TURK TELEKOM SİBER GÜVENLİK KAMPI

GRUP ÇALIŞMASI

KULLANICI DAVRANIŞ ANALİTİĞİ

(USER BEHAVIORAL ANALYTICS)

HAZIRLAYANLAR

Faruk ULUTAŞ

Nazife İNANÇ

Ensar EMEKLİ

İçindekiler

Kullanıcı Davranışı Analitiği (UEBA)

Kullanıcı Davranış Analitiği (UBA) Nedir?

Kullanıcıların her gün ürettiği ağ olaylarına ilişkin içgörü toplama sürecidir. Toplandıktan ve analiz edildikten sonra, güvenliği ihlal edilmiş kimlik bilgilerinin kullanımın,yanal hareketi ve diğer kötü niyetli davranışları tespit etmek için kullanılabilir.

User Behavioral Analytics çözümleri, insan davranışı modellerine bakar ve ardından bu modellerden gelen anlamlı anormallikleri (potansiyel tehditleri gösteren anormallikler) tespit etmek için algoritmalar ve istatistiksel analizler uygular. Cihazları veya güvenlik olaylarını izlemek yerine, UBA bir sistemin kullanıcılarını takip eder.

Kullanıcı Davranış Analizi(UBA) Nasıl İşler?

Potansiyel bir tehtidin, bir çalışan gibi davranan dış taraf mı yoksa ihmal veya kötü niyetli bir tür risk oluşturan gerçek bir çalışan mı olduğunu daha kolay belirlememizi sağlar. Kullanıcı Davranış Analizi, bir IP adresi veya bir varlığın aksine, ağdaki etkinliği belirli bir kullanıcıya bağlar. Bu, bir kullanıcı alışılmadık veya olası olmayan bir şekilde davranmaya başlarsa, geleneksel çevre izleme araçları tarafından işaretlenmemiş olsa bile, davranışı hızlı bir şekilde tespit edebileceğine, anormal olup olmadığını belirleyip ve bir araştırma başlayabileceği anlamına gelir.

Örneğin, çalıntı kimlik bilgisi, sızma testleri ve gerçek suçlular tarafından kullanılan bir saldırı vektörüdür. Suçlu kimlik bilgilerini kimlik avı saldırıları, kötü amaçlı yazılım, anahtar kaydı ve hatta üçüncü taraf bir veri ihlali yoluyla elde etse de, tek ihtiyaç duydukları tek bir doğru kullanıcı adı ve parola kombinasyonudur; oturum açabildiklerinde, algılanmadan bir ağ içinde sessizce hareket edebilirler. Ancak, bir saldırgan içeri girdikten sonra, genellikle normal bir kullanıcının aksine hareket etmeye başlar. Davetsiz misafir, genellikle "kill-chain" olarak adlandırılan şeyde adım adım ilerleyerek, baskın yapılacak daha ilginç hedefler ve dışarı sızacak veriler arar.

Kullanıcı Davranış Analitiğinin(UBA) Amacı Nedir?

Analitik araçları, SIEM, IDS/IPS, sistem günlüklerinin çok büyük miktarda veriyi anlamlandırmaya yardımcı olur ve diğer araçlar bir araya geliyor. UBA araçları, sistemlerin davranışına ve bunları kullanan kişilere odaklanan özel bir güvenlik analitiği türü kullanır.

Kullanıcı ve Varlık Davranış Analizi (UEBA) Nedir?

Kullanıcı ve varlık davranışı analitiği (UEBA), yalnızca kurumsal ağdaki kullanıcıların değil, aynı zamanda bu ağdaki yönlendiricilerin, sunucuların ve uç noktaların davranışındaki anormallikleri tespit etmek için algoritmalar ve makine öğrenimi kullanan bir siber güvenlik çözümüdür.

UEBA, normal günlük kalıplardan veya kullanımdan kaynaklanan düzensizliklerin olduğu her türlü tuhaf veya şüpheli davranışı tanımaya çalışır. Örneğin, ağdaki belirli bir kullanıcı her gün düzenli olarak 20 MB'lık dosyaları indirir ancak 4 GB'lık dosyaları indirmeye başlarsa, UEBA sistemi bunu bir anormallik olarak kabul eder ve bir BT yöneticisini uyarır veya otomasyonlar mevcutsa, otomatik olarak bağlantıyı keser. bu kullanıcı ağdan.

UEBA, insan davranışını izlemekten daha ileri gider; makineleri izler. Bir şube ofisindeki bir sunucu, bir günde normalden binlerce daha fazla istek alabilir ve bu da olası bir dağıtılmış hizmet reddi (DDoS) saldırısının başladığının sinyalini verir. BT yöneticilerinin bu tür bir etkinliği fark etmemesi ihtimali vardır, ancak UEBA bunu fark edecek ve daha fazla işlem yapacaktır.

UEBA yazılımı yeni uygulamanın başlatılması, ağ üzerindeki aktiviteler ve dosya erişimleri gibi kullanıcı hareketlerine odaklanır. Dosyaya ne zaman erişildi, kim erişti ve nasıl bir aktivitede bulundu gibi kontrolleri yapar.

UEBA yazılımı şüpheli olabilecek davranışları örnekleyerek saldırganı tespit etmeye yardımcı olur. Saldırıyı durdurmak için herhangi bir aksiyon alamaz, onun yerine tespit sağlar ve tehdidin vereceği zararı minimize eder.

Kullanıcı Davranış Analitiği Neden Önemlidir?

