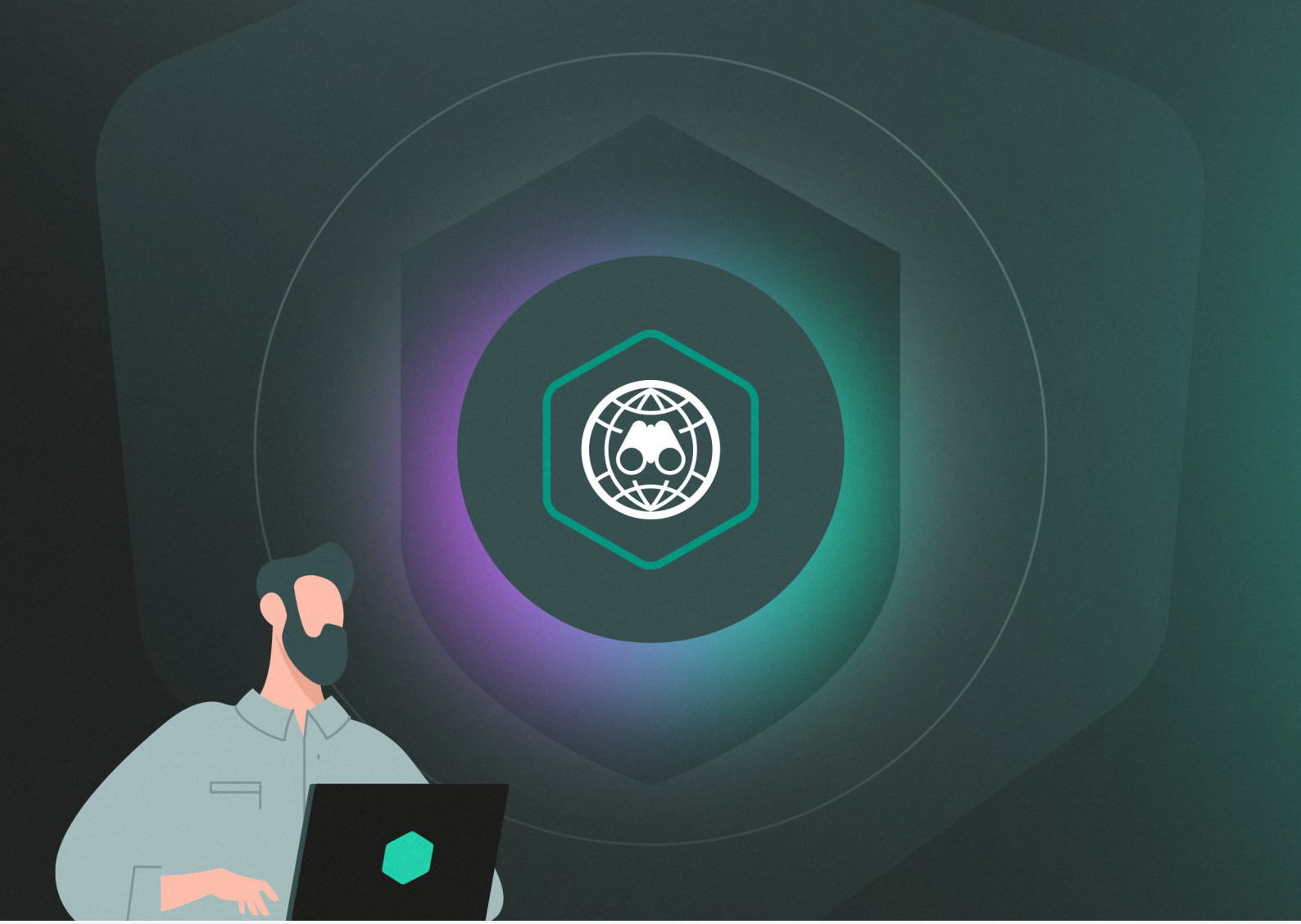


Kaspersky Tehdit İstihbaratı

Tehdit istihbaratı kaynaklarını değerlendirme

kaspersky GELECEĞİ YAKALAYIN

Daha fazla bilgi edinmek için kaspersky.com adresini ziyaret edin
#geleceğiyakalayın

