Kaspersky for Business

KASPERSKY lab

Büyük Ölçekli İşletmeler İçin Uç Nokta Tespit ve Yanıt Çözümlerine Yönelik Yatırım Rehberi 2017-2018

www.kaspersky.com.tr

#truecybersecurity

İçindekiler

Giriş

Her kuruluşun en önemli iş hedeflerinden birisi, karar verme sürecinde güvenebileceği verilerin ve sistemlerin sürekli kullanılabilirliğini korumaktır. Sürekli gelişen tehdit ortamı, üst yönetim düzeyine kadar tüm birimlerin siber güvenlik konusuna odaklanmalarına neden olmaktadır. BT operasyonel ve güvenlik ekipleri, güvenlik olaylarına ve veri ihlallerine yanıt olarak kapsamlı ve birleştirici bir yaklaşım göstermelidir.

Siber güvenlik, artık işletmelerin başarısını sağlayan iş sürekliliği arayışında üst düzey yönetim tarafından tanınan "İlk 3" öncelikten biri haline gelmiştir.

Günümüzün iş liderleri, kuruluşlarına özel siber tehdit ortamını daha iyi anlamalıdır. Liderler kendilerine aşağıdaki gibi sorular sormalıdır:

- Kuruluşum endüstri sektörümüze ve şirketimize yönelik temel tehditleri ve güvenlik risklerini biliyor mu?
- Siber saldırıları hızlı bir şekilde tespit edip durdurabilir miyiz?
- Genel iş geliştirme stratejimiz kapsamında siber riskleri azaltmak için kendimizi nasıl konumlandırıyoruz?

Topun ağzındaki uç noktalar

Sunucularınız, iş istasyonlarınız ve cep telefonlarınız gibi kurumsal uç noktalar, iş süreçlerini oluşturan ve uygulayan veriler, kullanıcılar ve kurumsal sistemler arasındaki sinerjinin merkezidir. Çok sayıda ayrı cihazdan oluşan bu merkez, hem iş hem de güvenlik açısından her ağın en önemli unsurudur.

Bu uç noktaları korumak ve uç noktaların altyapınıza yasa dışı giriş noktaları olarak kullanılmalarını önlemek için bilgi güvenlik ekiplerinizin; gelişmiş algılama, tehdit avı, Risk Göstergesi tarama, zararlı yazılım analizi, adli bilişim, global tehdit istihbarat uygulaması ve resmi bir Olay Yanıt sürecinin oluşturulması ile ilgili süreçleri ve teknolojileri benimsemesi gerekir.

Peki bunun için nereden başlanılmalıdır? Modaya uyarak doğrudan gelişmiş makine öğrenimi mi benimsenmeli? Tehdit avı becerileri mi iyileştirilmeli? Yoksa izleme ve Güvenlik İşlemleri Merkezi'ni büyütmeye mi odaklanılmalı? En iyisi bu alanların tamamını ve daha fazlasını kapsayan yeni Uç Nokta Tespit ve Yanıt (EDR) çözümlerini tercih etmektir. Peki bir EDR çözümünden tam olarak neler bekleyebilirsiniz ve hangi EDR çözümünü seçmelisiniz?

Bu Belge, size en iyi hizmeti sağlayacak EDR çözümünü seçmenize yardımcı olabilir. Hedefimiz, piyasada bulunan çeşitli EDR becerileri arasındaki önemli farkları vurgulamak ve işletmenizde iş sürekliliğini ve güvenliğini güvence altına almak için en değerli teknolojileri belirlemenize yardımcı olmaktır.

Uç Noktalarla İlgili Her Şey Tespit ve Yanıt

Uç nokta güvenliğine yeni yaklaşım

Saldırıları önlemek için çevrenizi koruyun. Bu, her zaman makul bir strateji olmuştur. BT çevreniz iyi korunuyorsa uç nokta koruması, yalnızca genel güvenlik stratejinizde ek bir katman olur.

Ancak mobil cihazlar, bağlı cihazlar (Nesnelerin İnterneti) ve bulut bilişim gibi teknolojiler nedeniyle bırakın BT çevrenizi korumayı tanımlamak bile çok zor olduğu için bu yaklaşım yeterli değildir. Ayrıca tehditlerin gelişmesi, savunmaya yönelik çevre temelli yaklaşımı kullanılamaz hale getirmiştir.

Hedefli saldırılar, karmaşık sızma tekniklerindeki keskin artış, kötü amaçlı dosyasız yazılımların ve yasal yazılımların kullanımı, normal kullanıcıların çalınan kimlik bilgileri, yasal hakların kullanımı, güvenlik politikaları sorunlarının suistimal edilmesi ve yanlış yapılandırmalar... Bu gibi sorunların tamamı, kuruluşların entegre güvenlik çözümlerinin ve stratejilerinin önemini anlamasını sağlamıştır. Bu farkındalık, SIEM uygulamasının ve Güvenlik İşlem Merkezleri'nin (SOC'ler) büyümesine yol açmıştır. Kurumsal siber güvenlik proaktif, çok yönlü ve yüksek uzmanlığa sahip hale gelmek zorunda kalmıştır.

Değişen dünya, yeni bir uç nokta güvenlik yaklaşımını benimsemeye hazırdır. Uç noktalar yeniden odak noktası haline gelmiştir. Her zaman her uç noktasının kendi güvenlik çevresini gerektirdiğini anlayan ileri görüşlü BT Departmanları olmuştur. Ancak kısmen bu yaklaşımı **benimsemeyen** ve her cihaz üzerinde yeterli görünürlük elde edemeyen kuruluşlar nedeniyle genel güvenlik düzeyi düşmüştür ve uç noktalar siber suçluların ilk ana hedefi olmaya devam etmektedir.

Daha proaktif olma

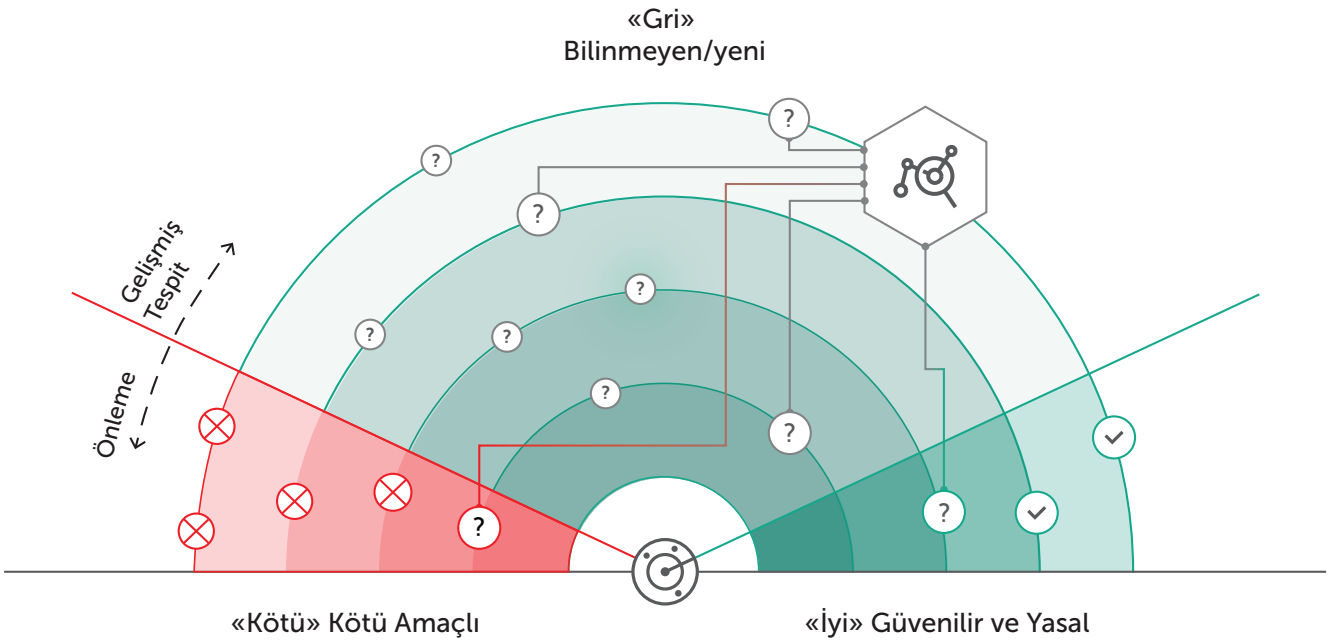
Son zamanlarda düzenleyici kuruluşlar, sürekli izlemeyi ve ağınızdaki her uç noktada olay kaydı gerektiren yeni gereklilikleri (GDPR, PCI DSS vb.) zorunlu hale getirmektedir. Birçok kuruluşun, mevcut güvenlik çözümü tarafından kaydedilen olay/olay sayısı artmaktadır. Bu nedenle kaydedilen her olayın doğrulanması ve analiz edilmesi, başlı başına bir sorun haline gelir. Bu görevleri yerine getirmek için Tersine Mühendislik, Kötü Amaçlı Yazılım Analizi, Adli Bilişim ve Olay Yanıtı'nda gerekli becerilere sahip güvenlik uzmanlarının çok değerli ve az sayıda olması işi daha da zorlaştırır.

