yöntemleri içerir.

Grup #1

GRUP-1

Saldırı Türleri ve Saldırılara Karşı Güvenceye Alınan Teknikler

Saldırı Türleri:

1. Zehirleme Saldırıları
2. Yanıltıcı Saldırılar
3. Saldırıya Karşı Transfer

Saldırılara Karşı Alınan Teknikler

1. Savunma Öğrenimi
2. Saldırı Tespit Sistemleri
3. Saldırıların Hafifletilmesi
4. Veri Ön İşleme

Grup #1

GRUP-1

Yapay Zeka Tabanlı Sızma Tespit Sistemleri

Yapay zeka tabanlı sızma tespit sistemleri (YZT STS), günümüzün karmaşık siber tehditlerine karşı korunmak için yaygın olarak kullanılan gelişmiş güvenlik önlemlerinden biridir. Bu sistemler, bilgisayar ağlarında gerçekleşen potansiyel saldırıları tespit etmek ve önlemek amacıyla yapay zeka tekniklerini kullanır.

Yapay zeka tabanlı sızma tespit sistemleri şu maddeleri içerir;

1. Veri Toplama ve İzleme
2. Veri Analizi
3. Anormallik Tespiti
4. Tehdit Tespiti
5. Uyarı ve İnceleme

Grup #1

Avantajları ve Bazı Sınırlamaları

Yapay zeka tabanlı sızma tespit sistemlerinin avantajları;

1. Saldırıların hızlı tespiti
2. Ölçeklenebilirlik
3. Öğrenme yeteneği

YZT STS bazı zorlukları ve sınırlamaları;

1. Yanlış pozitifler
2. Gelişmiş saldırı teknikleri
3. Gizlilik endişeleri

Yapay Zeka Destekli Ağ Güvenlik Duvarları

Güvenlik duvarı, yapay zeka ve makine öğrenme tekniklerini kullanarak ağ uygulamalarını korumak için gelişmiş güvenlik önleme sistemleridir. Yapay zeka sayesinde, ağımızdaki tehditleri daha hızlı ve etkili bir şekilde tespit edebilir, anormal aktiviteleri önleyebilir ve sıfır günlük saldırılara karşı koruma sağlayabiliriz.

Yaygın kullanılan güvenlik duvarları

- Saldırı İmza Tabanlı Güvenlik Duvarları
- Davranış Tabanlı Güvenlik Duvarları
- Makine Öğrenimi Tabanlı Güvenlik Duvarları
- Derin Öğrenme Tabanlı Güvenlik Duvarları
- Akıllı İstemci Tabanlı Güvenlik Duvarları

Ayrıca yapay zeka destekli ağ güvenlik duvarları gelişmiş veri analitiği ve davranış analizi kullanarak, saldırıları gerçek zamanlı olarak tespit edebilir ve hızlı tepki vermeyi sağlar.

Otomatik Saldırı Savunma Sistemleri

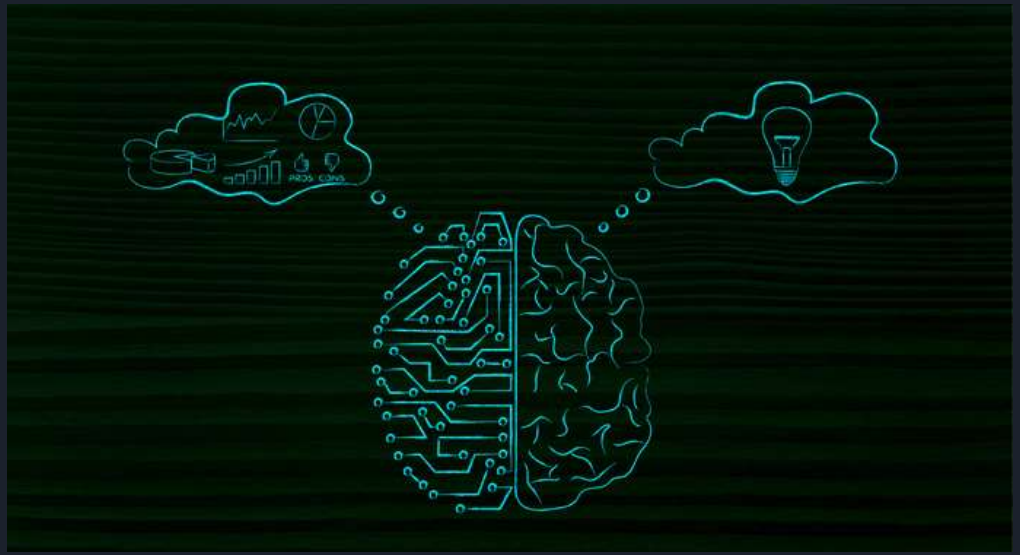
Otomatik saldırı savunma sistemleri bilgisayar ağlarını ve sistemlerini saldırılara karşı korumak ve saldırıları otomatik olarak tespit edip önlemek için kullanılır.