Tanıtım

Genişleyen saldırı alanı ve tehditlerin büyüyen karmaşıklığı nedeniyle yalnızca bir olaya müdahale etmek yeterli değildir. Giderek karmaşıklaşan ortamlar, saldırganlar için birden fazla fırsat sağlar. Her sektör ve her kuruluş korunması gereken kendine özgü verilere sahiptir ve kendi uygulama, teknoloji vb. setini kullanır. Bütün bu faktörler, her gün ortaya çıkan yeni yöntemler de düşünüldüğünde, bir saldırı yapmanın olası yöntemlerine oldukça fazla sayıda değişken katar.

Son birkaç yılda, farklı tehdit türleri ve farklı tehdit aktörü türleri arasındaki sınırların belirsizleştiği gözlenmiştir. Daha önce sınırlı sayıda kuruluş için tehdit oluşturan yöntemler ve araçlar, daha geniş bir pazara yayılmıştır. Bunun bir örneği, Shadow Brokers grubu tarafından çıkarılan bir kod dökümünün, gelişmiş açıkları, bu tür karmaşık bir koda başka şekilde erişimi olmayacak suç gruplarının kullanımına sunmasıdır. Başka bir örnek de, siber casusluğa değil, hırsızlığa, APT gruplarının katıldığı diğer faaliyetleri finanse etmek için para çalmaya, odaklanan gelişmiş kalıcı tehdit (APT) kampanyalarının ortaya çıkmasıdır. Bu liste daha da uzatılabilir.