Bu noktada, gelişmiş tehditlere odaklanan birçok güvenlik süreci ve SOC izleme yaklaşımlarının çoğu temelde uyarı esaslıdır ve tepkiseldir. Güvenlik görevlileri, güvenlik analistini uyarmadan önce bir ihlal kanıtı elde etmeyi bekler. Daha sonra olay yanıt ekibi, harekete geçer. Olay yanıt ekipleri, en iyi ihtimalle saldırının izlerini "ölüm zincirinin" en son aşamasında tespit eder. En kötü ihtimalle ise hasarı belirlemek için yalnızca beklemek zorunda kalırlar. Bazen bu bekleyiş, sistemin ihlal edilmesinden aylar sonra sona erebilir. Bu yaklaşım, kesinlikle tatmin edici değildir. Dolayısıyla kuruluşlar, özellikle proaktif olay tespiti ve yanıtı açısından güvenlik süreçlerini gözden geçirmektedir.

Peki bu durum, uç nokta çözümlerini nasıl etkiler?

Tehdit Avı, son derece nitelikli ve deneyimli güvenlik uzmanları tarafından yürütülen tehdit arama özelliklerini kullanarak kurumun içinde gizlenen gelişmiş tehditlerin ortaya çıkarılmasına yardımcı olur.

Yeni nesil uç nokta çözümleri, kuruluşun karşılaştığı yeni tehditlerin etkili bir şekilde tespit edilmesine ve bilinmeyen ya da tanımlanamayan tehditlerin gizlenebileceği "gri bölgedeki" olayların kontrolüne ve analiz edilmesini odaklanır. Bu noktada proaktif "tehdit avı" devreye girer.



Uç nokta korumasının sınırlarını aşma

Etkili tehdit avı, doğrudan gelişmiş bir Güvenlik İşlemleri Merkezi'nin becerilerine bağlıdır. Dışarıdan satın alınan güvenlik çözümlerinin yükseltilmesi yeterli değildir. Yeni gereksinimler, geleneksel Uç Nokta Koruması (EPP) çözümlerinde uygulanamaz. Bu gereksinimler, çözüme uyum sağlayamaz veya etkili şekilde çalışamaz.

Geleneksel Uç Nokta Koruması ile etkili bir şekilde kapatılan bazı önemli konulara ve uç nokta güvenliğinin günümüzde karşılaştığı yeni zorluklara göz atalım:

Bu yeni zorluklarla nasıl mücadele edilebilir?

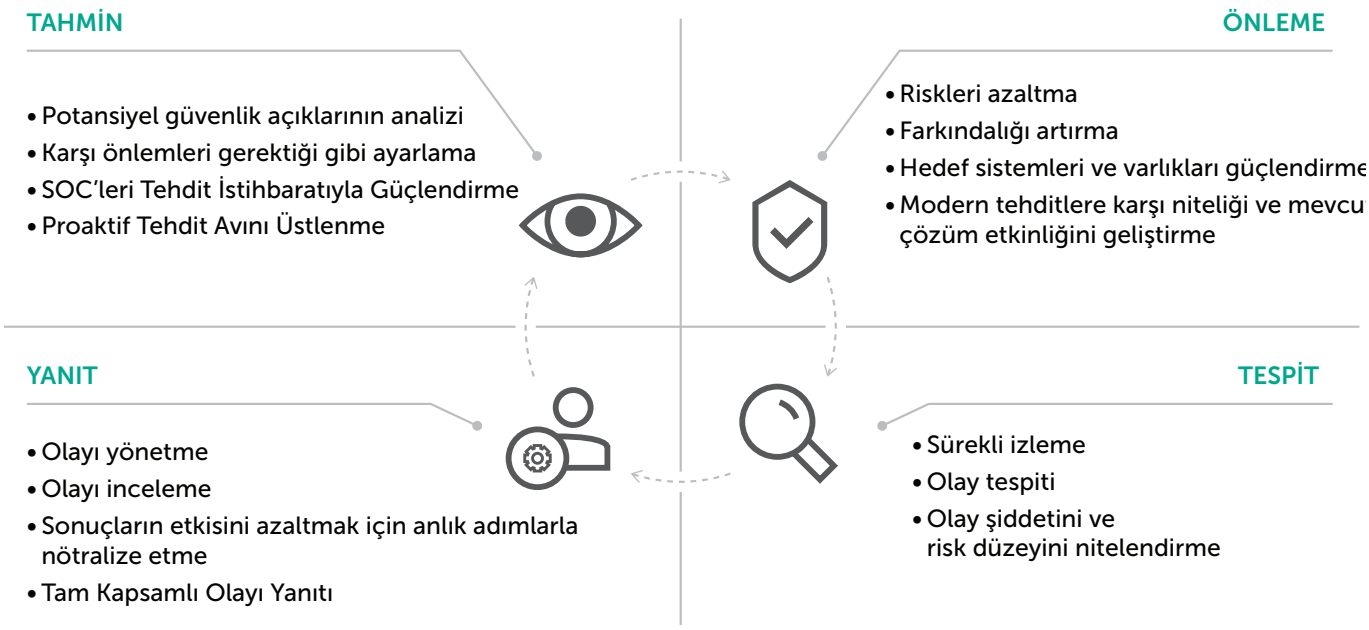
Geleneksel EPP çözümlerinin kapsadığı kontrol ve koruma sorunları:	Uç nokta güvenliği için yeni gelişmiş zorluklar:
Fidye yazılımı ve şifreleyiciler dahil olmak üzere mevcut tehditlere karşı otomatik koruma (hem önleme hem de geri alma) sağlama	Tüm ağda gerçek zamanlı olarak Risk Göstergeleri gibi izinsiz giriş kanıtlarını proaktif bir şekilde arama
Web/uygulamalar/cihazlar için güvenlik denetimlerini merkezi olarak yönetme ve uygulama	İzinsiz giriş yapan kişinin ciddi hasarlara yol açma şansı olmadan izinsiz girişi tespit etme ve düzeltme
Güvenlik açığı değerlendirme ve düzeltme eki yönetme süreçlerini merkezi olarak yönetme	Gerçek zamanlı olarak uç noktada neler olduğunu anlamak için ağ güvenlik kontrollerinden gelen uyarıları ilişkilendirme
Cihazlardaki kurumsal verileri ve bilgileri koruma	Diğer güvenlik çözümlerinin tespit ettiği uyarıları ve olası olayları doğrulama
Uç nokta düzeyinde web ve e-posta koruma ilkelerini dağıtma	Binlerce uç noktada olayları hızlı bir şekilde inceleme ve merkezi olarak yönetme
Uç nokta kullanıcılarına, kendi ihtiyaçlarına göre hazırlanmış belirli güvenlik etki alanı setleri sağlama	Rutin güvenlik ekibi işlemlerini otomatik hale getirerek olay yanıt sürecini (manuel işlemler, 3. seviye beceriler, aşırı uyarı yükleme vb.) daha ucuz hale getirme