Otomatik Saldırı Savunma Sistemlerinin Günümüzde Kullanım Alanları

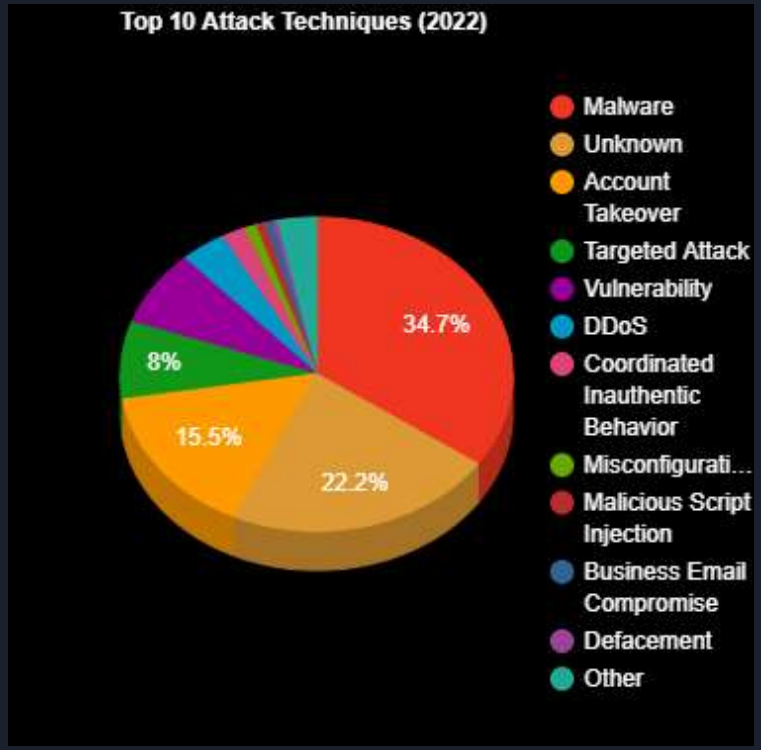
- Bilgi Teknolojileri Güvenliği
- Endüstriyel Kontrol Sistemleri
- Savunma ve Güvenlik
- Otomotiv Sektörü
- Akıllı Şehirler

Yapay Zeka ve Ağ Davranış Analizi (NBA)

Ağ davranış analizi, kötü amaçlı etkinlik gösterebilecek olağandışı varlıkları belirlemek için kurumsal ağ verilerini toplama ve analiz etme işlemdir.

