AWAKE

EXCLUSIVE NETWORKS

Gelişmiş Ağ Trafik Analizi

Bulunuşu ve Önemi

AWAKE

Gelişmiş Ağ Trafik Analizi Bulunuşu ve Önemi

Giriş

Son birkaç yılda gerçekleşen veri ihlallerinin çoğu, güvenlik risklerini yönetmek isteyen bir kuruluş için yalnızca saldırı önleme öncelikli, çevre odaklı bir güvenlik yaklaşımının yeterli olmayacağını göstermiştir. Saldırılar, uzun soluklu olacak şekilde evrimleşti ve geleneksel zamanında saldırıyı önleme yaklaşımları yetersiz kalmaya başladı. Aslında, endüstri analistleri tespit ve müdahalenin artık kuruluşlar için en önemli öncelik olduğuna dikkat çekiyorlar.[1,2]

Bu değişen dinamiği gözünüzde canlandırmak için şu soruların cevabını sorgulayın; saldırı için Sunucu Mesaj Bloğu (Server Messaging Blocks - SMB) kullanarak paylaşılan dosyaları tespit edip ardından saldırı gerçekleştiren bir saldırganı nasıl tespit edersiniz? Veya birisinin telefon konuşmalarını kaydetmek için IP telefon sistemine girip girmediğini ne kadar çabuk anlarsınız? Cevaplar, her şeyi gören ve diğer veri kaynaklarının mücadele edebileceği kesin bir gerçeklik sunan ağda yatmaktadır. Hızlı ağ tespiti ve müdahale, nihayetinde bir saldırganın ağda geçirdiği süreyi azaltır ve böylece etkiyi en aza indirir. Ancak, tüm bunların etkili sonuç verebilmesi için , ağın kendi tanımı bile değişirken, ağ kendisini yenilemeli ve gelişmeli ki kullanıcılar, kurumlarını saldırılara karşı koruyabilsinler.

Gartner diyor ki...
Tespit ve Müdahale, Kurumlar için Birinci Güvenlik Önceliği

> "Ağ güvenliğinde tespit ve müdahale yaklaşımına geçiş, insanlar, süreçler ve teknoloji unsurları arasında yayılıyor. Önümüzdeki beş yıl içerisinde güvenlik pazarındaki büyümenin büyük bir kısmı buradan gelecek... Bu değişim, önlemenin önemsiz olduğu anlamına gelmediği gibi Bilgi Güvenliği Yetkilileri (CISO) de güvenlik sorunlarını önleme olgusunu bir kenara itmiyor. Sadece, saldırıyı önlemenin, algılama ve müdahale ile ilişkilendirilmediğinde beyhude bir çaba olduğunun altını çiziyor."
>
> - Sid Deshpande, Principal Research Analyst at Gartner

Ağ güvenliğinin gelişimi

Önce IDS geldi

Bugün nerede olduğumuz ve nereye gittiğimiz hakkında konuşmadan önce, bu evrimleri anlayabileceğimiz bir çerçeve oluşturmak faydalı olacaktır. Ağ saldırı tespit sistemlerinin (Intrusion Detection Systems - IDS) ilk versiyonları kötü amaçlı yazılımın imzaları için ayrı paketlere veya oturumlara bakarak bilinen kötü amaçlı yazılımları tespit etmek için yaratılmıştı.

