Siber düşmanlarınızın daima bir adım önünde olun

Kaspersky Tehdit İstihbaratı

kaspersky geleceği yakalayın

Kaspersky
Threat Intelligence

Kaspersky Tehdit İstihbaratı

Kaspersky'nin Tehdit İstihbaratı size siber tehditleri azaltmak için dünya lideri araştırmacılar ve analistlerden oluşan ekibimizin sağladığı istihbarata erişim sunar.

Kaspersky'nin siber güvenliğin her alanındaki bilgisi, deneyimi ve derin istihbaratı, INTERPOL ve Bilgisayar Acil Durum Müdahale Ekipleri (CERT) dahil olmak üzere dünyanın önde gelen emniyet güçleri ve devlet mercileri tarafından güvenilir bir ortak olarak kabul edilmemizi sağlamıştır. Kaspersky Tehdit İstihbaratı; teknik, taktiksel, operasyonel ve stratejik Tehdit İstihbaratına anında erişmenizi sağlar.

Kaspersky Tehdit İstihbaratı, kurumların siber tehditlere karşı korunmasına yardımcı olacak eyleme geçirilebilir öngörüler sunmak için çalışan uzman ekibimiz tarafından analiz edilen istihbarat kaynaklarını, tehdit verisi beslemelerini ve kurum içi araştırmaları birleştirerek küresel tehdit ortamının kapsamlı bir görünümünü sunar.

Taktiksel

Güvenlik operasyonlarını ve olay müdahalesini destekleyen düşük seviyeli, çok çabuk bozulabilen bilgiler. Yeni keşfedilen bir saldırının yürütülmesiyle ilgili IOC'ler taktik istihbarata bir örnektir.

Roller:
- SOC Analiz Uzmanı

Sistemler:
- SIEM
- NGFW
- IPS
- IDS
- SOAR

İşlemler:
- Tehdit Avlama
- İzleme

Operasyonel

Bu seviye genellikle kampanyalar ve daha üst düzey TTP'lere ilişkin verileri içerir. Bu bilgiler, belirli aktör ilişkilendirmelerinin yanı sıra rakiplerin kabiliyetleri ve niyetleri hakkında da bilgi içerebilir.

Roller:
- SOC L3 Analisti
- DFIR Analisti
- IR Analisti

Sistemler:
- SIEM
- NTA
- EDR/XDR
- TIP

İşlemler:
- Olay Müdahalesi
- Tehdit Avlama

Stratejik

Bu seviye, C düzeyindeki yöneticileri ve yönetim kurullarını risk değerlendirmeleri, kaynak dağıtımı ve kurumsal strateji hakkında ciddi kararlar alma konusunda desteklemektedir. Bu bilgiler eğilimleri, aktör motivasyonlarını ve sınıflandırmalarını içerir.

Roller:
- CISO
- CTO
- CIO
- CEO

İşlemler:
- IS stratejisi oluşturulması
- Farkındalık artırma

Kaspersky Tehdit İstihbaratı uygulama şeması

Kaspersky Tehdit İstihbaratı sizi daha güçlü kılar

Tehditleri proaktif olarak tespit edin ve önleyin

Kaspersky Tehdit İstihbaratı, en güncel tehditler ve güvenlik açıkları hakkında sizi bilgilendirerek sistemlerinizi saldırı henüz gerçekleşmeden önce korumanız için proaktif önlemler almanızı sağlar.

Dijital ayak izinizle ilgili farkındalığınızı artırın

Kaspersky Tehdit İstihbaratı, saldırıya veya tehlikeye açık olabilecek tüm varlıklarınız dahil olmak üzere, dijital ayak izinizin kapsamlı bir görünümünü sunar.

Tehdit algılama yetkinliğinizi geliştirin

Kaspersky Tehdit İstihbaratı, mevcut güvenlik çözümlerinizi en yeni tehdit istihbaratıyla desteklemenize yardımcı olarak gelişmiş tehditleri tespit etme ve engelleme becerinizi geliştirir.

Olay müdahalenizi iyileştirin

Kaspersky Tehdit İstihbaratı, sizi tehlikeye atabilecek tehditler ve tehlike göstergeleri hakkında gerçek zamanlı bilgiler sunar. Böylece, olaylara hızlı ve etkili bir şekilde yanıt verebilirsiniz.