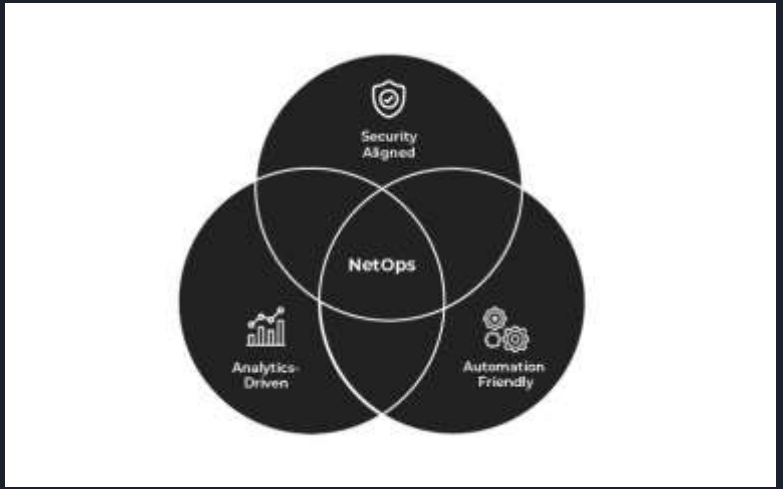


Neden İhtiyaç Duyuluyor ?



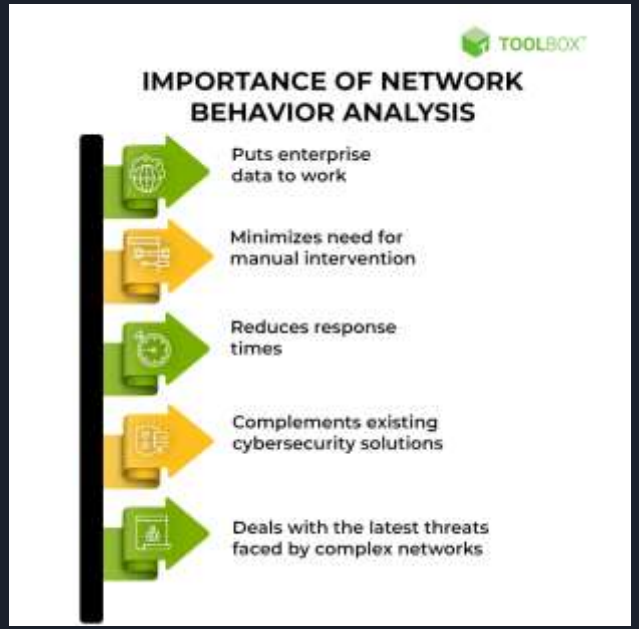
Ağ Davranış Analizinin Özellikleri

- Ağ Görünürlüğü
- Ağ Davranışı Algılama
- Tehdit Tanımlama ve Azaltma



Önemi Nedir ?

- Tahmini yıllık 10,5 trilyon dolar siber suç hasarı.
- Kurumlarda güvenlik ihtiyacı.
- Manuel müdahaleyi en aza indirme.
- Yanıt süresinin azaltılması.
- Mevcut siber güvenlik çözümlemelerini tamamlaması.
- Karmaşık ağların karşılaştığı son nesil tehditleri anlaması.

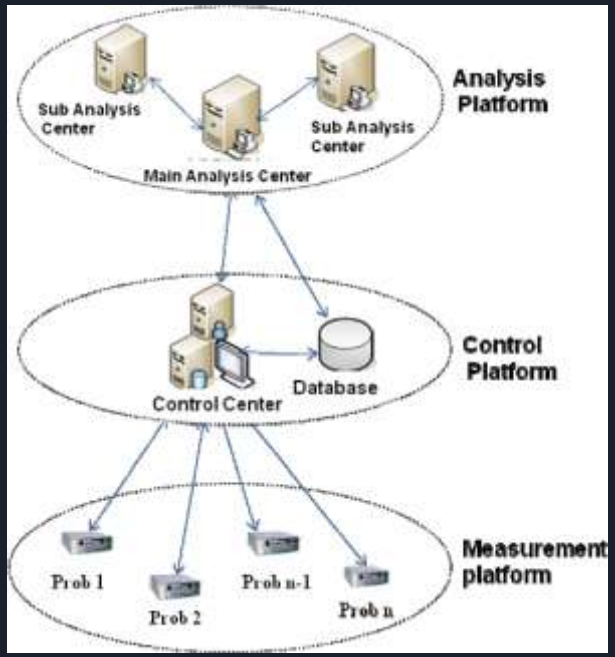


Grup #1

NBA Nasıl Çalışır ?