Uç nokta siber güvenlik stratejiniz: uyarlanabilir, gelişmiş, öngörücü

Tespit etmesi hatta bazen yok edilmesi bile zor olan hedefli saldırılar ve gelişmiş tehditler kapsamlı ve uyarlanabilir bir güvenlik stratejisi gerektirir.

En etkili Uyarlanabilir Güvenlik Çerçeveleri'nden biri olan bu çerçeve, Gartner tarafından tanımlanan uygulanabilir güvenlik mimarisi üzerine kurulmuştur. Gartner yaklaşımı, dört önemli alana dayalı bir etkinlik döngüsü sağlar: Önleme, Tespit Etme, Yanıtlama ve Tahmin Etme.

- **Önleme:** gelişmiş tehdit riskini azaltmak için yaygın tehditlerin engellenmesi ve temel sistemlerin güçlendirilmesi
- **Tespit Etme:** hedefli bir saldırının veya mevcut bir ihlalin belirtisi olabilecek etkinliklerin hızlı bir şekilde keşfedilmesi
- **Yanıtlama:** tehdidi tam olarak kontrol altına alma, incelemeler gerçekleştirme ve saldırılara uygun şekilde yanıt verme
- **Tahmin Etme:** yeni hedefli saldırıların nerede ve nasıl ortaya çıkabileceğini öğrenme



Uyarlanabilir Güvenlik Modeli

Bu yaklaşım, başta uç noktalara yönelik sistemler olmak üzere geleneksel önleme sistemlerinin tespit teknolojileri, tehdit analizleri, yanıt kabiliyeti ve önleyici güvenlik teknikleriyle birlikte çalışması gerektiğini öne sürer. Bu çalışma şekli sayesinde şirketin karşılaştığı yeni zorluklara karşı sürekli olarak uyarlanabilen ve yanıt verebilen bir siber güvenlik sistemi oluşturulur.

Çok katmanlı ve önleme tabanlı teknolojiler, hedefli saldırılara karşı koruma sağlamak için bu yeni ve proaktif yaklaşımın temel bir unsurunu oluşturur. Ancak, saldırgan yeterince motive olmuşsa veya başarılı bir saldırı gerçekleştirmek için üçüncü bir kişi tarafından tutulduysa yalnızca önleme tabanlı bir yaklaşım yeterli olmaz. Ayrıca mevcut manuel işlemleri basitleştirirken ve yanıt araçlarını otomatik hale getirirken tehditleri hızlı bir şekilde tespit edebilme, kararlar alma ve sızma olasılığını tahmin edebilme becerilerine sahip olmalısınız.

Uç Nokta Tespit ve Yanıt (EDR) Teknolojisini Tanımlama

EDR benzeri bir çözümün temel özellikleri

Gördüğümüz üzere Gartner, EDR çözümlerinin şu ana özelliklere sahip olması gerektiğini belirtir:

- güvenlik olaylarını tespit etme
- ağ trafiğinin veya işlem yürütmenin uzaktan denetlenebileceği şekilde olayı uç noktada kontrol altına alma
- güvenlik olaylarını inceleme
- uç noktaları virüs bulaşmadan önceki haline getirme

Uç Nokta Olay Tespiti

Uç nokta etkinlikleri ve nesneler, politika ihlallerini **izleyerek** veya dışarıdan beslenen gizliliği bozma göstergelerini (IOC'ler) doğrulayarak güvenlik olaylarını tespit edin

Olay İncelemesi

Güvenlik olaylarını inceleyin.
İnceleme işlevi oluşan tüm teknik değişiklikleri ve işletmeye etkisini belirlemek için tüm birincil uç nokta etkinliklerinin **geçmişe dönük** zaman çizelgesini içermelidir

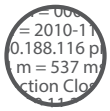
(öncelik yükseltme, yayma, dışarı sızma, mümkünse C&C ve kötü amaçlı özniteliklerin jeo konumu)

Olay Sınırlandırma ve Yanıtı

Olayı uç noktada **tutun** ve uç noktaları bulaşma öncesi duruma **getirerek düzeltin**

Kötü niyetli dosyaları kaldırın, geri alın ve diğer değişiklikleri onarın veya diğer araçların uygulaması için kullanılabilecek düzeltme talimatları da oluşturulabilir

Adli Bilişim Verilerini Toplama

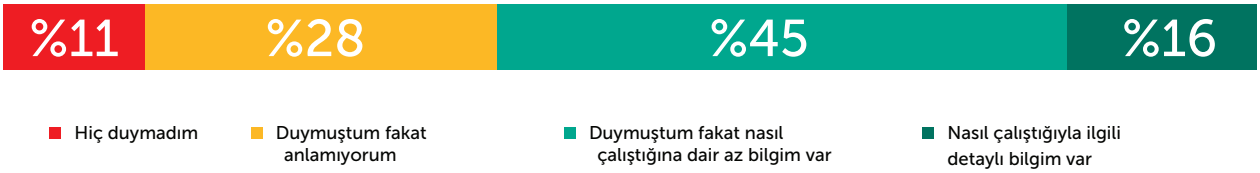


Daha fazla detay için veri kümelerini, RAM dökümleri, HDD anlık görüntüleri vb. **toplayın**

Kuruluşlar EDR'nin işleyişini ne kadar iyi anlıyor ve bu teknolojiler iş sürekliliğine ne kadar katkı sağlıyor? 2016 yılında kurumsal firmalarla ilgili olarak düzenlenen bir Kaspersky Lab araştırmasında bazı rahatsız edici sonuçlar elde edildi.

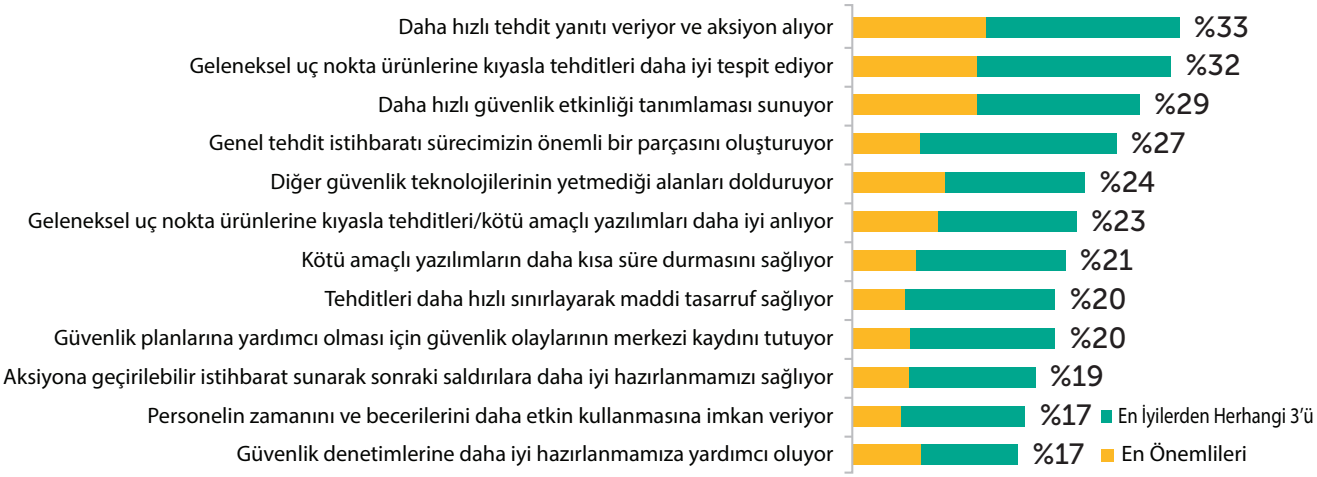
Anket sorusu: "EDR sınıfı çözümleri ne kadar iyi biliyorsunuz?"