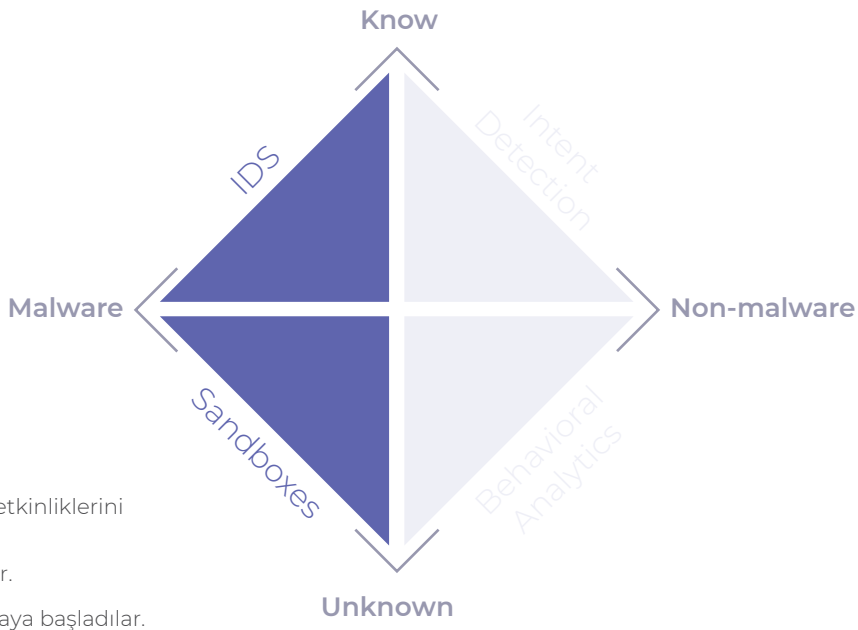
Ancak o model bir çok sorunu da çözümsüz bırakıyordu:

- Malware'lerin her çeşitini nasıl tespit edersiniz?
- Kaç imza, çok fazla imza demektir?
- Değişken doğru bilinen yanlışlarla nasıl baş edersiniz?

[1] https://www.gartner.com/en/newsroom/press-releases/2017-03-14-gartner-says-detection-and-response-is-top-security-priority-for-organizations-in-2017
[2] https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

Daha sonra Sandbox çıktı

Saldırganlar, malwarelerde basit ancak ince değişiklikler yaparak IDS'leri atlatmaya başladılar. Bu, bilinmeyen malwareler çağını ve temel yeni bir zorluğu beraberinde getirdi: güvenlik açığının istismar edildiğine dair önceden bilgi sahibi olmadan, bir kişi nasıl imza oluşturabilirdi? Cevap: SandBox. Bunlar, bir şeyin muhtemelen kötü amaçlı olup olmadığını belirlemek için statik ve dinamik analizlerin bir kombinasyonunu kullandı. Bu bir süre işe yaradı ve bazı IDS sorunlarının üstesinden gelmeyi başardı.



Güvenlik ekipleri, malwareleri engelleyecek yetkinliklerini geliştirdikçe saldırganlar da taktik değiştirdi. Saldırılarında malwareleri kullanmayı azalttılar.

Ayrıca saldılar uzun soluklu ve çok adımlı olmaya başladılar. Aylarca, haftalarca sürmese bile günlerce sürer hale geldi. Ağ paketlerinde ve dosyalarda zaman analizlerini yaparak saldırıları önleyemez hale geldiler. Saldırganlar artık hedef organizasyondaki insanlara giderek daha fazla odaklanıyor, meşru kimlik bilgilerini çalıyor ve daha sonra bunları ortama zaten yerleştirilmiş araçlarla kullanıyor - Python gibi komut dosyası dillerini veya PowerShell, WMI veya psexec gibi sistem yardımcı programlarını ve hatta Microsoft Word veya Excel gibi üretkenlik araçlarını.

Ağ Trafik Analizi: Davranışsal Analitik

Güvenlik endüstrisi, bu gelişen saldırılara ağ trafiği analizi (Network Traffic Analysis - NTA) ile yanıt verdi - yaklaşımı "bilinen kötü" nün tanımlanmasından "normal veya iyi" olanın temelini oluşturmaya kaydırdı ve ardından bu temelden anormallikleri "potansiyel olarak kötü" olarak tespit etti. Bu yaklaşım " veri bilimi " , " makine öğrenmesi " ve " yapay zeka "gibi kelimelerle yoğun bir şekilde pazarlandı.

Davranışsal analitik ve anomali tespiti bazı sorunları da beraberinde getirdi:

Eğitim
Algoritmaların neyin "normal" olduğunu anlaması gerekir. Bu zaman alır - genellikle 30 ila 90 gün sürer. Bu süre, teknolojiyi değerlendirmeye veya ortamınıza yerleştirmeye çalışırken sinir bozucu olabilir. Ama daha da kötüsü: ya çevre zaten tehlikeye atılmışsa? Ardından saldırganın davranışı temelin bir parçası olur!

