Kaspersky®
Threat Intelligence

Stratejik tehdit istihbaratı kullanım senaryoları

İnternet yaşamlarımızın büyük kısmını domine etmektedir. Sağladığı düşük maliyetli ve yüksek hızlı iletişim, interneti başarılı işletmelerin ve hükümetlerin çok temel ve kritik bir bileşeni haline getirmektedir. Dinamik ve bileşik ortamlar rekabet gücünü canlandırırken, iletişimi geliştirme, kişisel, gizli ve diğer verileri koruma ve kritik sistemlerin ve iş süreçlerinin gözetimi ve kontrolünü sağlayarak çeşitli önemli işlevler sağlamaktadır. Ancak sürekli artan bağlanabilirlik, saldırı yüzeyini genişletirken düşmanlar her düzeyde olası her güvenlik açığından yararlanmak için hazır bekliyor.

Son birkaç yıl boyunca farklı tehdit türleri ve tehdit aktörü türleri arasındaki sınırlar netliğini yitirmiştir. Bunun bir örneği, gelişmiş güvenlik açıklarını (NSA tarafından geliştirildiği iddia edilen) normalde bu tür karmaşık kodlara erişemeyecek olan suçlu grupların kullanımına sunan Shadow Broker grubunun kod dökümüdür. Başka bir örnek ise, gelişmiş hedefli tehdit (APT) saldırılarıdır; bu saldırılar siber casusluğa değil, APT grubunun dahil olduğu diğer faaliyetleri finanse etmek için para çalma gibi hırsızlık faaliyetlerine odaklanmaktadır.

Tehdit unsurları, para hırsızlığından rakipleri alt etmeye, kimlik hırsızlığına ve sahtekarlığa kadar çok çeşitli amaçlara sahiptir. Ayrıca, her endüstri ve kuruluşun korumak isteyeceği benzersiz verileri, benzersiz bir uygulama seti, kullandığı teknolojiler vb. vardır. Tüm bu faktörler saldırıların gerçekleşme şeklini çeşitlendiriyor ve her gün yeni saldırı yöntemlerinin ortaya çıkmasına sebep oluyor.

Bu hızla değişen tehdit ortamında, dijital dönüşümle işletme büyümesini teşvik etmek son derece zorlayıcı olabilir. Ayrıca işletme liderleri genel iş hedeflerine ve önceliklerine karşı siber riskleri sürekli olarak tartarak stratejik bir yaklaşım benimsemelidir.

Riskleri anlamak, yeni bir girişim başlatma, yeni bir bölgesel ofis açma veya bir teknoloji yatırımı planlarken bilinçli kararlar verme imkanı tanır. Ayrıca ileriye dönük azaltma stratejilerinin geliştirilmesine ve ilgili bütçe ve personel gereksinimlerinin gerekçelendirilmesine de yardımcı olur.

Stratejik tehdit istihbaratı, saldırganların motivasyonları ve özellikleri de dahil olmak üzere saldırı eğilimleri, teknikleri ve yöntemlerine yönelik yüksek düzeyde bir görünüm sunar ve belirli bir soru takımını yanıtlamaya yardımcı olur:

- Düşmanlarınız kim? Sizden ne istiyorlar?
- Sektörünüzde veya bölgenizde hangi tehdit grupları etkin?
- Kullanılan saldırı vektörleri nelerdir?
- Kurumunuza yapılan saldırıyla mücadele etmek için en iyi yöntem nedir?
- Özellikle sizi hedef alan saldırganın elinde hangi bilgiler var ve bu saldırgan hangi yol haritalarını takip ediyor?
- Halihazırda gerçekleşen bir saldırı oldu mu? Saldırı tehdidine maruz kalmaya yakın mısınız?
- Risk profilinizi azaltmak için hangi eylemler gereklidir?

Bu soruları anlamak ve bu sorulara kritik varlıklarınıza, sistemlerinize ve iş süreçlerinize yönelik yanıtlar planlamak, kapsamlı bir risk analizi gerçekleştirmenize, yönetici kademesindeki lider ekibinize net ve alakalı risk senaryoları iletmenize ve böylece belirli program, teknoloji ve personel yatırımlarını gerekçelendirmenize olanak tanır. Bu benzersiz fikirlere sahip olduğunuzda bilgi güvenliği stratejinizi siber suçluların birincil hedefi olarak işaretlenen alanlarda toplayabilirsiniz. İzinsiz giriş yapan saldırganları geri püskürtmek ve başarılı bir saldırının yaratacağı riskleri an aza indirmek için hızlıca ve tam doğrulukla hareket edebilirsiniz.