Yanıt:



Kaynak: 250'den Fazla Çalışanı Olan İşletmelerdeki BT Uzmanları

Aynı zamanda görüşülen şirket temsilcileri, kendi beklentilerini ve kurumlarındaki EDR çözümlerinin kullanımından elde etmek istedikleri sonuçları açıkça belirtti:



Anlayış ve net beklentiler konusundaki bu eksiklik, ciddi bir sorunu yansıtır. EDR çözüm sağlayıcıları, doğal olarak bu beklentileri karşılamayı ister. Bu nedenle deneme aşamasında heyecan verici görünen ve çok fazla şey vaat eden "yok etme özellikleri" geliştirirler. Ancak bu özellikler, genellikle müşterinin yeni veya mevcut olay yanıtı, inceleme ve tehdit avı süreçlerine eklendiğinde kullanışsız ve pahalı hale gelir.

Sonuç olarak EDR, bazı çevrelerde şüphe uyandırmaya başlamıştır.

Uç Nokta Tespit ve Yanıt çözümlerinin yükselişi ve düşüşü

Maalesef ki EDR çözümlerini ilk benimseyen firmalar, her zaman teknolojiye meraklı firmalar değildi. İlk EDR çözümlerinden birçoğunda eksiklikler olması, bazı müşterilerin hayal kırıklığına uğramasına neden oldu.

Ne yazık ki günümüz piyasasında mevcut tüm temel işlevleri ve olası EDR teknolojileri çeşitlerini inceleyen karşılaştırmalı bir analiz veya bağımsız bir rapor bulunmamaktadır. Ayrıca, henüz olgunlaşmamış olan bu pazardaki birçok "birinci nesil" ürün, başlangıçta uzmanların ve kurumların beklentilerini karşılayamamıştır.

Çoğu çözüm karmaşık işlevsellik yerine bazı "yok etme özellikleriyle" piyasaya çıkmıştır. İlk başlarda EDR; ağ güvenliği tehdit istihbaratı, tehdit avı, kötü amaçlı yazılımlara karşı koruma, olay yanıtı ve adli bilişim özelliklerini birleştirme ve otomatikleştirme özelliğine sahip entegre bir çözüm yerine yalnızca bir grup analiz ve araştırma aracından oluşuyordu. Bu teknolojik araç kitinin, sunduğu özelliklere göre çok pahalı bir çözüm olduğu ve ortalama bir güvenlik uzmanının bu araçların kullanımında ustalaşması için son derece zor özelliklere sahip olduğu ortaya çıktı.

Bazı EDR çözümleri ise verimlilik vaatlerini de karşılayamadı. Bir EDR çözümü, kötü amaçlı yazılım olayına yanıt verirken uç noktalardan bilgi (imzalar ve kötü amaçlı yazılım davranışı) toplar ve bu bilgiler daha sonra gelecekteki bulaşmaları belirlemek için kullanılabilir. Ancak çözüm, tespit teknolojileri ve güvenlik sistemleri ile sıkı bir şekilde entegre edilmezse çakışma ve çoğalma riski artar. Bu durum, aslında verimliliği ve etkililiği artırmak yerine daha fazla manuel işlem üretir ve iş akışını aksatır. EDR, güvenlikle ilgili verilerin saklandığı ek bir depo haline gelir. Bu veriler, kendi başına olayın nasıl başladığını ve yeniden olmasının nasıl engellenebileceğini gösteremez. Kök nedenin çözümü iş akışına yerleştirilemezse kuruluş, kesin bir çözüme ulaşamaz ve olayın yeniden gerçekleşme riski azaltılamaz.

Başlangıçta piyasada bulunan çözümlerin bir başka eksikliği ise APT'leri keşfetmek veya incelemek için tasarlanmamış olmalarıdır. EDR sahipleri, APT'leri incelemek için bu olaylarda genellikle satıcının çalışanları olan dış uzmanlar kullanmak veya pahalı ek eğitimler satın almak zorundadır. Tespit edilen her ihmal için bir olay yanıt ekibine başvurma zorunluluğu, orijinal EDR çözümünün uygun maliyetli olduğu konusunda şüphe uyandırır.

Son zamanlarda belirli günlüklerin ve verilerin kurulu aracılar veya merkezi depolar yerine satıcının bulut çözümüne aktarıldığı EDR bulut çözümleri yaygınlaşmaya başlamıştır. Ancak bu akım, daha fazla olayın üretilmesine ve daha yavaş tepki sürelerine (ve bazen hiç tepki verilmemesine) yol açmıştır.

Ancak, bu sorunların birçoğu geçmişte kalmıştır. Şu anda EDR piyasasını izleyenler, ilk kullanıcıların deneyimlerini düşünerek yatırımlarının olası sonuçları konusunda ön yargılı olmamalıdır. Günümüzde pazar büyümüş ve olgunlaşmıştır.

Peki günümüzde bir EDR'den neler beklemelisiniz ve hangi etkenleri göz önünde bulundurmalısınız? EDR projenizi başlatırken göz önünde bulundurmanız gereken 5 zorluğa göz atalım.

EDR projesi başlatılırken en sık karşılaşılan 5 zorluk

Yeni bir teknolojiyi veya bilinmeyen süreçleri benimseyen kuruluşlar, mutlaka bazı yeni zorluklarla karşılaşır. EDR çözümleri, geleneksel EPP çözümlerinden daha pahalıdır. Bu nedenle SIEM veya adli bilişim araçlarının masraflarıyla karşılaştırıldığında EDR yatırımınızı katma değer açısından makul göstermek karmaşık bir iş haline gelebilir.

Kurumsal düzeydeki bir EDR çözümünün temel işlevi, **güvenlik ekibine soru odaklı incelemeler yapma becerisini sağlamasıdır.** Görünürlük elde etmek için tehdit avı ipuçları yinelemelidir ve sorular ya da hipotezlerle başlar. İlk soru veya hipotez, siber ölüm zincirinin adımlarına bağlı olarak "Veri sızdırma veya kötü amaçlı yazılım iletişimi gerçekleşiyor mu?" veya "Dış bir etki alanına şüpheli bir bağlantı varsa bağlantı muhtemelen ağın bu kısmından geçiyordur. Peki bağlantı hangi uç noktadan ve süreçten kuruluyor?" gibi bir soru olabilir.

EDR çözümü, bu özellikleri sunmak için, **veri toplama** ve **depolama özelliklerinin** yanı sıra **incelemeye yardım işlevine** sahip olmalıdır. Ayrıca, **olay bulma** hem otomatik hem de manuel unsurları içermelidir. Son olarak ilk olay tespit edildiğinde güvenlik ekibi ve tehdit yanıt ekibi tehdidi **kolayca kontrol altına almak**, uç noktaları **onarmak** ve belirli etkinliklerin gerçekleşmesini **önlemek** için gerekli araçlarla donatılmış olmalıdır.