Yasal düzenlemelerle ve standartlarla uyumlu olmanızı sağlar

Tüm şirketler kendi sektörlerinde çeşitli yönetmeliklere ve standartlara tabidir. Kaspersky Tehdit İstihbaratı, bu gereksinimleri karşılamanıza yardımcı olarak yönetmelikler ve standartlarla uyumluluğunuzu destekler.

Şirketinizin tehdit istihbaratı konusundaki uzmanlığını zenginleştirin

Sektördeki en deneyimli ve saygın araştırmacılar arasında yer alan uzman Kaspersky ekibi, Bilgi Güvenliği ekiplerinize zengin bir bilgi birikimi ve uzmanlık sunar.

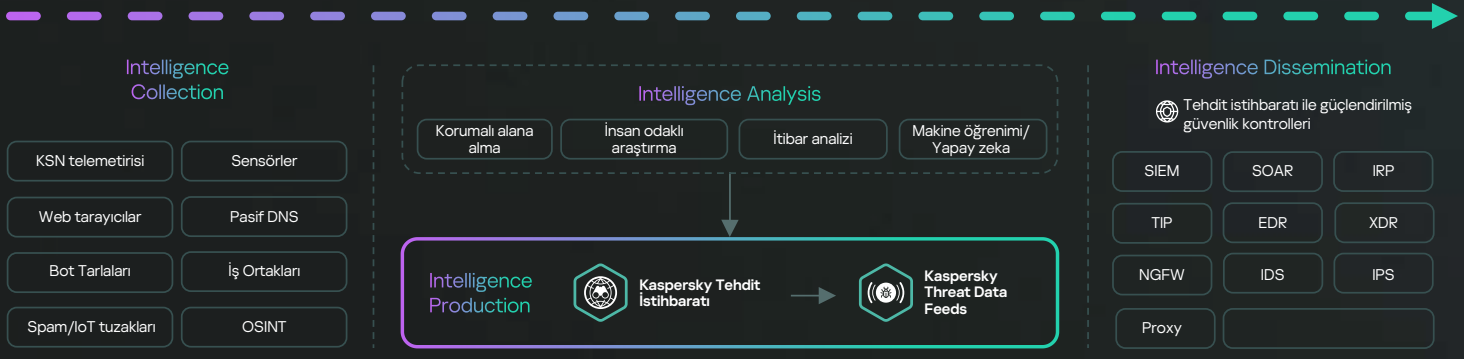
Kaspersky
Threat Data

Kaspersky Threat Data Feeds

Siber saldırılar her gün gerçekleşmektedir. Savunmanızı tehlikeye atmaya yönelik siber tehditlerin sıklığı, karmaşıklığı ve gizlenme taktikleri de sürekli gelişip artmaktadır. Saldırganlar, işletmenizin işleyişini aksatmak veya müşterilerinize zarar vermek için karmaşık izinsiz giriş zincirleri, saldırılar ve şirketinize yönelik geliştirdikleri Taktikler, Teknikler ve Prosedürler (TTP'ler) kullanır. Bu tehditlerden etkili biçimde korunmak için tehdit istihbaratına dayalı yeni yöntemler gerektiği açıktır.

Güvenlik ekipleri, şüpheli ve tehlikeli IP'ler, URL'ler ve dosyalarla ilgili bilgileri içeren en güncel tehdit istihbaratı beslemelerini SIEM, SOAR ve Tehdit İstihbarat Platformları gibi mevcut güvenlik sistemlerine entegre ederek ilk uyarı triyajı süreçlerini otomatikleştirebilir. Böylece triyaj uzmanlarına, araştırılması veya daha fazla araştırma ve müdahale için olay müdahale ekiplerine bildirilmesi gereken uyarıları anında göndermek için yeterli bağlam sağlanır.