Zayıf yönlendirme
Çoğu durumda temel belirleme, davranışları 3. katman IP adreslerine de atfeder. Bununla birlikte, IP adresleri herhangi bir modern ağda sıklıkla değişir: tek bir gün içinde, belirli bir aygıt birden çok IP adresine sahip olabilir ve birden çok aygıta benzersiz bir IP adresi atanabilir. Sistem, IP adreslerine göre uyarı verirse, birden fazla cihazdan gelen davranışları bir araya getirir ve IP'ler arasında hareket eden gerçek cihazların ve kullanıcıların davranışlarını izleyemez ve karakterize edemez. Öte yandan, MAC adreslerine dayanıyorsa, ilk ağ sıçramasının ötesinde görünürlüğünü kaybeder. Öyleyse, bir cihaz veya kullanıcı gibi belirli şey için neyin anormal olduğunu gerçekten nasıl bilebilirsiniz?

Davranışlar her daim değişir
Modern ağlar, yeni uygulamalara bağlı olarak, eski alışkanlıkların bırakıldığı ve yenilerinin ortaya çıktığı dinamik bir yapıdır. Örneğin, bir güvenlik temeli oluşturulduktan sonra bilgi işlem departmanı yeni bir yedekleme çözümü sunduğunda ne olacağını düşünün. Ağdaki her sistem, verileri önceden bilinmeyen bir konuma yüklediği için ortaya bir anormallik çıkar. Bu, yanlış pozitiflere ve yeniden eğitim ihtiyacına yol açar.

Nihayetinde, NTA çözümleri umut vaat ederken, güvenlik ekipleri bazen hem süregelen değeri görmek hem de çözümün operasyonel maliyetlerini korumaya çalışırken sorunlar yaşadı.

Gelişmiş Ağ Trafik Analizi

Son on yılda ağ işleme, veri analizi ve güvenlik araştırması alanlarında muazzam yenilikler yaşandı. Yukarıda tarif ettiğimiz eksiklikleri özellikle çözmek için bu ilerlemelerden yararlanan yeni bir çözüm kategorisi şimdi ortaya çıkıyor. Daha da önemlisi, bugün karşı karşıya olduğumuz tehditlerle mücadele etmenize yardımcı olacak yetenekler de ekliyor. Gelişmiş ağ trafiği analizi çözümleri, çeşitli şekillerde birinci nesil davranışsal analitik çözümlerinin ötesine geçiyor.

Veri Kaynakları

Öncelikle, ağ nedir?

İş yüklerinin buluta taşındığı ve uzaktaki çalışanların genellikle istisna değil kural olduğu sınırların kalktığı bir dünyada, ağın tanımı değişiyor. Gelişmiş NTA çözümleri, bunlar ister geleneksel TCP / IP tarzı paketler, ister bir vswitch'ten geçen bulut verileri, Saas uygulama verileri ve API haberleşmesi gibi "sanal ağ trafiği" olsun, ağ haberleşmesini analiz etmeye odaklanır. Bu çözümler, aynı zamanda, güvenlik ekiplerinin görünmez kabul ettiği operasyonel teknoloji ağlarına da odaklanır. Bu gelişmeler, güveniğin otomatize edilmiş, ağa bağlı çalışma ortamına engel teşkil etmediğinden emin olmak zorundadır.

Tam paket analizi veya sadece meta-veri

Birinci nesil NTA çözümleri, öncelikle protokol başlıkları veya ağ akışı bilgileri gibi üçüncü ve dördüncü katman ağ meta verilerini işledi. Neden? Çünkü 7. katman aracılığıyla akan tam paket verileri çok daha büyüktür ve gerçek zamanlı olarak işlenmesi daha zordur. Ancak bu hacim aynı zamanda çok daha fazla sinyal anlamına gelir - algılama doğruluğunu iyileştirmek, varlıkları izlemek ve belki de çözümün büyük ve karmaşık ağlara ölçeklenmesine yardımcı olmak için yararlı olan sinyal. Örneğin, Kerberos paketlerinde bulunan kullanıcı bilgileri gibi sinyaller protokol başlıklarında veya ağ akışında görünmez. Tam paketler aynı zamanda size etkinlik kaydını anlama ve saklama ve daha sonra zamanda geriye gitme ve ilk meydana geldiklerinde kötü niyetli olarak algılanmamış olabilecek davranışları geriye dönük olarak algılama yeteneği sağlar. Bu aktivite kaydı, tam paket verisine göre depolama alanı açısından da önemli ölçüde daha küçüktür.