Ortalama bir veri ihlali, bir şirkete milyonlara mal olabilir ve genellikle iç tehditler içerir. Bu, kötü aktörler sağlık kayıtları veya fikri mülkiyet gibi hassas verileri çalınmadan önce şüpheli etkinliği tanımayı önemli hale getirir. Bununla birlikte, güvenlik duvarları veya şifreleme gibi çevreye yönelik kurumsal güvenlik teknolojileri, kimlik avı, kötü amaçlı yazılım veya kimlik bilgisi hırsızlığı yoluyla bir kuruluşun verilerine zaten erişim kazanmış olan kötü niyetli kişileri durdurmak için hiçbir şey yapmaz .

Dahası, SaaS, bulut ve mobil uygulamaların yaygın olarak benimsenmesi, risk yönetimini daha da zorlaştırdı Bu uygulamaların ve hizmetlerin çoğu, BT tarafından resmi olarak onaylanmayabilir, bu da onları kullanan kötü aktörleri tespit etmeyi zorlaştırır. Bu, güvenlik açığı olabilecek noktaları ortadan kaldırmak ve güvenlik ekiplerinin veri hırsızlığı girişimlerini proaktif olarak belirlenmesine, analiz etmesine ve yanıt vermesine yardımcı olmak için uygulamalar, kullanıcılar, ağlar, bulut hizmetleri ve cihazlar arasında sürekli görünürlük ihtiyacı yaratır.

Kullanıcı davranışı analitiği, her kullanıcının etkinliğini sürekli olarak izleyerek ve ardından anormal davranışı bir ihlale yol açmadan önce bulup işaretlemek için tehdit algılamayı kullanarak bu zorluğun üstesinden gelir. Bu, kuruluşların yalnızca çevreyi korumak yerine sistemlerindeki hassas verileri korumasını sağlar.

UEBA için En İyi Uygulamalar

UEBA, kullanıcıların ve diğer varlıkların kötü niyetli davranışlarından ortaya çıktı. UEBA araçları ve süreçleri, önceki izleme sistemlerinin yerini almayı amaçlamaz, bunun yerine bunları tamamlamak ve

şirketinizin genel güvenlik duruşunu geliştirmek için kullanılmalıdır. Bir başka harika uygulama da, büyük verinin depolama ve hesaplama güçlerinden yararlanarak, makine öğrenimi ve istatistiksel analiz kullanarak gereksiz veri uyarılarının oluşmasını önlemek ve üretilen büyük miktarda verinin altında ezilmemektir. UEBA, kullanıcıları ve diğer varlıkları izleyerek, bir tehdidin göstergesi olabilecek davranış kalıplarındaki anormallikleri tespit ederek güvenliği güçlendirmek için makine öğrenimi ve algoritmalar kullanır. Günümüz işletmeleri, güvenliğe daha proaktif bir yaklaşım benimseyerek ve kullanıcı ve varlık davranışına ilişkin daha fazla görünürlük kazanarak, daha güçlü bir güvenlik duruşu oluşturabiliyor, tehditleri daha etkili bir şekilde azaltabiliyor ve güvenlik ihlallerini önleyebiliyor.

- Kuruluşunuzun risk profilini anlayın.
- UEBA'yı nasıl kullanmayı düşündüğünüzü belirleyin; bu dağıtım hangi kullanım durumlarını ele alacak?
- UEBA çözümünüzün kullanacağı veri kaynaklarını tanımlayın.
- Hangi davranışların kullanım durumlarınızla alakalı olduğunu tanımlayın.
- UEBA bildirimlerini kimin ve ne zaman alacağını belirleyin.
- Hem dahili hem de harici kullanıcılar ve varlıklar için hesap oluşturun.
- Süreçlerinizin ve politikalarınızın UEBA'yı benimsemenizle uyumlu olmasını sağlayın.
- UEBA çözümünüzü düzenli ve kapsamlı bir şekilde test edin.

UEBA'nın “Üç Sütunu”

Kullanıcı ve Varlık Davranışı Analitiği için Pazar Kılavuzunda Gartner, UEBA çözümlerinin tanımını üç kategoriye göre oluşturur.

-Kullanım Durumları

UEBA'nın birincil kullanım durumu, çok çeşitli farklı tehditlerin tespit edilmesini içerir. Bununla birlikte, Gartner'ın bir şeyi "saf oyun UEBA platformu" olarak görmesi için genel bir yaklaşım olamaz. Bunun yerine, birden çok farklı kullanım durumunu tanımlamalı ve ele almalıdır.

-Veri Kaynakları

Saf oyun UEBA platformu, veri kaynaklarından yerel olarak çekme, günlük yönetimi ve SIEM araçlarıyla entegrasyon veya veri göllerinden çekme dahil olmak üzere verileri toplamak ve düzenlemek için birden çok yol sunar. Özel enstrümantasyon ajanları olmadan bunu başarabilir.

-Analitik

Pure-play UEBA, gelişmiş, sofistike analitiği vurgular. Bunlar, platformun gerçekleştirmeyi amaçladığı her bir bireysel kullanım durumuna göre özelleştirilmiş analitik modelleri kullanmalıdır. Bu analitik yöntemleri ve süreçleri, gerektiğinde temel analitiklerle desteklenmelidir.