Kaspersky Tehdit Verisi Beslemesi, ağlarınızı ve sistemlerinizi siber tehditlere karşı korumanıza yardımcı olmak için gerçek zamanlı tehdit istihbaratı bilgileri sunar. Veri beslemeleri, bilinen kötü amaçlı yazılımlar, kimlik avı web siteleri, en son güvenlik açıkları ve istismarlar ve diğer siber tehdit türleri hakkında bilgiler içerir - bunlar, kötü amaçlı trafiği engellemenize, güvenlik yazılımınızı güncellemenize ve siber saldırılara karşı korunmak için başka önlemler almanıza yardımcı olacak bilgilerdir.



1

Veriler, Kaspersky Security Network ve kendi tarayıcılarımız, botnet tehditleri izleme hizmeti (botnetleri ve hedeflerini 7/24 izler), spam tuzakları, araştırma gruplarından gelen veriler, iş ortakları vb. dahil olmak üzere çok çeşitli güvenilir kaynaktan toplanır.

2

Toplanan tüm bilgiler, çeşitli ön işleme yöntemleri kullanılarak gerçek zamanlı olarak dikkatlice kontrol edilir ve temizlenir. Söz konusu ön işleme yöntemleri arasında korumalı alanda test etme (sandboxing), istatistiksel ve sezgisel analiz, benzerlik araçları, davranış profili oluşturma ve uzman analizleri bulunur.

3

Veri Beslemeleri, bir uyarı veya güvenlik olayı hakkında tehdit bilgilerinin toplanmasına ve ayrıntılara inilmesine yardımcı olur. Ayrıca şu soruları yanıtlayabilmenize de yardımcı olur: 'Kim? Ne? Nerede? Neden?' Böylece, bir saldırının kaynağını belirleyebilmenizi sağlayarak şirketinizi her türlü karmaşıklıktaki tehditlerden korumak için hızlı karar vermenizi mümkün kılar.

Bağlamsal veriler

Bağlamsal veriler, verilerin geniş kapsamlı kullanımını daha fazla doğrulayarak ve destekleyerek “büyük resmin” ortaya çıkarılmasına yardımcı olur. Kaspersky tarafından sağlanan akışlardaki girişler, tehditleri hızlı bir şekilde onaylamanıza ve önceliklendirmenize yardımcı olan aşağıdaki bağlamsal verileri içerir:

1. Tehdit adları
2. Kötü amaçlı web kaynaklarının IP adresleri ve domain’leri
3. Kötü amaçlı dosya grupları
4. Savunmasız ve tehlike altındaki unsurlar
5. MITRE ATT&CK sınıflandırmasına göre hazırlanmış saldırı taktikleri, teknikleri ve prosedürleri
6. Zaman damgaları
7. Coğrafi Konum
8. Bilinirlik ve daha fazlası

Kaspersky Tehdit Verisi Beslemeleri faydaları

Bir yandan güvenlik analistlerinize, araştırılması veya daha fazla araştırma ve müdahale için olay müdahale ekiplerine bildirilmesi gereken uyarıları anında tespit edebilmeleri için yeterli bağlamı sağlarken, diğer yandan ilk triyaj sürecini otomatikleştirerek

olaylara müdahale ve adli bilişim yetkinliklerinizi geliştirir ve hızlandırır.

SIEM’ler, Güvenlik Duvarları, IPS/IDS, Güvenlik Proxy’si, DNS çözümleri ve Anti-APT dahil olmak üzere,

güvenlik çözümlerinizi, siber saldırılara ilişkin bilgi sağlamak ve saldırganların niyetinin, yetkinliklerinin ve hedeflerinin daha iyi anlaşılmasını mümkün kılmak için sürekli güncellenen Güvenlik İhlal Göstergeleri (IOC’ler) ve eyleme geçirilebilir bağlamla destekler. Önde gelen SIEM’ler (ArcSight, IBM QRadar, MS Sentinel, Splunk vb. dahil) ve TI Platformları tamamen desteklenir.

Hassas varlıkların ve fikri mülkiyetin

enfekte olmuş cihazlardan kurumunuz dışına sızdırılmasını önler. Marka itibarınızı korumak, rekabet avantajınızı sürdürmek ve iş fırsatlarını güvence altına almak için enfekte olmuş varlıkları hızlı bir şekilde tespit eder.