Aktiviteler ve meta-veri Bir Analoji

Kolluk kuvvetindeyseniz ve suç iletişimlerini izliyorsanız, yeni kaydedilen telefon hatlarını soruşturmak bunu yapmanın bir yoludur. Oldukça verimsiz bu çalışma büyük ihtimalle yeterli gelmeyecektir. Gelişmiş bir yöntem ise arama kayıtlarını izlemektir. Kimin kiminle, ne kadar süreyle konuştuğunu size söylerler. Dolayısıyla, araştırmanız için bir hedefiniz varsa, "meta veri" telefon kayıtlarını sıralayabilir ve büyükanneye yapılan aramalar ile suç ortağı aramaları arasında ayrım yapmaya çalışabilirsiniz. Ya bunun yerine görüşmedeki ses kayıtlarına dayalı olarak, gerçek bir kriminal konuşma gerçekleştiğinde otomatik olarak uyarılsaydınız; veya yeni bir telefon numarasının ortaya çıktığını anında bilseydiniz?

Görünebilirlir bariyerlerini aşma

Sonuç çıktıları

Şu senaryoyu göz önünde bulundurun: İstanbul ofislerindeki iki sunucu arasında yatay hareket olduğunu varsayalım. Bu etkinliği görmenin bir yolu, bu iki cihaz arasındaki ağa dokunmaktır. Ancak bu sadece çok küçük ağlarda mümkün ve pratik olabilir. Bununla birlikte, birçok iletişim, bir yan etki olarak üretilen ağ çıktılarıyla sonuçlanır. Yanal hareket örneğinde, bu, bir aygıtın diğerine erişmesi için etki alanı denetleyicisinden verilen Kerberos bileti olabilir. Bunları gözlemlemek ve derinlemesine ayrıştırmak, NTA sensörlerinin yalnızca nispeten sınırlı sayıda konuma yerleştirilmesi ve buna rağmen geniş bir görünürlük sunması avantajına sahiptir. Bu durumda, Kerberos bileti yani "sonuçtaki çıktı", iletişime ilk elden tanık olmaya gerek kalmadan yanal hareketin kanıtını sağlar. Çoğu durumda, saldırganın bu sonuç olarak ortaya çıkan eserler üzerinde hiçbir kontrolü olmadığını da unutmamak gerekir.

Şifrelenmiş trafik analizi

Şifreleme kullanımının artması, ağ trafiğinin görünürlük ve tespitler için uzun vadeli uygun bir kaynak olmamasının birincil nedeni olarak sıklıkla tartışılmaktadır. Şifrelenmiş trafik analizi, analistlerin tam yüke bakmadan tam yükü analiz ederek tehditleri açığa çıkarmasına olanak tanır[3].

Bu, bir TLS 1.3 dünyasında şifre çözmenin kurallar ve gizlilik sonuçlarını ve bunu yapmanın teknik zorluklarını ortadan kaldırır[4].

[3] https://awakesecurity.com/webinars/ja3-reasons-to-rethink-your-encrypted-traffic-analysis-strategies-webinar/
[4] https://www.zdnet.com/article/snooping-on-https-is-about-to-get-harder-tls-1-3-internet-encryption-wins-approval/

Akıllı Veri Bilimi

Varlık takibi

İlk nesil davranışsal analiz çözümleriyle ilgili zorluklardan biri, davranışların geçici olan IP adreslerine atfedilmesiydi. Tam paket verilerinde mevcut olan daha derin sinyal ile, gelişmiş NTA çözümleri yalnızca takip etmekle kalmaz, aynı zamanda ağdaki varlıkları - cihazları, kullanıcıları, uygulamaları ve diğerlerinin yanı sıra, profillerini de izleyebilir. Makine öğrenimi ve analitik daha sonra davranışları ve daha da önemlisi ilişkileri bu adlandırılmış varlıklarla ilişkilendirebilir. Açıkçası bu varlık görünümü, insan analistler için bir IP adresleri listesinden çok daha anlamlıdır.