Şimdi kuruluşların gelişmiş EDR çözümlerini seçerken veya mevcut Uç Nokta Güvenlik çözümlerini Tespit ve Yanıt açısından geliştirmeye çalışırken dikkate alması gereken 5 yaygın zorluğa göz atalım.

1

Uç nokta verileri: çok fazla görünürlük

Uç nokta korumasının tüm biçimleri, yeni verilerin toplanması, depolanması ve analizi ile başlar. Teorik olarak ne kadar çok veri toplayabilirseniz avantajınız o kadar artar. Aynı teori geçmişte SIEM sistemleri için de geçerliydi. Ancak toplanan büyük hacimli verileri yorumlamak için EDR operatörü, ilgili bağlama da ihtiyaç duyar. Örneğin, kötü bir etki alanına giden kötü amaçlı bir bağlantının hızlı bir şekilde keşfedilmesi, bu durumun hangi uç noktadan kaynaklandığı, işlemin nasıl başlatıldığı, kök nedenin ne olduğu ve hangi varlıkların etkilenmiş olabileceği bilinmediğinde daha az değerlidir.

Piyasadaki gelişmemiş EDR çözümleri bazı verileri toplar, ancak doğru bağlamı sağlamaz. Örneğin hangi makinelerin belirli bir karma toplamına sahip bir dosyayı içerdiğini hızlı bir şekilde operatöre bildirebilir ancak bu dosyanın makinelerde nasıl ortaya çıktığına dair bilgi vermez. Oluşturulan işlemlerin bir listesi, herhangi bir görselleştirme olmadan nesne ve etkinlikler için sağlanabilir. Normal olmayan davranışlar veya sapmalarla ilgili karmaşık uyarılar sağlanabilir ancak temel taramalar ve kararlar sağlanmaz.

Bazı çözümler, uç noktalardan gelen tüm verileri toplar, sonra bu verileri doğrudan arayüze yansıtır. Bu çözümler, doğrudan veritabanı için bir pencere işlevi görür. Operatör, güvenlik uzmanlığının yanı sıra bir veri bilimci veya büyük veri uzmanı değilse bu ham verilerden yola çıkarak bilinçli bir karar vermesi mümkün değildir.

Genellikle bu sistemler, birisi tarafından doğrulanmak zorunda olan binlerce ileti ve milyonlarca uyarı oluşturur. En büyük kuruluşlarda bile izleme ve yanıt ekibi, 50-60'dan fazla orta-yüksek öneme sahip olayla aynı anda ilgilenemez. Sonuç olarak, her şeyi bulan bir çözüme sahip olmamıza rağmen bu çözüm bulduğu sonuçlarla ilgili neredeyse hiçbir işlem yapılamaz. Çok fazla veri olmasına rağmen bunlar anlamayı sağlamak için yeterli değildir.

Çözüm olarak uyarıları güvenlik ekibiniz ve harici yönetilen güvenlik hizmetleri tedarikçisi ile paylaşabilirsiniz. Ancak bunun için doğru eğitime ve uzmanlığa sahip bir tedarikçi bulmanız gerekir. Ayrıca olay önceliklendirmesi olmadan bu çözüm, yüksek miktarda bir yatırım gerektirebilir ve kritik olmayan uyarılarda kaynakların boşa harcanmasına neden olabilir. Bir başka sorun ise tüm yönetilen güvenlik hizmetleri tedarikçilerinde görülen güven, veri güvenliği ve uyumluluk kısıtlamaları konularıdır.

Öneriler:

- Yalnızca uyarılarla riski otomatik olarak açığa çıkarabilmenizi sağlayan çözümleri değil aynı zamanda derin özelleştirme sağlayan çözümleri arayın. Bu özelleştirmeye farklı kullanıcı rolleri yapılandırmak, VIP grupları belirlemek, hızlı bir şekilde beyaz liste oluşturmak gibi özellikler dahil edilebilir. Bu sayede önemli olan uyarıları doğru bir şekilde vurgulayabilir, önemsiz uyarıları azaltabilir ve harici yönetilen güvenlik hizmetleri tedarikçisiyle yalnızca önemli bilgilerin paylaşıldığını denetleyebilirsiniz.
- Kuruluşunuzda ne ölçüde veri analizi yapmayı beklediğinizi ve ne kadar çok veriyi depolayacağınızı ve işleyeceğinizi düşünün. Şirket içinde terabaytlarca veri saklamaya hazırlanmak, büyük miktarda ek donanım masrafı anlamına gelebilir.

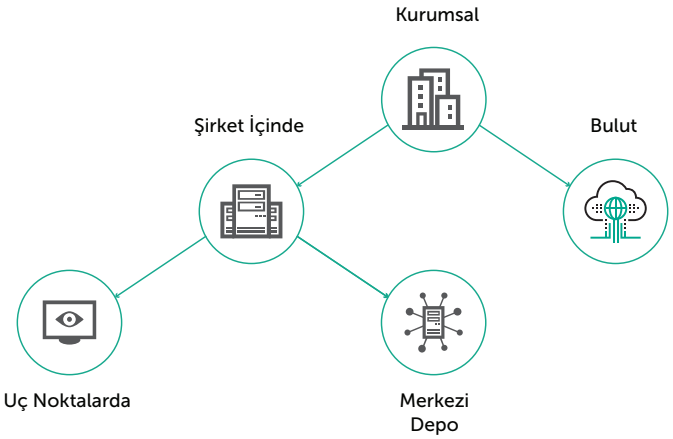
2

Toplanan ve depolanan verilerin sorumluluğu

Verilerle ilgili bir diğer önemli özellik, verilerin toplanma ve depolanma şeklidir. EDR satıcısına sormanız gereken sorular şunlardır:

- Ne kadar veri depolanıyor ve neden?
- Hangi veriler depolanır?
- Nerede depolanır?

Birkaç olası depolama yaklaşımı vardır:



Şimdi onlara daha yakından bakalım.

Bulut

Birçok satıcı verileri depolamak ve hatta EDR aracılarını (diğer adıyla MDR) yönetmek için bulut çözümleri sunar. Bu çözümler, uygun olmakla birlikte herhangi bir zamanda yükleyebilecekleri veri miktarıyla sınırlıdır. Bu, aynı zamanda kuruluşun dışına veri aktaran açık bir kanalın bulunması anlamına gelir ki bu durum bazı ortamlarda sorunlara yol açabilir. Bu seçeneği incelerken sorulacak sorular şunlardır:

- Güvenlik verilerini ortak bir buluta göndermeye hazır miyiz? Çözümü ne kadar kontrol edebileceğiz?
- Verilerimi depolayacak satıcı veya bulut sağlayıcısı (bu üçüncü bir taraf olabilir) güvenilir midir? Sağlayıcının kendi siber güvenlik hizmetleri ne kadar iyidir?
- Bu hizmeti kullanmak, dahili güvenlik standartlarına ve/veya düzenleyici gerekliliklere uygunluğu ihlal edebilir mi?
- Çözüme yalnızca önemli olmayan az miktarda veri gönderilirse çözüm ne kadar etkili olabilir?