Müşterilerinize sektördeki lider tehdit istihbaratını sağlayarak

işletmenizin yönetilen güvenlik hizmeti sağlayıcısı (MSSP) yönünü büyütün. Bilgisayar Acil Durum Müdahale Ekibi (CERT) olarak sahip olduğunuz siber tehdit algılama ve tanımlama yetkinliğini geliştirin ve genişletin.

Kaspersky CyberTrace

Kaspersky CyberTrace

Tehdit verisi beslemeleri ile mevcut tehdit istihbaratı kaynaklarındaki sürekli büyüme, kuruluşların hangi bilgilerin kendileri için önemli olup olmadığını belirlemesini zorlaştırır. Ayrıca, tehdit istihbaratlarının farklı formatlarda olması ve çok sayıda Tehlike Belirtisi (IoC'ler) içermesi, SIEM ve diğer ağ güvenliği denetimlerinin bu istihbaratı işlemesini zorlaştırır.

Güvenlik Operasyonu Merkezleri, SIEM sistemleri gibi makine tarafından okunabilen, en güncel tehdit istihbaratı ile mevcut güvenlik kontrollerini bir araya getirerek ilk saptama sürecini otomatikleştirebilir. Ayrıca incelenmesi veya daha ayrıntılı bir şekilde incelenmek veya yanıtlanmak üzere olay yanıt ekiplerine taşınması gereken uyarıları hemen tespit edebilmek üzere güvenlik analistlerine yeterli bağlamı sağlar.

Kaspersky CyberTrace, analistlerin mevcut güvenlik operasyonlarında tehdit istihbaratından daha etkili bir biçimde faydalanmasına yardımcı olmak üzere tehdit verisi beslemeleri ile SIEM çözümlerini kusursuz biçimde entegre eden bir tehdit istihbaratı platformudur. JSON, STIX, XML ve CSV formatlarında her türlü tehdit istihbaratı akışıyla (Kaspersky, diğer tedarikçiler, OSINT veya kendi müşteri akışlarınızdan gelen) entegre olur ve çok sayıda SIEM çözümü ve günlük kaynağıyla kullanıma hazır entegrasyonu destekler.

Öne Çıkan Noktalar

Daha da derin analiz sağlamak için her gösterge hakkında ayrıntılı bilgiler. Her sayfa, belirli bir gösterge için tüm istihbarat sağlayıcılarından gelen bilgilerin tamamını içerir (kopyaların önlenmesi), böylelikle analistler tehditleri yorumlar kısmında tartışabilir ve her bir gösterge hakkındaki dahili tehdit istihbaratlarını ekleyebilir.

Entegre veri beslemelerinin ve bunların kesişim matrislerinin etkinliğini ölçmek için kullanılan veri beslemesi kullanım istatistikleri, en başarılı tehdit istihbaratı sağlayıcılarının seçilmesine yardımcı olur

IoC'leri etiketlemek IoC yönetimini kolaylaştırır. Herhangi bir etiket oluşturup bu etiketin önemini belirleyin ve IoC'leri manüel olarak etiketlemek için bu etiketi kullanın. Ayrıca bu etiketlere ve etiketlerin ağırlıklarına göre IoC'leri sınıflandırabilir ve filtreleyebilirsiniz

Araştırma grafiği, CyberTrace üzerinde depolanan verileri ve algılanan tehditleri görsel olarak izleyebilmenizi ve tehdit benzerliklerini görmenizi sağlar

Göstergeleri dışa aktarma özelliği, gösterge setlerinin güvenlik politikası listeleri (engelleme listeleri) gibi güvenlik kontrollerine aktarılmasına ve tehdit verilerinin Kaspersky CyberTrace vakaları veya diğer TI platformları arasında paylaşılmasına olanak verir