Daha iyi bir temel

Çoğu BT ortamı, tamamen meşru nedenlerle sürekli olarak değişiyor. Sürekli yeniden eğitim olmadan, birinci nesil NTA, değişiklikler gerçekleştiğinde yanlış değerlerle sizi yanıltabilir. Ancak yeniden eğitim zahmetlidir ve tamamlanana kadar sizi kör bırakır. Gelişmiş NTA çözümlerinin benimsediği daha iyi bir yaklaşım, ortamdaki varlıkların çoğunluğuna kıyasla bir kuruluşa veya az sayıda varlığa özgü davranışları izlemektir. Modeli oluşturmak için haftalarca veya aylarca beklemek yerine, temeldeki veriler hemen kullanılabilir olduğundan, geçmiş davranışa dayanan geleneksel zamansal istatistiksel modellerle karşılaştırıldığında, bu modellerin öğrenilmesi daha kolaydır. Ek olarak, kuruluş genelinde davranışlar değiştikçe taban çizgisi gerçek zamanlı olarak gelişir. Ve varlık izleme göz önüne alındığında, temel, trafik modellerine ek olarak kaynak ve hedef varlıkların anlaşılmasından da büyük ölçüde yararlanır. Bu daha iyi temel, böylelikle, yukarıdaki örneğimizde olduğu gibi, BT yeni bir yedekleme sistemi sunduğunda anormalliklerin tanımlanmasını önler.

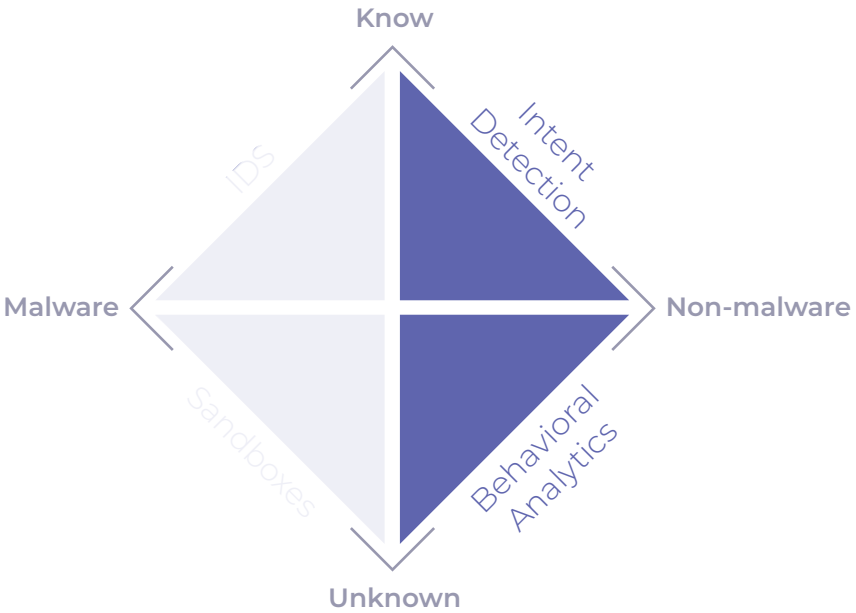
Geniş Kullanım Alanı

Tespit ve Müdahale vs Sadece Tespit

Gelişmiş NTA çözümleri davranışları varlıklara atfettiğinden, yalnızca tespit için değil, aynı zamanda inceleme ve karşı iş akışlarını etkinleştirmek için de zengin bir veriye sahiptir. Analistler artık noktaları bir araya getirmek için DHCP ve DNS günlükleri, yapılandırma yönetimi veritabanları ve dizin hizmeti altyapısı gibi birden çok veri kaynağına bakmak zorunda değil. Bu, özellikle başlangıçta bu veritabanlarında çoğu zaman görünmeyen yönetilmeyen cihazlar için güçlüdür. Her üç kuruluştan ikisinin kapsamlı görünürlükle mücadele ettiği IoT, bulut ve gölge BT çağında[5], güvenlik etkinliği yalnızca bir şeyi ne kadar hızlı tespit ettiğinize değil, aynı zamanda onu ne kadar hızlı ve kararlı bir şekilde izlediğinize, temel nedeni belirlediğinize ve tepki verdiğinize de bağlıdır.