Kaynak ve Hedef Adresler

- Kaynak ve Hedef TCP, UDP Portları
- ICMP tipi kodları
- Paket Boyutu
- Her Akıştaki SYN ve ACK paketlerinin miktarı



GRUP-1

YAPAY ZEKA TABANLI SİBER İSTİHBARAT

Yapay Zeka Destekli Tehdit İstihbaratı (YDTİ), tehdit istihbaratının toplanması, analizi ve değerlendirilmesinde yapay zeka (YZ) teknolojilerinin kullanılması anlamına gelir. YDTİ, güvenlik alanında birçok farklı sektörde, özellikle siber güvenlik, terörle mücadele ve suçla mücadele gibi alanlarda kullanılan bir yöntemdir.

YDTİ'nin amacı, büyük veri kaynaklarından elde edilen bilgileri otomatik olarak işleyerek, tehditleri önceden tanımlamak, analiz etmek ve değerlendirmek için bilgi sağlamaktır.

YDTİ, güvenlik ekiplerine hızlı ve etkili bir şekilde tehditlerle ilgili bilgi sağlamak için kullanılır.

YDTİ aynı zamanda tehdit istihbaratında analistlere yardımcı olabilir. Analistler, büyük miktarda veriyi elle işlemek yerine, yapay zeka algoritmalarını kullanarak hızlı bir şekilde önemli bilgileri belirleyebilirler.

Grup #1

SİBER TEHDİT İSTİHBARATINDA HANGİ ÖZELLİKLER BULUNMALIDIR ?

- Özel Tehdit Yöntemleri
- Tehdit Verileri
- Raporlara erişim imkanı
- Çözüm İmkanı

Grup #1

GÜVENLİK AÇIĞI TESPİTİ NEDİR ?

Güvenlik açığı yönetimi, güvenlik açıklarını ve yanlış yapılandırmaları keşfetmeye, önceliklendirmeye ve düzeltmeye yönelik risk tabanlı bir yaklaşımdır.

Güvenlik açığı yönetimi, bilgisayar sistemlerinizi, ağlarınızı ve kurumsal uygulamalarınızı siber saldırılardan ve veri ihlallerinden koruyan sürekli, proaktif ve genellikle otomatikleştirilmiş bir süreçtir. Bu nedenle de genel bir güvenlik programının önemli bir parçasıdır. Kurumlar, olası güvenlik zayıflıklarını belirleyerek, değerlendirerek ve ele alarak saldırıların önlenmesine ve meydana gelmesi durumunda hasarı en aza indirmeye yardımcı olabilir.

GÜVENLİK AÇIĞI YÖNTEMLERİ AVANTAJLARI

- **Gelişmiş güvenlik ve denetim**
- **Görünürlük ve raporlama**
- **Operasyon verimlilikleri**

GRUP-1

GÜVENLİK AÇIKLARINI YÖNETMEK

Bir güvenlik açığı yönetimi programınız olduğunda, bilinen ve olası güvenlik açıklarının yanı sıra yanlış yapılandırmaları yönetmek için dört temel adım vardır.

1. **Güvenlik açıklarını belirleyin**

1. **Güvenlik açıklarını değerlendirin**

1. **Güvenlik açıklarını ele alın**

1. **Güvenlik açıklarını raporlayın**

Grup #1

Saldırı tespiti ve önleme

Bir bilgisayar korsanı sistemimize girmeye çalıştığında bu bir saldırı olarak tanımlanır ve ağ saldırı tespit sistemleri bu tür müdahaleleri tespit eden bir sistemdir. NIDS, bir ağ üzerindeki paketleri gözetir, farklı kötü amaçlı etkinlik işaretlerini izlemek için ağ trafiğini analiz eder. Bu sistemin temel amacı, bilgisayar korsanının sistemimize girip girmediğini tespit etmektir.
Bir ağ saldırı tespit sisteminin temel işlevleri şunları içerir:

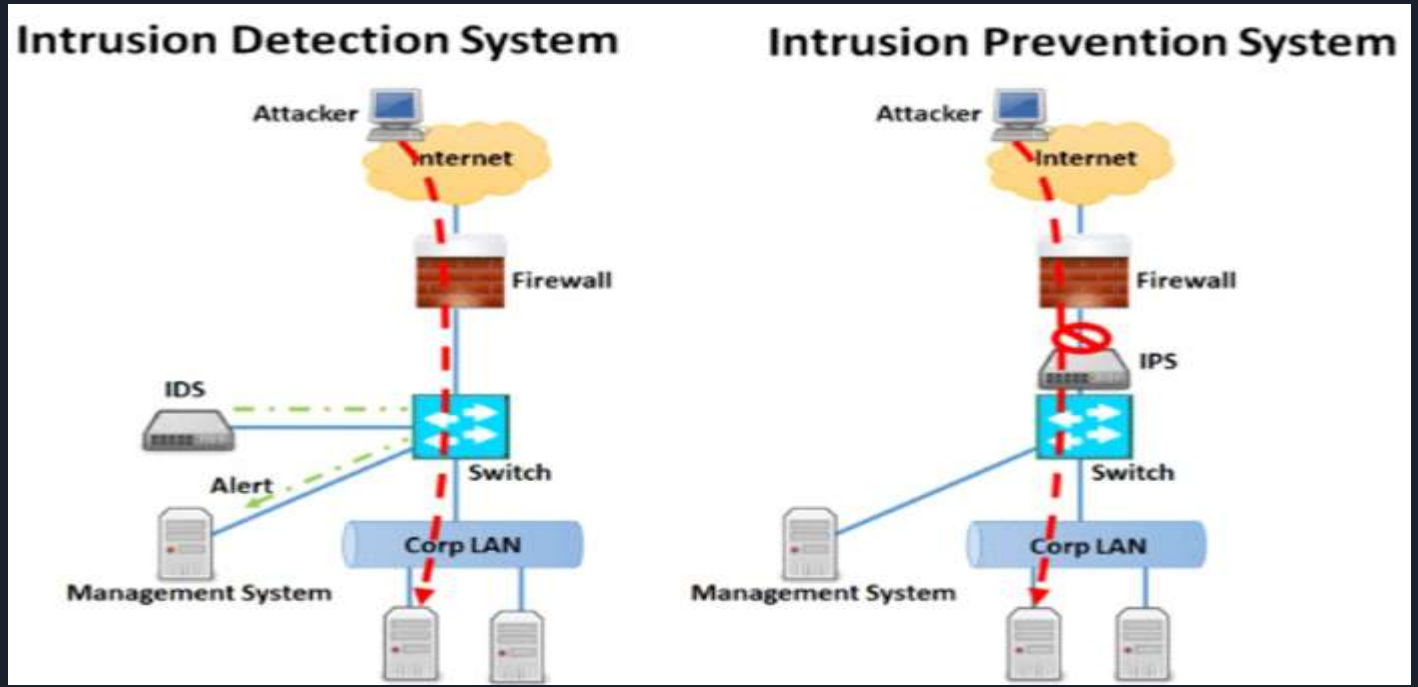
Saldırı tespiti: Gerçek zamanlı ağ izlemesi yaparak gerçekleştiği andan itibaren güvenlik tehditlerini ve saldırıları tespit eder.

Saldırı bilgisi: Eğer bu sistem bir saldırı tespit ederse saldırı hakkında bilgi verir.