Aracıda

Her cihazda bir yerel önbellek, ağır depolama ve bulut arasında bir uzlaşma sağlar. Bu yaklaşım, ağ üzerinde daha az etkiye sahiptir ve çok sayıda aracı aynı anda desteklenebilir. Önemli bilgiler, uç nokta önbelleğine kaydedilir ve tüm analizler sorgu yoluyla gerçek zamanlı olarak gerçekleşir. Ancak merkezi olmayan depolama, bilgileri analiz etmek ve yanıtlamak için her zaman en hızlı ve en etkili yöntem değildir. Örneğin, ağın alt bölümü kullanılamıyorsa etkilenen makinelerden gelen verileri genel analize dahil etmek mümkün olmayacaktır.

Merkezileştirilmiş şirket içi depo

Tüm önemli bilgiler toplanır ve depoya sahip özel bir sunucu tarafından analiz edilir. Tüm görevleri, yerel veritabanı ve çözümleme araçları (örneğin, bir korumalı alan) yerine getirir. Bu yerel yaklaşım birçok avantaja sahiptir. Veriler, teorik olarak aracılı depolamada olduğu gibi, güvenliğin riskli olduğu cihazlarda depolanmaz. Bilgisayar kaynakları üzerinde herhangi bir yük yoktur. Uç nokta sorgularını ve "hızlı arama" işlemini veritabanının üzerinde gerçek zamanlı olarak gerçekleştirebilirsiniz. Bunun gibi şirket içi çözümler, özellikle kuruluş dışına veri aktarımının, düzenlemeler veya güvenlik standartları tarafından engellendiği yerlerde kullanışlıdır.

Öneriler:

- Bulut depolama için bulut EDR sağlayıcınızı veri gizliliği ve kontrol açısından değerlendirin
- Hassas ortamlar ve düzenlemelere uyumluluk nedeniyle dışa veri aktarımı konusunda potansiyel kısıtlamaların olduğu durumlar için şirket içi, tamamen izole uygulama ve tehdit istihbaratının özel teslimi seçeneklerini değerlendirebilirsiniz.
- Aracı tabanlı veri depolaması için bir uç nokta kullanılamadığında veya saldırgan tarafından ele geçirildiğinde ne olacağını kontrol edin (aracının kendisi, bilgisayar ve veriler nasıl korunuyor)
- Şirket içi çözümler için dahili veri depolama kapasitesini ve her cihazdan gönderilen veri miktarını kontrol edin.

Aracı sayısı donanım gereksinimlerini belirleyecektir. Bir EDR çözümü yüz binlerce aracıyı desteklemek için yalnızca küçük bir sunucu gerektiriyorsa tuhaf olan bazı şeyler vardır. Ortalama olarak bir uç nokta, günde yaklaşık 10 megabaytlık kullanışlı telemetri oluşturur. Dolayısıyla 10.000 adet düğümünüz varsa günde 100 gigabayt veya geçmişi kapsayan bir aylık veritabanı için 3 TB veri elde etmeniz gerekir.

3

Tespit: manuel tehdit yakalama/otomatik motorlar

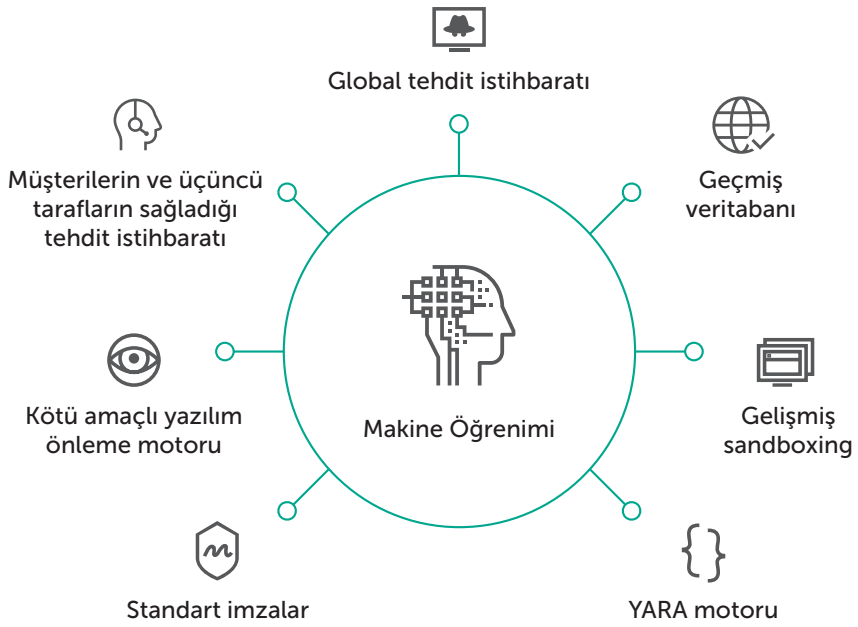
Veri ve depolama ile ilgili konuları değerlendirdikten sonra, veri analizine göz atalım. Satıcınızın araç kitleri, veritabanları ve kaynakları ile manuel olarak gerçekleştirilen tehdit avı ve izleme ile doğrudan EDR sisteminiz tarafından otomatik olarak gerçekleştirilen tehdit avı ve izleme becerilerini karşılaştıralım. Saldırı ne kadar erken tespit edilirse finansal kayıplar ve yaşanacak kesintiler de o kadar azalır. Bu nedenle tespitin hızı ve etkililiği büyük önem taşır. Tek başına manuel tespit teknikleri, genellikle en hızlı veya en etkili yaklaşım değildir. Birçok satıcı, sözde "gelişmiş tespit teknikleri" (uç noktalarda gerçek zamanlı risk göstergesi taraması ve merkezi olarak depolanan adli bilişim veritabanlarında hızlı arama) sağlayarak olay keşif becerilerine otomatik bir unsur ekler.

Toplanan verilerinizden tam olarak faydalanmak için analistlerinizin ağ üzerindeki riskleri ve tehditleri ortaya çıkarmasına yardımcı olacak güçlü otomatik veri analiz tekniklerine ihtiyaç duyarsınız. Çok boyutlu ve çok katmanlı analiz, yalnızca sürekli olarak yeni güvenlik olaylarını değil aynı zamanda uygulanabilir istihbarat bilgilerini de sağlamalıdır. Böylece güvenlik ekibiniz doğru kararları verebilir ve kritik olmayan olaylara gereksiz zaman harcamaz.

Bu tür gelişmiş tespit ve tehdit bulma teknolojileri, yalnızca kötü niyetli etkinlikleri açığa çıkarmakla kalmamalı aynı zamanda daha karmaşık ihlalleri tespit etmek için "kötü amaçlı yazılımın ötesine" geçmelidir. Burada EPP çözümlerinin temelini oluşturan önleme teknolojilerinin filtreleme katmanlarını değil gelişmiş analitik sistemleri kastediyoruz.

Birden çok tespit teknolojisi kullanan güvenlik çözümleri, kuruluşunuza ciddi zararlar verilmeden önce saldırıları ve izinsiz girişleri belirleme şansınızı önemli ölçüde artırabilir. EDR çözümleri; statik, davranış tabanlı ve dinamik analizi birleştiren Gelişmiş Tehdit Tespiti, global tehdit istihbaratına gerçek zamanlı erişim ve makine öğrenim teknolojileri sunmak için entegre edilen birden çok tespit motoru kullanmalıdır.

Buradaki asıl amaç, tahminleri doğrulama, yeni incelemeler başlatma ve mevcut incelemeleri destekleme özelliğine sahip şirket içi "virüs analiz laboratuvarının" özelliklerini sağlamak için mümkün olduğu kadar farklı tespit motorundan faydalanmaktır.