UEBA vs. SIEM vs. SOAR vs. XDR: Terminoloji ve Teknolojideki Temel Farklılıklar

UEBA ürünleri, tehdit algılamayı ele almanın yalnızca bir yoludur. Diğer ilgili teknolojiler şunları içerir: SIEM sistemleri, olası tehditleri belirlemek ve uyarılar vermek için birden fazla kaynaktan veri toplar. SIEM sistemleri, uyumluluk sorunlarını tespit etmek için yaygın olarak kullanılır ve siber saldırılarla ilişkili şüpheli davranış kalıplarını belirlemek için istatistiksel modeller kullanır. SIEM ürünleri, çoğu yanlış pozitif olabilen yüksek hacimli uyarılarla bilgi güvenliği ekiplerini yorabilir. Güvenlik düzenleme, otomasyon ve yanıt (SOAR) sistemleri, zengin olay verileri toplayarak ve potansiyel tehditleri ve anormallikleri belirlemek için otomasyonu kullanarak SIEM sistemlerinde iyileşir. SOAR sistemleri, güvenlik veri kaynaklarıyla entegrasyon gerektirir ve yine de bilgi güvenliği analistlerinden önemli ölçüde çaba gerektirir. Genişletilmiş algılama ve yanıt (XDR) sistemleri, en yeni nesil uç nokta algılama ve yanıt (EDR) sistemleri ve ağ algılama ve yanıt (NDR) sistemleridir. EDR, son kullanıcı bilgisayarları ve kurumsal sunucular gibi uç nokta sistemlerine odaklanırken, NDR ağ aktarımlarını izler. XDR, UBA ve UEBA işlevselliğinin yanı sıra SOAR ve SIEM ile yakınsayan, gelişmekte olan bir teknolojidir. İlgili teknolojilerin bolluğu göz önüne alındığında, farklı türdeki tehdit algılama araçları önemli ölçüde örtüşmektedir. Diğer bilgi güvenliği sistemlerinde olduğu gibi, UBA ve UEBA, siber güvenlik araç setindeki birçok araçtan biri olarak düşünülmelidir. Bu farklı sistemler arasındaki örtüşme potansiyeline rağmen, kuruluşun kullanım durumlarını anlamak, siber güvenlik uzmanlarının doğru yöne işaret etmesine yardımcı olabilir. Şirketlerin, yalnızca günlüğe kaydedilenleri değil, bir saldırganın faaliyetlerinin ve tekniklerin her yönü de dahil olmak üzere, bir saldırının hemen hemen sonraki aşamalarına kadar tüm ağlarındaki tüm olayları görmelerini sağlar. Şirketlerin ağ cihazlarının ve kullanıcı hesaplarının profilini oluşturmasını sağlar. Göreceli kolaylıkla devreye girer. Kısa sürede kendini amorti eder, ancak yine de hangi tür güvenlik sorunlarının aranacağını ve bunların nasıl tanımlanacağını bilmek için bir güvenlik ekibinin uzmanlığını gerektirir. Geniş olmasına rağmen sığ olan kapsama alanı sunar. Yerel olayları takip edemez.

UEBA ve SIEM Teknolojisi: Neden bunları birlikte kullanmalısınız?

Birçok kuruluş UEBA ve SIEM teknolojilerini birlikte kullanmayı tercih ediyor. Bu iki sistem türü arasındaki farklara bakıldığında, birbirlerini nasıl tamamladıkları vurgulanır:

UEBA sistemleri, gerçek zamanlı veri yakalama ve analizine odaklanır. SIEM sistemleri, zaman içindeki tek bir noktadan sınırlı bir zaman periyoduna kadar belirli bir süre boyunca olay verilerini inceler.

UEBA sistemleri, potansiyel tehditleri meydana gelirken otomatik olarak işaretlemek için makine öğrenimine güvenirken SIEM sistemleri, siber güvenlik uzmanlarına tehditleri manuel olarak aramak için güçlü bir araç sağlar.

UEBA sistemleri, günlükler ve hem yapılandırılmış hem de yapılandırılmamış veri kümeleri dahil olmak üzere birçok farklı veri türünden olayları toplar. UEBA, tehdit kanıtlarını bir araya getirmek ve tehditleri azaltmaya yönelik yaklaşımları belirlemek için makine öğrenimine bağlıdır. Buna karşılık, SIEM sistemleri, genellikle yapılandırılmış günlüklerden gelen gelen verilere dayatılan daha fazla yapıya sahip olma eğilimindedir.

UEBA sistemleri, farklı tehditleri karşılaştırmak ve hangi sistemlerin hangi yollarla risk altında olduğunu belirlemek için risk puanlamasına bağlıdır. SIEM sistemleri, sistem bilinen saldırılarla ilişkili bir etkinlik modeli algıladığında otomatik olarak oluşturulan uyarılara ve bildirimlere bağlıdır.

SIEM ve UEBA sistemlerini birleştirmek kuruluşlara fayda sağlayabilirken, bazı uzmanlar SIEM'in UEBA'yı birleştirmeye ve değiştirmeye hazır olduğunu öne sürüyor.