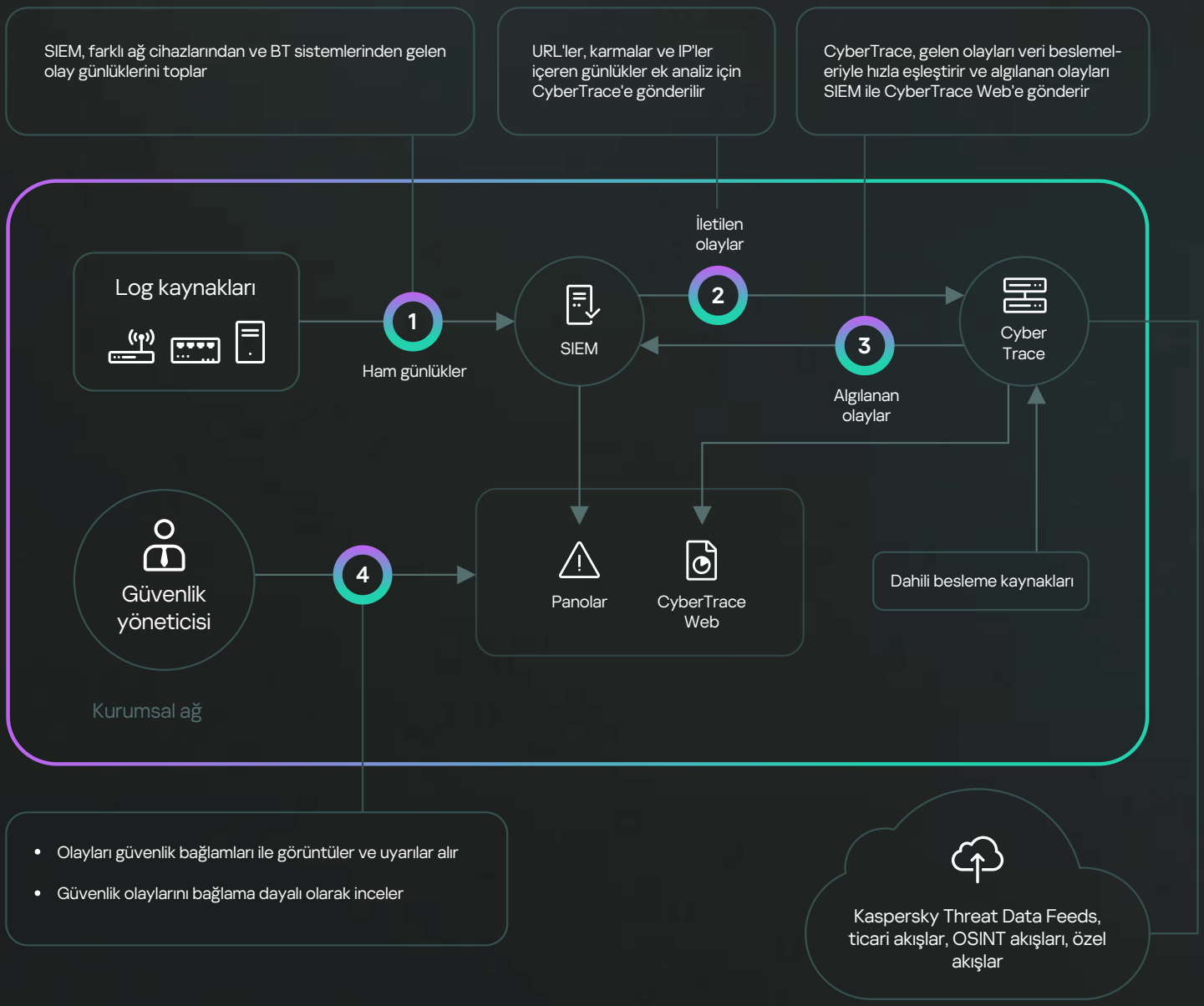
Geçmişe dönük ilişkilendirme özelliği (geçmişe yönelik tarama), geçmişte açığa çıkarılan tehditleri bulmak üzere en güncel veri beslemelerini kullanarak önceden kontrol edilen olaylardan elde edilen gözlemlenebilir verileri analiz etmenizi sağlar

Çoklu kiracılı mimari seçeneği, MSSP'leri ve büyük çaplı kurumsal kullanım durumlarını destekler

Algılanan olayları SIEM çözümlerine göndererek hem analistler hem de SIEM üzerindeki yükü azaltır

HTTP RestAPI, tehdit istihbaratlarını aramanıza ve yönetmenize yardımcı olur

Nasıl çalışır?



Kaspersky CyberTrace gelen günlükleri ve olayları ayrıştırır, elde edilen verileri akışlarla hızla eşleştirir ve kendi tehdit algılama uyarılarını oluşturarak SIEM iş yükünü önemli ölçüde azaltır.