Niyet Tespiti

Tüm bu yeteneklerin sunmak için bir araya getirdiği şey, kötü niyet tespiti dediğimiz şeydir. Örneğin, PowerShell'in Twitter'a bağlanmak için kullanıldığını görüyorsanız ve bu davranış düzenli olarak ortaya çıkıyorsa, büyük olasılıkla bir tür komut ve kontrol kanalı olabilir.



Aslında bu, düşmanın kötü amaçlı yazılım değil, kötü amaçlı Power-Shell gibi önceden var olan bazı araçları kullandığı modern saldırıların tipik bir örneğidir. Bugün, yalnızca en gelişmiş güvenlik ekipleri bu tür etkinlikleri bulabiliyor ve bunu öncelikle manuel avlanma yoluyla yapıyorlar. Adından da anlaşılacağı gibi, bu, bir çıkmaza gelene kadar veya bir şey bulana kadar bir ipucunu takip etmeyi ve ardından işlemi defalarca yinelemeyi içerir. Bu, zaman alıcıdır, yüksek derecede beceri gerektirir ve kolayca kopyalanamaz. İyi niyetli güvenlik ekiplerinin karşılaştığı temel zorluk, çoğu analistin aramak istediklerini sözlü olarak ifade edebilmesi, ancak güvenlik teknolojisi yığınları aracılığıyla

[5] https://www.helpnetsecurity.com/2018/09/11/internal-dysfunction-security-risk/

otomatikleştirilebilecek bir şekilde ifade etmekte zorlanmasıdır. Örneğin, "daha önce karşılaşmadığım bir ülkeden bağlantı görürsem beni uyar" demek bir şeydir. "Herhangi biri bu veritabanı sunucusuna bağlanırsa ve aktardığı veri miktarı tarihsel ortalamanın iki katı ve daha fazlasıysa beni uyar" gibi bir şey ifade etmek çok daha zordur.

Gelişmiş NTA çözümleri, bu süreci otomatikleştirmeye ve çoğu kuruluşun avlanmasını engelleyen beceri ve çaba engelini azaltmaya odaklanır. Bunu yapmak için, yalnızca makine öğrenimini ve davranışsal analitiği değil, aynı zamanda çok özel saldırgan taktikleri, teknikleri ve prosedürlerini (TTP'ler) arayabilen kural tabanlı algılamayı da desteklerler. Kuralların kendilerinin tanımlanması kolaydır ve varlıklar, zaman, protokoller ve diğer ilgili parametreler arasında otomatik olarak ilişkilendirilebilirken, bilinen bir saldırgan öldürme zincirine veya Mitre ATT & CK[6] gibi bir çerçeveye eşlenebilir. Bu, bir araştırmacının veya analistin haftalar veya aylar boyunca olay dizilerini aramasına olanak tanır.

Örneğin, "indirme boyutuyla da eşleşen bir HTTP dosyası indirildikten birkaç dakika sonra başlayan SMB dosya aktarımlarını" arayan bir kural tanımlayabilirsiniz. Örneklerin gösterdiği gibi, kurallar sadece düşük seviyeli ilkel verilerin (örneğin, port ve protokol parametreleri) değil, yüksek seviyeli davranışların (örneğin, internete erişmek için tarayıcı olmayan istemcilerin kullanılması) araştırılmasına izin verir. Bu davranışsal kural mekanizması, bu nedenle daha geniş bir analist popülasyonu için daha erişilebilirken, aynı zamanda geleneksel imzalardan daha sağlam ve daha uzun ömürlüdür.