UEBA Araçları

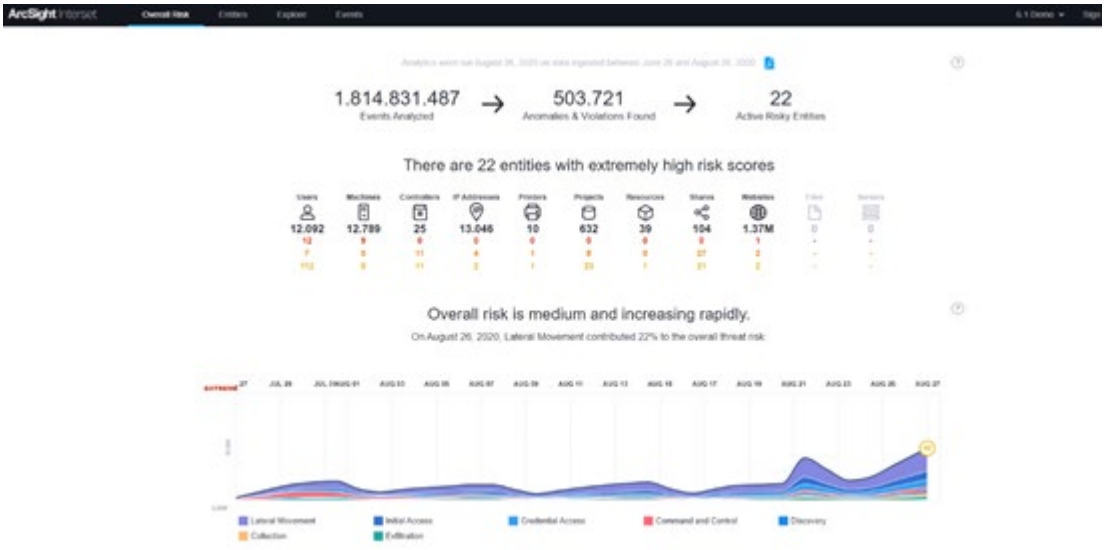
Fortinet FortiInsight, Gurucul UEBA, Splunk, Cynet, LogRhythm, Rapid7 InsightIDR, Exabeam, Microsoft Sentinel, Cynet 360 AutoXDR, IBM QRadar User Behavior Analytics, Microsoft Defender for Identity, Interset..

UEBA Teknolojisiyle Interset

Interset, 2015 yılından itibaren güvenlik operasyonlarında davranış analizi tekniğini kullanarak olası iç tehditleri modelleyen ve güncel, karmaşık risk durumlarını tespit eden bir ürün olarak karşımıza çıkmaktadır. Bu doğrultuda 0-100 arası risk puanları aracılığı ile iç tehditleri dikte ederek; kendi outputları ile SIEM outputları arasında ilişkilendirme yöntemiyle aksiyonu mümkün kılmaktadır.

Interset Nedir? Ne Amaçla Kullanılır?

Interset, çoğunlukla dış tehditlere karşı konfigüre edilen SIEM ürünlerinin yanında kuruluş bünyesinde meydana gelen ve var olan en riskli varlık ve davranışları belirleyerek, iç tehditleri tespit etme imkanı sunmaktadır. Değişen çalışma biçimlerine bağlı olarak artık çalışanlar şirket dışında herhangi bir lokasyondan, evden ya da cep telefonundan çalışmaya devam edebilmektedir. Veri/hesap ihlali/hırsızlığı, kullanıcılar tarafından istemli yada istemsiz etkinliklerle ilişkili olarak gerçekleşebilmektedir. Bu doğrultuda Interset risk durumlarını belirleyerek normalin dışında gerçekleşen durumları monitör imkanı sunmaktadır. Bu sayede kurumlar tarafından olası tehditlerin fark edilerek büyük resmin daha net görülebilmesi, küçük ayrıntıların belirginleştirilmesi ile sağlanmaktadır.