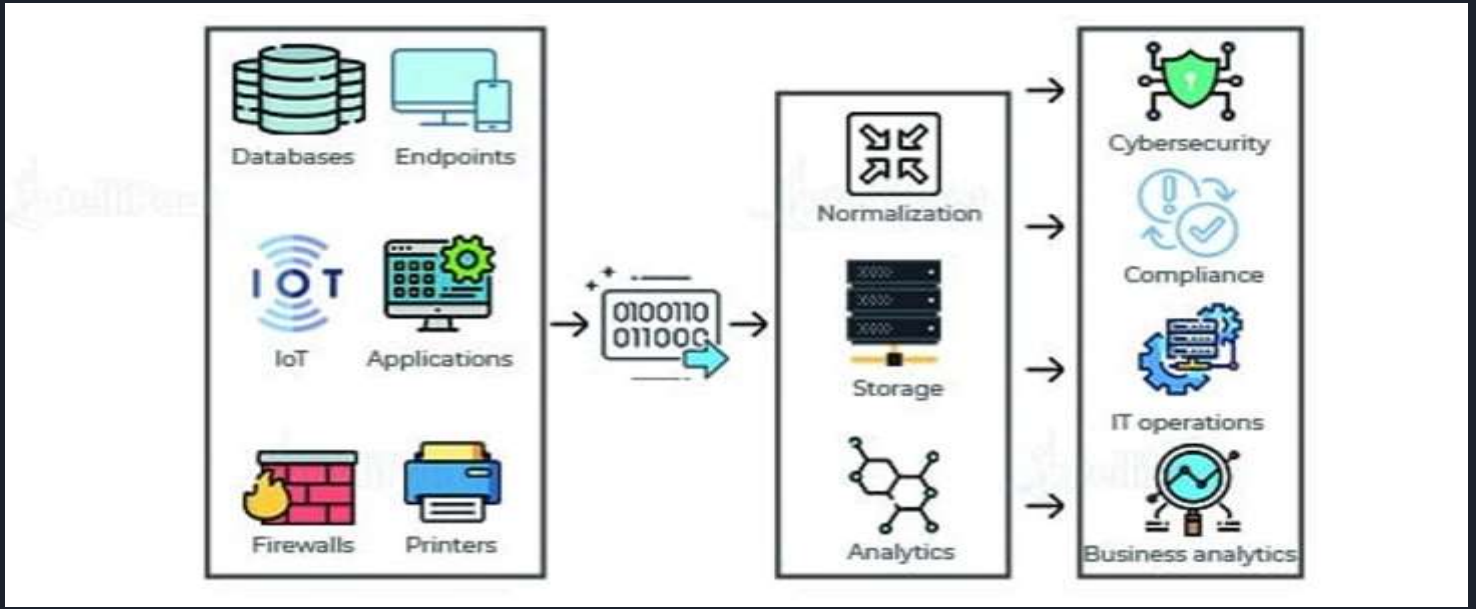
Düzeltici adımlar: Sistem tarafından bir saldırı tespit edildiğinde, aktif sistemler saldırıyı çözmek için önlemler alırlar.

Depolama: Olayları yerel olarak ya da saldırı olması durumunda da depolar.