Satıcıya bağlı olarak tespit teknikleri ve kullanılan motorlar, manuel araç kitini ve otomatik sistemleri bir kombinasyonla bir araya getirecektir:

Manuel Tespit Araçları

- Risk Göstergeleri'ni yükleme ve otomatik/manuel arama
- Geçmişe yönelik verilerde hızlı arama
- Korumalı alan teknolojisi (belirli bir nesneyi özel veya bulut tabanlı bir korumalı alanına gönderme özelliği)
- Satıcının tehdit istihbarat kaynaklarına erişim

Otomatik Algılama

- Kötü amaçlı yazılımlara karşı koruma
- YARA kuralları (satıcı ve/veya güvenlik ekibiniz tarafından özelleştirilebilir)
- Tehdit istihbaratı (satıcı tarafından otomatik olarak sağlanır)
- Bilinirlik hizmetleri (dosyalar veya/ve etki alanları)
- Şüpheli nesnelerin otomatik korumalı alan analizi
- Makine öğrenimi
  - Derin öğrenme (imzasız - nöral ağ)
  - Yapay zeka (taban sıralama, davranış analizi)

Öneriler:

- EDR satıcınıza hangi tespit teknolojilerini mevcut ve kullanılabilir olduğunu sorun
- Şirket içi, OEM veya açık kaynak tespit motorları kullanıp kullanmadıklarını öğrenin
- Bu motorları besleyen tehdit istihbaratının kalitesini ve sunulma hızını keşfedin
- Birden çok tespit teknolojisi varsa bu teknolojiler nasıl entegre edilmiş ve ilişkilendirilmiş? (aynı olay için farklı motorlara kaydedilmiş olay bilgileri görmek istemezsiniz)

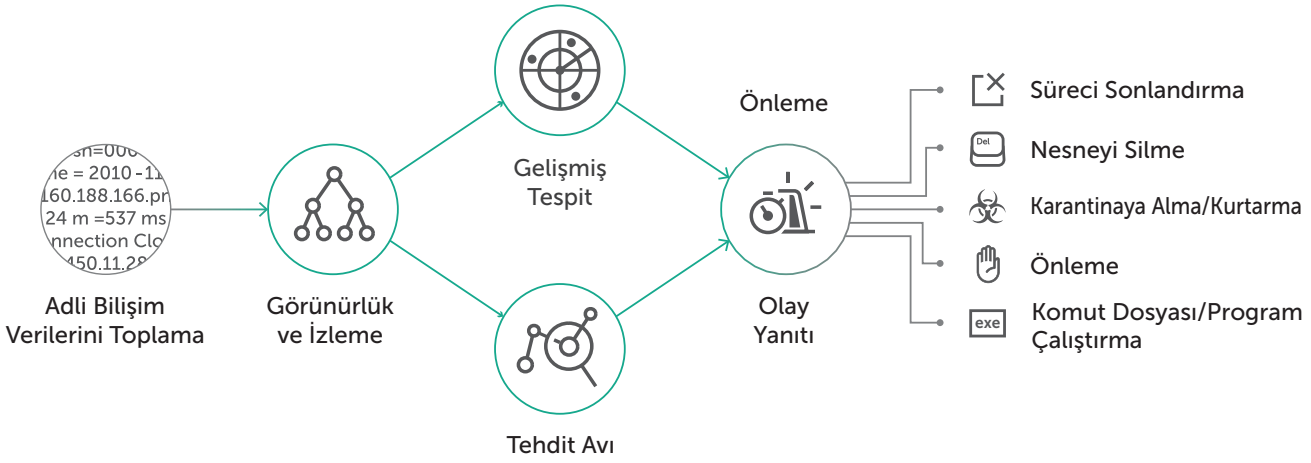
4

Tepki Vermeyin; Yanıtlayın

Bir olaya tepki vermek çok kolaydır. Ancak çözümü getiren asıl şey, etkili bir şekilde yanıt vermektir. Yanıt süreci, bir güvenlik olayı önceliklendirme ve ilk inceleme aracılığıyla doğrulandıktan sonra başlatılır. Olayın "hatalı pozitif" olmadığı doğrulandıktan sonra kesin ve doğru bir yanıt verilmesi gereklidir.

Olay Yanıt Yönetimi süreci olayın ciddiyetine bağlı olacaktır. Birçok olayın işinize olan etkisi nispeten daha düşüktür (girdikten sonra derhal tespit edildiğinde). Ancak veri ihlali, finansal bir suç, casusluk veya daha kötü suçlar gibi ciddi bir soruna yol açabilecek olaylar da vardır. Bunlar, Acil Yanıt ve İnceleme süreci gerektiren kritik durumlardır.

Manuel olarak bir olay bulduğunuzda veya üçüncü taraf güvenlik çözümü ya da EDR ürününüz aracılığıyla olası bir tehdit hakkında uyarıldıktan sonra süreç nasıl işler? Kuruluşunuz için önceliklendirme, inceleme ve yanıt süreçlerinin ana hatlarını belirlediniz mi? Bunlar olmadan güvenlik ekibiniz herhangi bir EDR çözümü çevresindeki iş akışı nedeniyle çabuk yorulabilir.



Etkin bir tehdidi tespit etmek, bir saldırıyı püskürtmenin ilk aşamasıdır. Tehdidi belirledikten sonra, binlerce uç noktada hızlı bir şekilde yanıt vermeniz gerekir. Etkili bir EDR çözümü, sorunsuz bir iş akışı ile şirket ağındaki tüm uç noktalarda olayların merkezi yönetimini sağlar. Ayrıca, çok çeşitli otomatikleştirilmiş yanıtlar, silme ve yeniden görüntüleme gibi geleneksel iyileştirme süreçlerini kullanmaktan kaçınmanıza yardımcı olur. Bu tür geleneksel süreçler, pahalı durma sürelerine ve verimlilik kaybına neden olur.

Temel yanıt işlevi satıcının yaklaşımına bağlıdır, ancak bu işlev aşağıdaki yaygın işlemlere odaklanmalıdır:

- PE dosyalarının, ofis belgelerinin ve komut dosyalarının başlatılmasını engelleme
- İş istasyonundaki dosyayı uzaktan silme özelliği
- Dosyayı iş istasyonundan karantinaya taşıma ve gerekirse kurtarma
- Dosyayı ele geçirme ve inceleme sırasında bir analiz gerçekleştirme (örneğin, zorunlu Korumalı Alan yürütme)
- İşlemi kapanmaya zorlama
- Programı/komut dosyasını çalışma istasyonunda çalıştırma

Bazı satıcılar daha kesin yanıtlar için ek senaryolar sağlayabilir. Bunlar ağ yalıtımı, işlem yalıtımı, kullanıcıyı devre dışı bırakma, geri alma ve düzeltme senaryolarını içerebilir.

Öneriler:

Çözümde aşağıdakileri arayın:

- Güçlü ve kapsamlı tehdit istihbarat veritabanları sağlama ve gerektiğinde size uzman destek ve danışmanlık sunma imkanına sahip satıcılar.
- Güvenlik ekibinizi etkili süreçler oluşturabilmesi ve yatırımınızdan en iyi şekilde faydalanılması için eğitebilecek etkili beceri eğitimi kursları tarafından desteklenen EDR çözümleri.
- Farklı konsollar veya çözümler arasında geçiş yapmaya gerek kalmadan tespit, manuel tehdit avı, üçüncü taraf Risk Göstergeleri ve Olay Yanıt süreçleri arasında sorunsuz bir iş akışı.
- İncelemeler sırasında bile son kullanıcılar için sessiz olan yani kullanıcı davranışını etkilemeyecek ve servis dışı kalma sürelerini artırmayan aracılar

5

Önleme – EDR mi EPP mi?