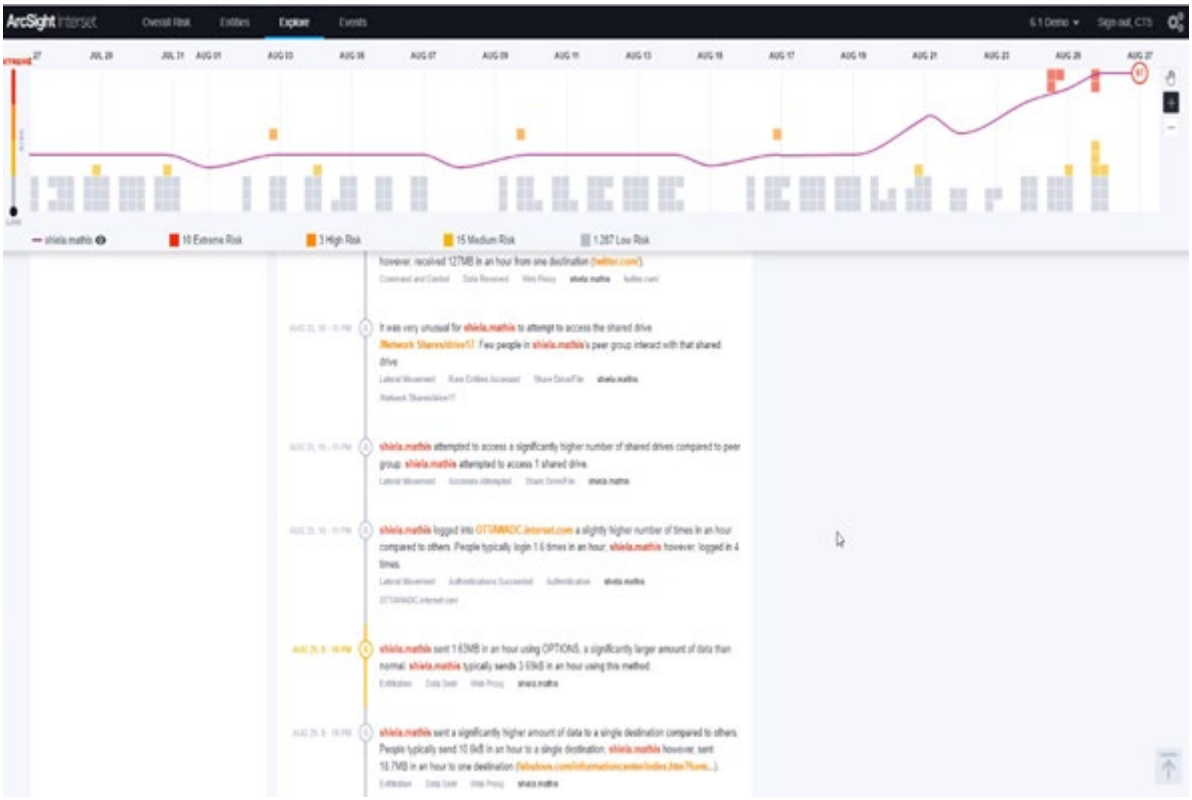


Interset Bileşenleri Nelerdir?

Anomali tespitinde görev alan IntersetAnalytics, tüm verileri monitör etme imkanı sunan Interset UI, verilerin raporlanmasına olanak tanıyan Interset Exports, file server olarak görev yapan ve Spark2 konfigürasyon dosyalarının bulunduğu Interset-spark-config-server ile Interset API bileşenlerinden oluşmaktadır.

Bunların yanında üçüncü parti bileşenleri aşağıda sıralanmaktadır.

- Elasticsearch, Logstash
- Kibana
- H2
- Apache HDFS
- Apache Spark2



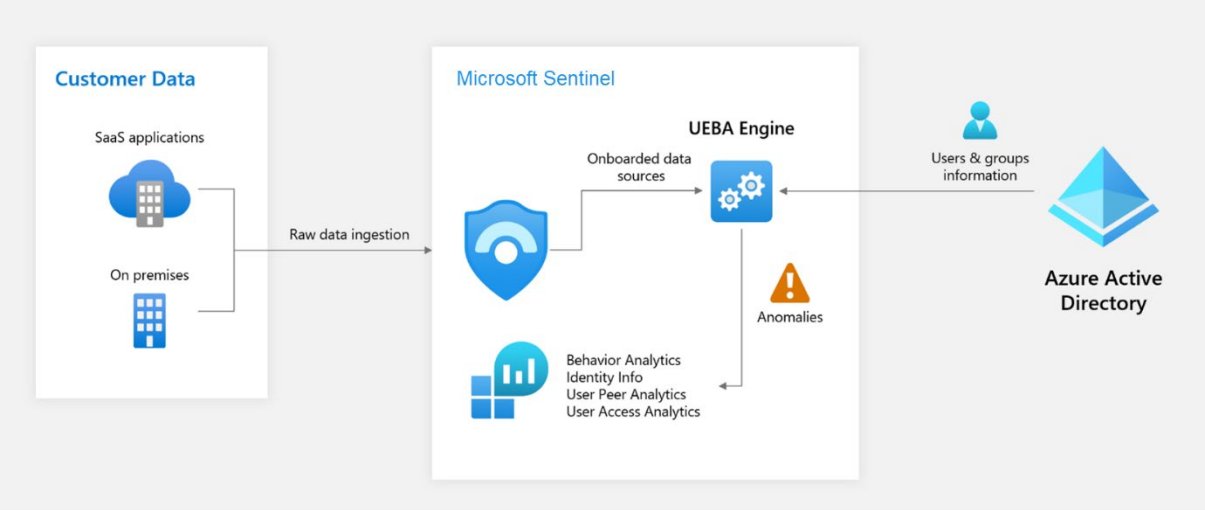
Interset Nasıl Çalışır?

Interset, tehdit olarak gruplayabileceği aksiyonları davranış analizi metodu ile tespit etmektedir. İlk adım olarak kurum için farklı başlıklar bünyesinde normal olan davranışı belirler. Akabinde davranış analitiğini kullanarak potansiyel riskleri gruplar ve puanlar.

Temelde agentlar (smartconnector) aracılığı ile toplanan loglar; vertica altyapısıyla entegre hale getirilir. Logstash-Elasticsearch aracılığıyla indexlenir,anlamlandırılır. Kibana aracılığıyla monitör edilebilir. H2, tüm kullanıcı kimliklerini muhafaza eder. IntersetAnalytics Spark2 desteği ile faaliyet gösterirken, analytics çıktıları HDFS tarafından depolanır.