Saldırı tespit sistemleri



SIEM çalışma mantığı



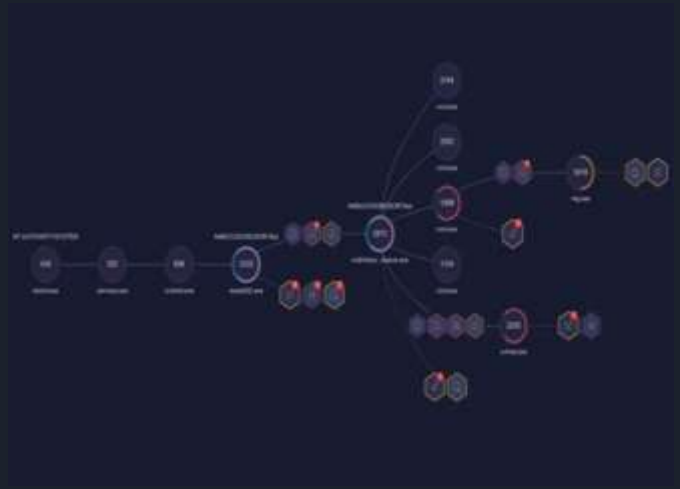
Defplorex

TrendMicro tarafından DefPloreX, büyük ölçekli siber suç adli tıp için kullanılan AI destekli bir makine öğrenme araç takımıdır. Adı ” Defacement eXplorer ” üzerinde bir kelime oyunudur ve milyonlarca tahrif edilmiş web sayfasını analiz etmek için açık kaynaklı kütüphanelere dayanmaktadır. Bu güvenlik yazılımı, meta veri kayıtları içeren dosyaları analiz eder, kaynaklarına erişmek için başsız tarayıcılar kullanır, tahrif edilmiş web sayfalarından veri alır ve sonuçları Elastik bir dizinde saklar. Elastik Arama, diğer sistemlere kolay entegrasyon ile verilere izin verir.

Grup #1

IBM Q-RADAR

IBM’in QRadar Danışmanı, şirketin kârlılığını korurken tehditleri daha hızlı düzeltmek için AI kullanan bir siber güvenlik yazılımıdır. QRadar SIEM, gizli saldırganları yakalamaya yardımcı olmak ve ciddi tehditlerin ve güvenlik açıklarının işletmelerin faaliyetlerini aksatmasını önlemek için yüksek sadakat uyarılarına öncelik vermektedir.

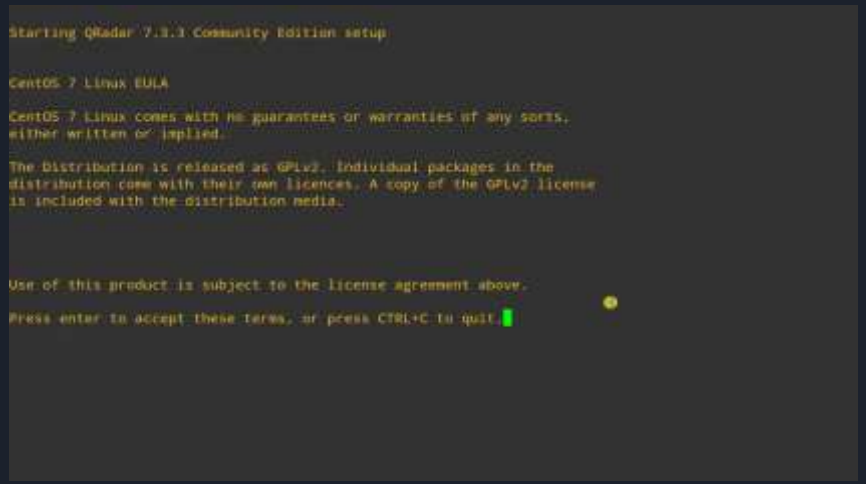


Grup #1

Tenable.io

Bulut tabanlı bir çözüm olarak sunulan Tenable.io, en geniş güvenlik açığı kapsama alanına, hızlı analiz için sezgisel dashboard görselleştirmelerine ve verimliliği en üst düzeye çıkarmanıza ve verimliliği artırmanıza yardımcı olan bir yapay zeka aracıdır.

IBM-QRadar nasıl kullanılır ?



Yapay Zeka ve Kimlik Doğrulaması

Kimlik doğrulama ve yetkilendirme süreçlerinde kullanıldığında güvenlik önlemleri artabilir. Ancak yapay zekanın kullanımıyla ilgili etik ve gizlilik konuları dikkate alınmalıdır. Kullanıcıların bu bilgilerinin doğru şekilde korunacağından emin olmak için uygun önlemler alınmalıdır.

Yapay Zeka ve Kimlik Doğrulaması

- Biyometrik Kimlik Doğrulaması
- Davranış Analizi
- Ses Analizi
- Doğal Dil İşleme
- Anomali Tespiti