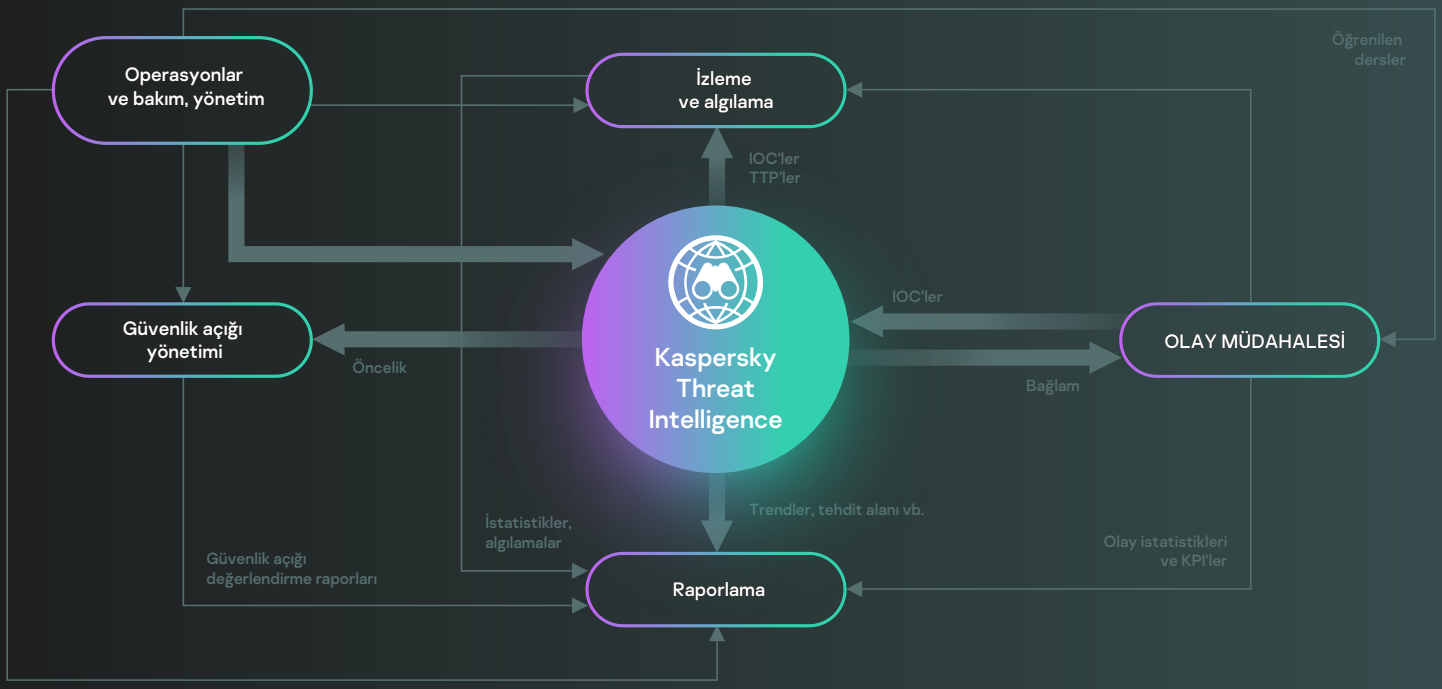
Yeni bir yaklaşıma ihtiyaç vardır

Daha önce sınırlı sayıda kuruluş için tehdit oluşturan yöntemler ve araçlar, daha geniş bir pazara yayılmıştır.

Kurumların gelişmiş ve hedefli saldırılarla giderek daha fazla karşı karşıya kaldığı göz önünde bulundurulduğunda, başarılı bir savunmanın yeni yöntemler gerektirdiği açıktır. İşletmelerin kendilerini korumak için proaktif bir yaklaşım benimseyerek güvenlik kontrollerini sürekli değişen tehdit ortamına sürekli olarak uyarlaması gerekir. Bu değişikliklere uyum sağlamanın tek yolu, etkili bir tehdit istihbarat programı oluşturmaktır.

Tehdit istihbaratı, tüm sektörlerde ve coğrafyalarda farklı ölçeklerdeki şirketler tarafından kurulan güvenlik operasyonlarının önemli bir bileşeni haline gelmiştir. İnsanlar tarafından okunabilen ve makine tarafından okunabilen biçimlerde sunulan tehdit istihbaratı, güvenlik ekiplerini, olay yönetimi döngüsü boyunca anlamlı bilgilerle destekleyebilir ve stratejik karar almaya yönelik bilgi sağlayabilir (Şekil 1).

Ancak dış tehdit istihbaratına yönelik artan talep, her biri çok çeşitli hizmetler sunan çok sayıda tehdit istihbaratı tedarikçisinin ortaya çıkmasına neden olmuştur. Çok sayıda karmaşık seçeneğe sahip geniş ve rekabetçi bir pazar, kuruluşunuz için doğru çözümü seçmeyi son derece akıl karıştırıcı ve sinir bozucu hale getirebilir.



Şekil 1

Tehdit İstihbaratına Dayalı Güvenlik Operasyonları

İşletmenizin özel ihtiyaçlarına göre belirlenmeyen tehdit istihbaratı durumu daha kötü bir hale getirebilir. Bugün birçok şirkette güvenlik analistleri, zamanlarının yarısından fazlasını, proaktif tehdit avı ve müdahalesi yerine, hatalı pozitif sonuçları ayıklamak için harcamakta; bu da algılama sürelerinde önemli bir artışa yol açmaktadır. Güvenlik operasyonlarınızı ilgisiz veya yanlış istihbaratla doldurmak, hatalı uyarıların sayısını daha da artırır ve müdahale kabiliyetleriniz ve şirketinizin genel güvenliği üzerinde ciddi, olumsuz bir etkiye neden olur.

En iyi istihbaratın hayata geçtiği yer...

Peki sayısız tehdit istihbaratı kaynağını nasıl değerlendiriyor, kuruluşunuzla en ilişkili olanları nasıl belirliyor ve bunları etkin bir şekilde nasıl işlevsel hale getiriyorsunuz? Neredeyse her tedarikçinin kendi istihbaratının en iyisi olduğunu iddia ettiği yığınla anlamsız pazarlama faaliyeti arasında yolunuzu nasıl buluyorsunuz?

Bu sorular, geçerli olsalar da, kesinlikle sormanız gereken ilk sorular değildir. Gösterişli mesajların ve iddialı vaatlerin cazibesine kapılan birçok kuruluş, en değerli istihbaratın kendi kurumsal ağlarının çevresinde yer aldığını tamamen göz ardı ederek, harici bir tedarikçinin onlara bazı süper güçler sağlayabileceğine inanıyor...