Microsoft Sentinel

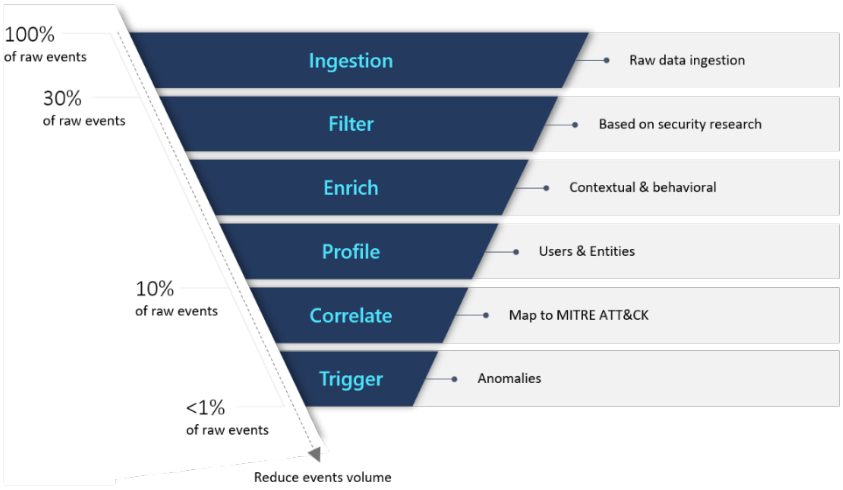
UEBA analiz mimarisi



Güvenlik Temelli Analiz

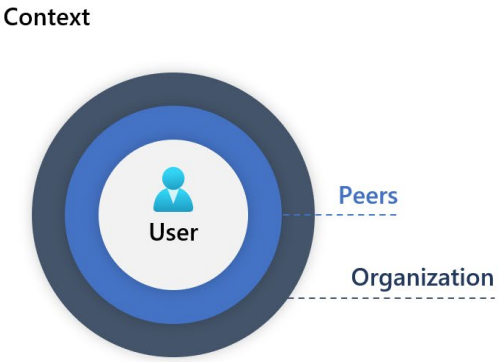
Gartner'ın UEBA çözümleri paradigmasından ilham alan Microsoft Sentinel, üç referans çerçevesini temel alan "dışarıdan" bir yaklaşım sunar:

- Kullanım örnekleri: Çeşitli varlıkları sonlandırma zincirinde kurban, fail veya özet nokta olarak yerleştiren taktikler, teknikler ve alt tekniklerden oluşan MITRE ATT&CK çerçevesiyle uyumlu güvenlik araştırmalarına dayalı ilgili saldırı vektörlerine ve senaryolarına öncelik vererek; Microsoft Sentinel özellikle her veri kaynağının sağlayabilecekleri en değerli günlüklere odaklanır.
- Veri Kaynakları: İlk ve en önemli destek Azure veri kaynakları olsa da, Microsoft Sentinel tehdit senaryolarımızla eşleşen verileri sağlamak için üçüncü taraf veri kaynaklarını dikkatle seçer.
- Analytics: Microsoft Sentinel, çeşitli makine öğrenmesi (ML) algoritmalarını kullanarak anormal etkinlikleri tanımlar ve bazı örnekleri aşağıda gösterilen bağlamsal zenginleştirmeler biçiminde net ve kısa kanıtlar sunar.



Microsoft Sentinel, güvenlik analistlerinizin bağlam içindeki anormal etkinlikleri ve kullanıcının temel profiliyle karşılaştırıldığında net bir şekilde anlamalarına yardımcı olan yapıtlar sunar. Kullanıcı (veya konak ya da adres) tarafından gerçekleştirilen eylemler bağlamsal olarak değerlendirilir ve burada "doğru" sonuç tanımlanan bir anomaliyi gösterir:

- coğrafi konumlar, cihazlar ve ortamlar arasında.
- zaman ve sıklık ufuklarında (kullanıcının kendi geçmişiyle karşılaştırıldığında).
- eşlerin davranışıyla karşılaştırıldığında.
- kuruluşun davranışıyla karşılaştırıldığında.



Microsoft Sentinel'in kullanıcı profillerini oluşturmak için kullandığı kullanıcı varlığı bilgileri, Azure Active Directory'nizden (ve/veya şirket içi Active Directory artık önizlemededir) gelir. UEBA'yı etkinleştirdiğinizde, Azure Active Directory'nizi Microsoft Sentinel ile eşitler ve bilgileri Log Analytics'teki *IdentityInfo* tablosu aracılığıyla görünen bir iç veritabanında depolar.

Artık önizleme aşamasında Kimlik için Microsoft Defender kullanarak şirket içi Active Directory kullanıcı varlığı bilgilerinizi de eşitleyebilirsiniz.

Puanlama

Her etkinlik, kullanıcının ve eşlerinin davranışsal öğrenmesine bağlı olarak belirli bir etkinliği gerçekleştiren belirli bir kullanıcının olasılığını belirleyen "Araştırma Önceliği Puanı" ile puanlanır. En anormal olarak tanımlanan etkinlikler en yüksek puanları alır (0-10 ölçeğinde).

Varlık Sayfaları

Bir varlık aramasında, uyarıda veya araştırmada bir kullanıcı veya konak varlığıyla (IP adresi varlıkları önizlemededir) karşılaştığınızda, varlığı seçebilir ve varlıkla ilgili yararlı bilgilerle dolu bir veri sayfası olan varlık sayfasına gidebilirsiniz. Bu sayfada bulacağınız bilgi türleri varlık hakkındaki temel bilgileri, bu varlıkla ilgili önemli olayların zaman çizelgesini ve varlığın davranışıyla ilgili içgörüleri içerir.

Varlık sayfaları üç bölümden oluşur:

- Sol taraftaki panel, Azure Active Directory, Azure İzleyici, Bulut için Microsoft Defender, CEF/Syslog ve Microsoft 365 Defender gibi veri kaynaklarından toplanan varlığın tanımlayıcı bilgilerini içerir.
- Orta panelde, varlıkla ilgili uyarılar, yer işaretleri, anomaliler ve etkinlikler gibi önemli olayların grafiksel ve metinsel zaman çizelgesi gösterilir. Etkinlikler, Log Analytics'ten önemli olayların toplamalarıdır. Bu etkinlikleri algılayan sorgular Microsoft güvenlik araştırma ekipleri tarafından geliştirilmiştir ve artık seçtiğiniz etkinlikleri algılamak için kendi özel sorgularınızı ekleyebilirsiniz .
- Sağ taraftaki panel varlıkla ilgili davranış içgörüleri sunar. Bu içgörüler anomalileri ve güvenlik tehditlerini hızla belirlemeye yardımcı olur. İçgörüler Microsoft güvenlik araştırma ekipleri tarafından geliştirilmiştir ve anomali algılama modellerini temel alır.