"Hepsi bir arada" bir çözüm sunmak amacıyla EDR çözümleri gittikçe daha fazla önleme unsurunu içine dahil etmektedir. Önleme özellikleri geliştikçe uç nokta önleme, görünürlük, tespit ve yanıt özellikleri tek bir uç nokta ürününde toplanacaktır.

Ancak şu anda bu aşamada değiliz. Tespit ve yanıt özelliklerinin yanı sıra önleme özelliğini de kapsayan bir çözüm aramak, ilgi çekici olsa da şu anda bu nokta üzerinde çok fazla durmamanızı öneririz. Ürününüzü öncelikle görünürlük, tespit ve yanıt özelliklerini göz önüne alarak seçin. Çözüm, ayrıca önleme unsuru da içeriyorsa bunu ek bir avantaj olarak değerlendirebilirsiniz. Ancak henüz gelişmemiş önleme özelliklerine sahip "yeni nesil" EDR çözümleri konusunda dikkatli olun. Geleneksel EPP'nizi bir EDR çözümüyle değiştirmeye çalışırsanız aynı önleme işlevi düzeyini elde etme ihtimaliniz düşüktür.

Ancak birçok EPP tedarikçisi artık kendi EDR'lerini satın almakta veya geliştirmektedir. Mevcut EPP'nizden memnunsanız ve EPP tedarikçiniz bir EDR çözümü sunuyorsa iki çözümün birbiriyle nasıl etkileşim kurduğunu ve sizin için birlikte nasıl çalışabileceklerini değerlendirmek mantıklıdır. Özellikle bu tür bir çözüm, EDR için ikinci bir aracı kurma ihtiyacını ortadan kaldırıyorsa kullanışlı olabilir.

Öneriler:

- EDR ürünün yol haritasını ve ek önleme özellikleri sunmak için zaman içinde nasıl gelişebileceğini inceleyin.
- Entegre uç nokta koruması, tespit ve Olay Yanıtı özellikleri size cazip geliyorsa mevcut EPP satıcınızın EDR tekliflerine göz atın ve diğer EDR satıcılarının hangi EPP özelliklerini sunduğunu inceleyin
- EDR'nin mimarisine ve özellikle EPP ve EDR için tek bir aracı kullanma özelliğini kontrol edin.

Kurumsal Uç Nokta Güvenliğinin Geleceği

Pazar liderleri, EDR özelliklerini geliştirmek için yeni teknolojileri benimsemeye ve dahili şirket içi gelişimlerden faydalanmaya çalışacaktır.

Şu anda uç nokta güvenlik pazarı, güvenlik uzmanlarına farklı satıcılarla dolu gibi görünebilir. Bu durumun devam edemeyeceği aşikârdır. Büyük ölçekli satıcılar, ürünlerini kullanarak portföy boşluklarını doldurmak ve markalarını geliştirmek için daha küçük işletmeleri yutacaktır. Pazar liderleri, EDR özelliklerini geliştirmek için yeni teknolojileri benimsemeye ve dahili şirket içi gelişimlerden faydalanmaya çalışacaktır.

Hem geleneksel kontrol ve koruma yöntemleri hem de gelişmiş teknolojiler sunan gerçek "Yeni Nesil" uç nokta güvenliği, EPP pazarındaki büyük firmaların çabalarıyla gelişecektir. EDR gibi gelişmiş uç nokta güvenlik aracılarının mevcut nesli, yalnızca gerçek EPP işlevselliğinin unsurlarını sunar. Satıcılar, şu anda tam işlevli bir uç nokta koruma takımı geliştirmeyi hedeflememektedir.

Uç nokta güvenliği, yeniden kurumsal dünyanın gündeminde yerini almıştır ve daha fazla ilgi çekmeye devam edecektir. Gelecekteki müşteriler, uç nokta etkinliği izleme özelliği ile birleştirilmiş gelişmiş uç nokta koruma teknolojilerini temel alan güvenlik stratejileri geliştirecek ve stratejilerini buna göre uyarlayacaktır.

Teknolojik olarak bu tür gelişmiş çözümler, koruma sağlamak için uyarlanabilir bir yaklaşım oluşturmanın yanı sıra sistem güçlendirme, kötü amaçlı yazılım etkinliklerini önleme ve gelişmiş tespit gibi özellikler sağlayacaktır. Bulut tabanlı tehdit istihbaratı ve şirket içi makine öğrenimi, aktif yanıt ve hızlı inceleme dahil olmak üzere tehdit avı ve derin davranış/tehdit istihbaratı analizi gibi özelliklere de önemli görevler düşecektir.

Kısa Zamanda Uygulanabilecek Öneriler

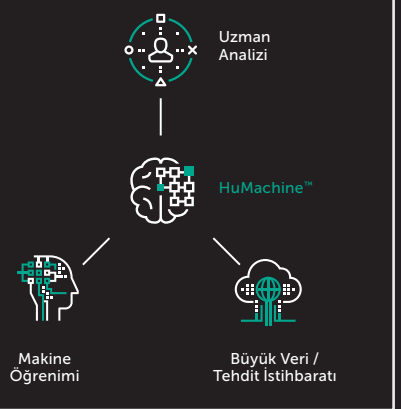
Daha derin uç nokta analizi ve koruması için artan ihtiyacı anlayan güvenlik uzmanları, kaçınılmaz bir şekilde uzun bir ihtiyaç listesiyle ve bunların tümünü sağlamak için kısıtlı bir bütçeyle karşılaşacaktır. Ancak şu anda bütçeniz olmasa bile birbirleriyle nasıl etkileşim kurduklarını ve dahili özelliklerini görmek için mevcut teknolojileri ve gelecekteki olası gelişmeleri değerlendirmek son derece mantıklıdır. Seçenekleri tam anlamıyla araştırıp test ederek işletmenizdeki karar vericilerin dikkatini yeni teknolojilerin sağladıkları özelliklere çekebilirsiniz. Böylece gelecek için daha kesin bir güvenlik bütçesi planı hazırlayabilir ve yatırım yapmanız gerektiğinde bunu bilinçli bir şekilde yapacağınızdan emin olabilirsiniz.

Derhal yapılması gerekenler

1. Genel güvenlik yeteneklerinizi değerlendirin. Mevcut Olay Yanıt süreciniz ne kadar hızlı ve ne kadar birleştirilmiş? Şu anda EDR dışında kendiniz için doğru çözümleri kullanıyor musunuz? Bu konuda endüstriniz ve rakiplerinize kıyasla hangi konumdasınız?
2. Uç noktalar üzerinde mevcut tespit becerilerinizi anlayın. Analizler gerçekleştirin ve ek istihbarat kaynaklarını inceleyin. Örneğin SIEM'iniz ile Tehdit Veri Akışı'nı kullanmayı deneyin
3. Şirket içi Olay Yanıt uzmanlığınızı nasıl geliştirmeye başlayacağınızı düşünün. Ekibinizin yeteneklerini değerlendirin ve etkili eğitim seçeneklerini araştırın.
4. Mevcut gerekliliklerinizi/gelecekteki taleplerinizi belirlemeye başlayın ve bunlara uygun olarak EDR çözümlerinin bazılarını eleyin.

Bazı yararlı bağlantılar

1. Olay Yanıt Yönergeleri: https://cdn.securelist.com/files/2017/08/Incident_Response_Guide_eng.pdf
2. Bu BT güvenlik hesaplayıcısıyla güvenliğinizi değerlendirin ve Global Kurumsal Çözümler Raporu'nu indirin: https://calculator.kaspersky.com/en/



Kaspersky Lab
Enterprise Cybersecurity:**www.kaspersky.com.tr/enterprise**
Siber Tehdit Haberleri: **www.securelist.com**
BT Güvenliğiyle İlgili Haberler: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com.tr