İzinsiz giriş algılama ve önleme sistemlerinden, güvenlik duvarlarından, uygulama günlüklerinden ve diğer güvenlik kontrollerinden alınan günlüklerden elde edilen veriler, bir şirketin ağında neler olup bittiği hakkında çok fazla bilgi ortaya çıkarabilir. Kuruluşa özgü kötü amaçlı yazılım etkinliği örüntülerini belirleyebilir. Normal bir kullanıcı ile ağ davranışı arasında ayrım yapabilir ve bir veriye erişim etkinliğini takip etmeye yardımcı olabilir.

Şekil 2

Dış Tehdit İstihbaratının İşlevsel Hale Getirilmesi

Bir saldırgan gibi düşünün

Etkili bir tehdit istihbaratı programı oluşturmak için yerleşik Güvenlik Operasyonu Merkezleri olanlar da dahil olmak üzere şirketler, bir saldırgan gibi düşünerek, en olası hedefleri tespit edip korumalıdır. Bir tehdit istihbaratı programından gerçek anlamda değer elde etmek, önemli varlıkların neler olduğunu ve kuruluşun hedeflerine ulaşmak için hangi veri setlerinin ve iş süreçlerinin kritik olduğunu çok net bir şekilde anlamayı gerektirir. Bu en değerli varlıkları belirlemek, şirketlerin, toplanan verileri harici olarak bulunan tehdit bilgileriyle daha fazla eşlemek için etraflarında veri toplama noktaları oluşturmasına olanak verir. Bilgi güvenliği departmanlarının kaynaklarının genellikle sınırlı olduğu düşünüldüğünde, bütün organizasyonun profilini çıkarmak büyük bir girişimdir. Çözüm, önce en hassas hedeflere odaklanarak riske dayalı bir yaklaşım benimsemektir.

Dahili tehdit istihbaratı kaynakları tanımlanıp işlevsel hale getirildikten sonra şirket, mevcut iş akışlarına harici bilgiler eklemeyi düşünmeye başlayabilir.

Bir güven meselesi

Dış tehdit istihbaratı kaynaklarının güven düzeyleri değişiklik gösterir:

- Açık kaynaklar ücretsiz olarak kullanılabilir ancak genellikle bağlamdan yoksundur ve önemli sayıda hatalı pozitif sonuç verir
- Ticari tehdit istihbaratı kaynakları çok daha güvenilirdir ancak bunlara erişim satın almak pahalı olabilir
- Finansal Hizmetler Bilgi Paylaşımı ve Analiz Merkezi (FS-ISAC) gibi sektöre özel istihbarat paylaşımı topluluklarına erişmek başlangıç için iyi bir seçenektir. Bu topluluklar son derece değerli bilgiler sağlasa da çoğu zaman geçitlidir ve erişim sağlamak için üyelik gerekir

Dış tehdit istihbaratı kaynaklarının seçiminde kılavuz ilke nicelikten çok nitelik olmalıdır. Bazı kuruluşlar, entegre ettikleri tehdit istihbaratı kaynağı sayısı ne kadar fazla olursa o kadar iyi görünürlük elde edeceklerini düşünebilir. Bu, bazı durumlarda doğru olabilir; örneğin, ticari olanlar dahil yüksek ölçüde güvenilir kaynaklar söz konusu olduğunda, kuruluşun özel tehdit profiline göre uyarlanmış tehdit istihbaratı sağlanır. Aksi takdirde, güvenlik operasyonlarınızın ilgisiz bilgilerle dolması gibi önemli bir risk söz konusudur.