Zaman Çizelgesi

Zaman çizelgesi, varlık sayfasının Microsoft Sentinel'deki davranış analizine katkısının önemli bir parçasıdır. Varlıkla ilgili olaylar hakkında bir hikaye sunarak varlığın belirli bir zaman dilimi içindeki etkinliğini anlamanıza yardımcı olur.

Önceden ayarlanmış çeşitli seçenekler arasından zaman aralığını seçebilir (örneğin *, son 24 saat*) veya özel tanımlı herhangi bir zaman dilimine ayarlayabilirsiniz. Ayrıca, zaman çizelgesindeki bilgileri belirli olay veya uyarı türleriyle sınırlayan filtreler ayarlayabilirsiniz.

Zaman çizelgesine aşağıdaki öğe türleri dahil edilir:

- Uyarılar - varlığın eşlenmiş varlık olarak tanımlandığı tüm uyarılar. Kuruluşunuz analiz kurallarını kullanarak özel uyarılar oluşturduysa kuralların varlık eşlemesinin düzgün yapıldığından emin olmanız gerektiğini unutmayın.
- Yer işaretleri - sayfada gösterilen belirli varlığı içeren tüm yer işaretleri.
- Anomaliler - Çeşitli veri girişlerinde ve kendi geçmiş etkinliklerine, eşlerine ve kuruluşun bütün olarak sahip olduğu etkinliklere karşı her varlık için oluşturulan dinamik temelleri temel alan UEBA algılamaları.
- Etkinlikler - varlıkla ilgili önemli olayların toplanması. Çok çeşitli etkinlikler otomatik olarak toplanır ve artık kendi seçtiğiniz etkinlikleri ekleyerek bu bölümü özelleştirebilirsiniz .

Entity Insights

Varlık içgörüleri, analistlerinizin daha verimli ve etkili bir şekilde araştırmalarına yardımcı olmak için Microsoft güvenlik araştırmacıları tarafından tanımlanan sorgulardır. İçgörüler varlık sayfasının bir parçası olarak sunulur ve konaklar ve kullanıcılar hakkında tablosal veriler ve grafikler biçiminde değerli

güvenlik bilgileri sağlar. Bilgileri burada bulundurmak, Log Analytics'e gitmek zorunda olmadığınız anlamına gelir. İçgörüler oturum açma işlemleri, grup eklemeleri, anormal olaylar ve daha fazlası ile ilgili verileri ve anormal davranışları algılamak için gelişmiş ML algoritmalarını içerir.

İçgörüler aşağıdaki veri kaynaklarını temel alır:

- Syslog (Linux)
- SecurityEvent (Windows)
- AuditLogs (Azure AD)
- SigninLogs (Azure AD)
- OfficeActivity (Office 365)
- BehaviorAnalytics (Microsoft Sentinel UEBA)
- Sinyal (Azure İzleyici Aracısı)
- CommonSecurityLog (Microsoft Sentinel)
- ThreatIntelligenceIndicators (Microsoft Sentinel)

Davranış Analizi Verilerini Sorgulama

Örneğin, kullanıcının belirli bir ülkeden ilk kez bağlanma girişimi olduğu bir Azure kaynağında oturum açamayan bir kullanıcının tüm servis taleplerini bulmak istiyorsak ve bu ülkedeki bağlantılar kullanıcının eşleri için bile sık rastlanmayan bir durumsa, aşağıdaki sorguyu kullanabiliriz:

```
Kusto

BehaviorAnalytics
| where ActivityType == "FailedLogOn"
| where ActivityInsights.FirstTimeUserConnectedFromCountry == True
| where ActivityInsights.CountryUncommonlyConnectedFromAmongPeers == True
```

Kullanıcı Eşleşmeleri Meta Verileri

Kullanıcı eşlerinin meta verileri tehdit algılamalarında, bir olayı araştırmada ve olası bir tehdidi avlamada önemli bir bağlam sağlar. Güvenlik analistleri, bir kullanıcının eşlerinin normal etkinliklerini gözlemleyebilir ve kullanıcının etkinliklerinin kendi iş arkadaşları ile karşılaştırıldığında olağan dışı olup olmadığını belirleyebilir.

Microsoft Sentinel, kullanıcının Azure AD güvenlik grubu üyeliği, posta listesi ve cetera temelinde kullanıcının eşlerini hesaplar ve sıralar ve UserPeerAnalytics tablosunda 1-20 derecesine sahip eşleri depolar. Aşağıdaki ekran görüntüsünde UserPeerAnalytics tablosunun şeması gösterilmekte ve Kendall Collins kullanıcısının en iyi sekiz dereceli eşleri gösterilmektedir. Microsoft Sentinel, sıralamayı

hesaplamak için tartımı normalleştirmek için *frequency-inverse belge sıklığı* (TF-IDF) algoritması terimini kullanır: grup ne kadar küçük olursa ağırlık o kadar yüksek olur.