Kural tabanlı algılamanın eklenmesiyle, gelişmiş NTA çözümleri ayrıca kuruluşa ve içindeki güvenlik ekiplerine görünürlük ve kontrol sağlayabilir. Gartner analisti, Avivah Litan'ın belirttiği gibi, "[Makine öğrenimi] Tedarikçiler kara kutuları satamaz." [7] Bunun yerine, gelişmiş NTA çözümlerini benimseyen kuruluşlar, bu platformları bir veri bilimine ihtiyaç duymadan, eğitim setlerini veya algoritmaları değiştirmek için belirli bir ağın nüanslarına uyarlayabilirler. Ek olarak, bu yaklaşım kuruluşa özgü tehditlerin özel olarak algılanmasına izin verir.

Elbette hiçbir tespit paradigması mükemmel değildir. Makine öğrenimi ve matematiksel analizi üst düzey kurala dayalı yaklaşımlarla birleştirmek, düşük yanlış pozitif ve negatiflerle daha yüksek doğruluk tespiti sağlar. Geleneksel olarak, kuruluşunuz dahilinde kuzey-güney yönünde görülen davranışları (kuruluşunuz ile dış dünya arasındaki etkileşimlerde kendini gösteren tehditler) ve ayrıca doğu-batı yönünü (varlıklar arasındaki etkileşimlerde kendini gösteren tehditler) tespit etmenizi sağlar. Başka bir deyişle, niyet tespiti, saldırgan güvenliğinizi yanlışlıkla veya kötü niyetle tehlikeye atan içeriden biri veya sizin ortamınıza giren ve şu anda ortamınıza giren harici bir saldırgan olsun, aynı şekilde geçerlidir.

Güvenlik ekibinin bakış açısından, algılamak için kullanılan zengin içerik, yanıtı hızlandırmak ve tehdidi araştırmak için diğer sistemlere pivot ihtiyacını ortadan kaldırmak için de kullanılabilir. Ve yeni bir kötü niyetli davranış kalıbı keşfedildiğinde, bunu tespit etmek basitçe yeni bir kural oluşturma ve sistemi otonom olarak sahip olma meselesidir ve ardından davranışı yakalamaktır.

Sonuç

Ağ verileri, varlıkların davranışları hakkında, günlükler veya uç nokta aracıları aracılığıyla çoğaltılması imkansız olan temel gerçeği sunar. Saldırganlar aracıları devre dışı bırakabilir, günlüklerden veya dosya sistemlerinden izlerini silebilirler, ancak bir paketi "göndermeyi geri alamazlar" ve sonuçta ortaya çıkan sonuçlardan kaçınamazlar. Düzgün bir şekilde donatılan ağda, hem gerçek zamanlı hem de geriye dönük algılamaya izin veren bir bellek de vardır. Ağ işleme, analitik ve güvenlik araştırmalarındaki son gelişmeler, geleneksel ağ güvenliğinin birçok zorluğunu ortadan kaldıran yeni bir algılama ve yanıtlama yetenekleri çağını mümkün kılmıştır. Gelişmiş ağ trafiği analizi çözümleri, uzun kurulum süreçleri ve eğitim / yeniden eğitim olmadan hızlı bir şekilde değer sunmak için şirket içinden buluta, sanala ve SaaS'ye kadar gelişen ağdan yararlanıyor. Her kuruluş, bunları güvenlik mimarisinin bir parçası olarak dikkate almak zorundadır.

[6] https://attack.mitre.org/wiki/Main_Page
[7] https://blogs.gartner.com/avivah-litan/2017/07/27/can-we-trust-black-box-machine-learning-when-it-comes-to-security-or-is-there-a-better-way/

AWAKE

Daha ayrıntılı bilgi için awakesecurity.com'u ziyaret edebilir veya Awake ürünlerinin Türkiye Distribütörü Exclusive Networks'ten bir uzmana danışabilirsiniz.

EXCLUSIVE NETWORKS

About Awake Security

Awake Security is the only advanced network traffic analysis company that delivers a privacy-aware solution capable of detecting and visualizing behavioral, mal-intent and compliance incidents with full forensics context. Powered by Ava, Awake's security expert system, the Awake Security Platform combines federated machine learning, threat intelligence and human expertise. The platform analyzes billions of communications to autonomously discover, profile and classify every device, user and application on any network. Through automated hunting and investigation, Awake uncovers malicious intent from insiders and external attackers alike. The company is ranked #1 for time to value because of its frictionless approach that delivers answers rather than alerts.