Uzmanlaşmış tehdit istihbaratı tedarikçileri tarafından sağlanan bilgilerdeki çakışma çok küçük olabilir. İstihbarat kaynakları ve toplama yöntemleri farklılık gösterdiğinden, sağladıkları analizler bazı açılardan benzersiz olacaktır. Örneğin, bir tedarikçi, belirli bir bölgede önemli bir yere sahip olması nedeniyle o bölgeden yayılan tehditler hakkında daha fazla bilgi sağlarken, bir başka tedarikçi belirli tehdit türleri hakkında daha fazla bilgi sağlar. Bu nedenle, her iki kaynağa da erişim sağlamak faydalı olabilir. Bunlar birlikte kullanıldıklarında büyük resmin ortaya çıkmasına ve daha etkili tehdit avlama ve olaya müdahale görevlerine kılavuzluk etmeye yardımcı olabilir. Bununla birlikte, bu tür güvenilir kaynakların, sağlanan istihbaratın kuruluşunuzun özel ihtiyaçlarına ve güvenlik operasyonları, olaylara müdahale, risk yönetimi, güvenlik açığı yönetimi, kırmızı takım oluşturma gibi kullanım durumlarına uygun olduğundan emin olmak için dikkatli bir ön değerlendirme de gerektirdiği unutulmamalıdır.

Ticari tehdit istihbaratı tekliflerini değerlendirirken dikkate alınması gereken konular

Çeşitli ticari tehdit istihbaratı tekliflerini değerlendirmek için hala ortak bir kriter yoktur ancak bunu yaparken dikkate alınması gereken bazı konular vardır:

Şirketinizin, tanımlanmış ilişkili süreçlerle birlikte bazı güvenlik kontrollerini halihazırda uyguladığı ve halihazırda kullandığınız ve bildiğiniz araçlarla tehdit istihbaratı yürütmenin sizin için önemli olduğu varsayılır. Bu nedenle, tehdit istihbaratının mevcut güvenlik operasyonlarınıza sorunsuz entegrasyonunu destekleyen teslim gönderme yöntemleri, entegrasyon mekanizmaları ve biçimler arayın

Küresel erişime sahip istihbarat arayın. Saldırılar sınır tanımaz. Latin Amerika'daki bir şirketi hedef alan bir saldırı Avrupa'dan başlatılabilir veya bunun tersi de olabilir. Tedarikçi, bilgileri küresel olarak sağlıyor ve birbirinden ayrı görünen faaliyetleri uyumlu kampanyalar halinde düzenliyor mu? Bu tür istihbarat, uygun eylemleri gerçekleştirmenize yardımcı olacaktır

Bağlam, veriden istihbarat çıkarır. Bağlamı olmayan tehdit göstergelerinin hiçbir değeri yoktur. "Bu neden önemlidir?" gibi anlamlı soruları yanıtlamanıza yardımcı olacak tedarikçiler aramanız gerekir. İlişki bağlamı (örn. algılanan IP adresleri veya belirli bir dosyanın indirildiği URL'ler vb. ile ilişkili alanlar) ek değer katarak olay araştırmasını hızlandırır ve ağda yeni elde edilen ilgili Güvenlik İhlal Göstergelerini ortaya çıkararak "kapsam belirleme"nin daha iyi yapılmasını destekler

Aşağıda örnek olarak sıralanan konulardaki uzun vadeli güvenlik planlamanız için bilgi elde etmek üzere daha stratejik bağlam arıyorsanız;

- Saldırı trendlerine üst düzey bir bakış açısı
- Saldırganlar tarafından kullanılan teknikler ve yöntemler
- Saldırıların arkasındaki amaçlar
- Tehdit Nitelendirmeler vb.,

bölgenizdeki veya sektörünüzdeki karmaşık tehditleri sürekli olarak ortaya çıkarma ve araştırma konusunda kanıtlanmış bir performansa sahip bir tehdit istihbarat tedarikçisi arayın. Tedarikçinin araştırma kabiliyetlerini şirketinizin özelliklerine göre uyarlama becerisi de önemlidir

Sonuç

Kaspersky olarak yirmi yılı aşkın bir süredir tehdit araştırmalarına odaklanıyoruz. İşlenecek petabaytlarca zengin tehdit verileri, gelişmiş makine öğrenimi teknolojileri ve tüm dünyadan eşsiz uzman havuzu ile, önceden görülemeyen siber saldırılara karşı bile bağışıklığınızı sürdürmenize yardım ederek dünyanın dört bir yanından elde edilen en güncel tehdit istihbaratını sizlere sağlamaya çalışıyoruz.

www.kaspersky.com.tr