Microsoft Sentinel, BehaviorAnalytics tablosunu temel alan kullanıma hazır bir dizi tehdit avcılığı sorgusu, keşif sorgusu ve Kullanıcı ve Varlık Davranış Analizi çalışma kitabı sağlar. Bu araçlar, anormal

TimeGenerated [UTC]	AADTenantId	UserId	UserPrincipalName	UserName	PeerUserId	PeerUserPrincipalName	PeerUserName	Rank	Type
9/16/2020, 12:00:00.000 AM	4b2462a4-bbee-...	63e00a3a-7628-...	kcollins@contoso.com	Kendall Collins	09ae034d-f53b-...	scantrell@contoso.com	Sam Cantrell	1	UserPeerAnalytics
9/16/2020, 12:00:00.000 AM	4b2462a4-bbee-...	63e00a3a-7628-...	kcollins@contoso.com	Kendall Collins	0872937f-1d3c-4...	nwagner@contoso.com	Nicole Wagner	2	UserPeerAnalytics
9/16/2020, 12:00:00.000 AM	4b2462a4-bbee-...	63e00a3a-7628-...	kcollins@contoso.com	Kendall Collins	38cde1ef-5079-4...	tphillips@contoso.com	Taylor Phillips	3	UserPeerAnalytics
9/16/2020, 12:00:00.000 AM	4b2462a4-bbee-...	63e00a3a-7628-...	kcollins@contoso.com	Kendall Collins	7eeba75a-48b3-...	hacook@contoso.com	Hayden Cook	4	UserPeerAnalytics
9/16/2020, 12:00:00.000 AM	4b2462a4-bbee-...	63e00a3a-7628-...	kcollins@contoso.com	Kendall Collins	ebe5a493-b729-...	mreyes@contoso.com	Miguel Reyes	5	UserPeerAnalytics
9/16/2020, 12:00:00.000 AM	4b2462a4-bbee-...	63e00a3a-7628-...	kcollins@contoso.com	Kendall Collins	a489f679-45c8-...	bstuart@contoso.com	Brandon Stuart	6	UserPeerAnalytics
9/16/2020, 12:00:00.000 AM	4b2462a4-bbee-...	63e00a3a-7628-...	kcollins@contoso.com	Kendall Collins	95289cbf-4ab6-...	eulopez@contoso.com	Eugenia Lopez	7	UserPeerAnalytics
9/16/2020, 12:00:00.000 AM	4b2462a4-bbee-...	63e00a3a-7628-...	kcollins@contoso.com	Kendall Collins	f3b662ce-a48a-...	rmurphy@contoso.com	Rowan Murphy	8	UserPeerAnalytics

davranışları gösteren belirli kullanım örneklerine odaklanmış zenginleştirilmiş veriler sunar.

Sonuç olarak UEBA ile neler yapabilirsiniz?

1. İçeriden gelen tehditleri tespit edin. Bir çalışanın veya belki de bir grup çalışanın kendi erişimlerini kullanarak verileri ve bilgileri çalarak dolandırıcı olabileceğini hayal etmek çok zor değil. UEBA, kendi personeliniz tarafından yapılan veri ihlallerini, sabotajları, ayrıcalık kötüye kullanımlarını ve politika ihlallerini tespit etmenize yardımcı olabilir.

2. Güvenliği ihlal edilmiş hesapları tespit edin. Bazen, kullanıcı hesapları tehlikeye girer. Kullanıcı, farkında olmadan kendi makinesine kötü amaçlı yazılım yüklemiş olabilir veya bazen yasal bir hesap sahtecilik olabilir. UEBA, sahtekarlık ve güvenliği ihlal edilmiş kullanıcıları gerçek zarar vermeden önce ayıklamanıza yardımcı olabilir.

3. Kaba kuvvet saldırılarını tespit edin. Bilgisayar korsanları bazen bulut tabanlı varlıklarınızı ve üçüncü taraf kimlik doğrulama sistemlerini hedefler. UEBA ile kaba kuvvet girişimlerini tespit edebilir ve bu varlıklara erişimi engellemenizi sağlayabilirsiniz.

4. İzinlerdeki değişiklikleri ve süper kullanıcıların oluşturulmasını tespit edin. Bazı saldırılar süper kullanıcıların kullanımını içerir. UEBA, süper kullanıcıların ne zaman oluşturulduğunu veya gereksiz izinler verilmiş hesaplar olup olmadığını tespit etmenize olanak tanır.

5. Korunan verilerin ihlalini tespit edin. Korunan verileriniz varsa, sadece güvende tutmak yeterli değildir. Bir kullanıcının bu verilere erişmek için meşru bir ticari nedeni olmadığında bu verilere ne zaman eriştiğini bilmelisiniz.

KAYNAKÇA

https://www.blackberry.com/us/en/solutions/endpoint-security/user-entity-behavior-analytics

https://blog.ubiminds.com/en-us/what-is-user-behavior-analytics/

https://docs.microsoft.com/tr-tr/azure/sentinel/identify-threats-with-entity-behavior-analytics

https://tr2tr.wiki/wiki/User_behavior_analytics

https://www.techtarget.com/searchsecurity/definition/user-behavior-analytics-UBA

https://www.cyberark.com/what-is/user-behavior-analytics/

https://www.netsmart.com.tr/2020/10/28/interset-ile-kullanici-davranis-analizi/

https://www.act.com/en-gb/user-behaviour-analytics/#:~:text=What%20is%20behaviour%20analytics%20used,journey%20taken%20by%20each%20user.

https://snowplowanalytics.com/what-is-behavioral-data/

https://docs.microsoft.com/en-us/defender-cloud-apps/tutorial-suspicious-activity

https://mevlutkuyumcu.medium.com/ueba-kullan%C4%B1c%C4%B1-varl%C4%B1k-davran%C4%B1%C5%9F-analizi-aa3e23123146