Kaspersky Lab şunları sunar:

Rapor türü	Sağlanan istihbarat	Kullanım senaryosu
APT Intelligence Reporting	• Çapraz sektör hedefleme ile siber casusluk saldırılarında saldırganların kullandığı taktik ve yöntemlerin açıklamaları • Saldırganların kullandıkları TTP'ler (Taktik, Teknik ve Prosedürler) ve tehdit aktör profilleri • İlgili TTP'leri gerçek dünya deneyimine dayanan düşman TTP'lerinin bilgi tabanı olan MITRE ATT&CK ile eşleştirme.	• Sektörünüzü veya bölgenizi hedefleyen tehdit aktörlerini ve bu aktörlerin neler kullandığını anlama • Hangi bilgi varlıklarının ve sistemlerinin risk altında olduğunu, güvenlik açığının potansiyel etkisini ve buna göre nasıl önceliklendirileceğini belirleme • Bilgi güvenliği stratejilerini düzenleyin, potansiyel saldırı vektörlerini ele alan belirli teknolojilere, personele ve programlara ilişkin yatırımları planlayın ve gerekçelendirin.
Finansal Tehdit İstihbarat Raporu	• Mali sektörü hedefleyen saldırganların kullandığı taktik ve yöntemlerin açıklamaları • ATM'ler veya Satış Noktası cihazları gibi belirli altyapılara ilişkin saldırılar hakkında bilgi • Finansal ağlara saldırmak için tasarlanmış, Darknet toplulukları ve çeşitli coğrafyalardaki forumlar tarafından kullanılan, geliştirilen ve satılan belirli araçlara ilişkin ilgili bilgiler.	• Küresel olarak finansal kurumları hedef alan düşmanları ve onların kullandığı TTP'leri tanımlama • Hangi bilgi varlıklarının ve sistemlerinin risk altında olduğunu, güvenlik açığının potansiyel etkisini ve buna göre nasıl önceliklendirileceğini belirleme • Bilgi güvenliği stratejilerini düzenleyin, potansiyel saldırı vektörlerini ele alan belirli teknolojilere, personele ve programlara ilişkin yatırımları planlayın ve gerekçelendirin.
Müşteriye Özel Tehdit İstihbaratı Raporlama	• Ağ çevresi, mevcut hizmetler ve mevcut güvenlik açıklarının pasif olarak tanımlanması • Özelleştirilmiş güvenlik açığı ve güvenlik açıklarından yararlanan yazılımların çözümlemesi • Kuruluşunuzu hedefleyen aktif veya pasif kötü amaçlı yazılımların tanımlanması, izlenmesi ve analizi • Veri ve kimlik bilgisi sızıntıları • Müşterilerin markalarını hedefleyen kimlik avı tehditleri • Özellikle bir şirketin müşterilerini, ortaklarını ve tedarikçilerini hedefleyen tehdit ve botnet etkinliğine yönelik deliller • İlgili siber suçlu TTP'leri dahil olmak üzere sektöre özgü analiz.	• Tanımlanan güvenlik açıklarını azaltmak için kaynakların kullanılabilirliğini ve doğru tahsis edilmesini sağlamak • Tedarik zinciri saldırılarını önlemek için üçüncü kişilerin karmaşık durum tespiti projelerini bildirme • Olası çalışan tehditlerini azaltmak için politika ve denetimler belirleme • Bulgulara (örn; üçüncü parti hizmetleri aracılığıyla ele geçirilen kurumsal kimlik bilgileri) dayalı belirli bir program geliştirerek şirket içi personel güvenlik farkındalığını artırma • Şirket markalarının kimlik avı amaçlıyetkisiz kullanımını izleyerek şirket itibarına yönelik olası zararları azaltma • Potansiyel saldırı vektörlerini ele alan belirli teknolojilere, personele ve programlara ilişkin yatırımları planlayın ve gerekçelendirin.

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

#truecybersecurity
#HuMachine

www.kaspersky.com.tr