Kaspersky Tehdit Veri Akışları ile CyberTrace kullanmanın faydaları

Çok büyük miktarlarda güvenlik uyarılarını etkili biçimde ayrıştırabilir ve önceliklendirebilir

Öncelik belirleme ve ilk müdahale süreçlerini iyileştirebilir ve hızlandırabilir

Proaktif ve istihbarata dayalı bir savunma oluşturulması

İşiniz için kritik olan uyarıların anında belirlenmesi ve IR ekiplerine iletilmesi

Kaspersky
Threat Lookup

Kaspersky Threat Lookup

Siber suçlar sınır tanımaz ve teknik kapasiteleri hızla gelişmektedir; siber suçluların hedeflerini tehdit etmek için dark web kaynaklarını kullandığı saldırıların giderek ne kadar geliştiği kolayca görülmektedir. Savunmanızı tehlikeye atacak yeni saldırı girişimi yöntemleri ortaya çıktıkça siber tehditlerin sıklığı, karmaşıklığı ve gizlenme taktikleri de sürekli artmaktadır. Saldırganlar, işletmenizin işleyişini aksatmak, varlıklarınızı çalmak veya müşterilerinize zarar vermek için karmaşık kill chain yöntemleri ve özelleştirilmiş Taktikler, Teknikler ve Prosedürler (TTP'ler) kullanmaktadır.

Kaspersky Threat Lookup, Kaspersky'nin siber tehditler ve bunların ilişkileri konusunda elde ettiği bilgi birikiminin tamamını tek ve güçlü bir web hizmeti üzerinden sunar. Amaç, güvenlik ekiplerinize mümkün olduğunca fazla veri sağlayarak siber saldırıları kuruluşunuzu etkilemeden önce önlemektir. Platform; URL'ler, etki alanları, IP adresleri, dosya grupları, tehdit adları, istatistiksel/davranışsal veriler, WHOIS/DNS verileri, dosya özellikleri, coğrafi konum verileri, indirme zincirleri, zaman damgaları vb. hakkında en güncel ve ayrıntılı tehdit istihbaratını alır. Sonuç olarak, yeni ve büyümekte olan tehditler küresel çapta görünür hale gelir; bu da kuruluşunuzun güvenliğini sağlamanıza yardımcı olur ve olaylara müdahaleyi destekler.

Nasıl çalışır?

Analiz edilecek nesneler

Öne Çıkan Noktalar

Güvenilir İstihbarat

Kaspersky Threat Lookup'ın önemli bir özelliği, eyleme geçirilebilir bağlam verileriyle zenginleştirilmiş tehdit istihbaratı verilerimizin güvenilirliğidir. Kaspersky, kötü amaçlı yazılım testlerinde alanında lider konumundadır ve sıfıra yakın hatalı pozitif sonuçla en yüksek algılama oranlarını elde ederek güvenlik istihbaratımızın benzersiz kalitesini kanıtlamıştır.

Tehdit Avlama

Saldırıların etkilerini ve sıklıklarını en aza indirmek için saldırıları önlemede, saptamada ve yanıtlamada proaktif olun. Saldırıları takip ederek en kısa zamanda etkili bir şekilde ortadan kaldırın. Bir tehdidi ne kadar erken fark ederseniz o kadar az hasara neden olur, onarımlar o kadar hızlı yapılır ve ağ operasyonları o kadar erken normale döner.

Kullanımı kolay

Web arabirimi veya RESTful API. Hizmeti manüel modda bir web arayüzü (web tarayıcısı) veya basit bir RESTful API aracılığıyla kullanın — hangisini tercih ederseniz

Çok çeşitli dışa aktarma formatları

Tehdit istihbaratının tüm avantajlarından faydalanmak, operasyon iş akışını otomatikleştirmek veya SIEM'ler gibi güvenlik kontrollerini entegre etmek için, IOC'leri (Güvenlik İhlal Göstergeleri) veya eyleme geçirilebilir bağlamı STIX, OpenIOC, JSON, Yara, Snort ve hatta CSV gibi yaygın olarak kullanılan ve daha düzenli, makine tarafından okunabilen paylaşım biçimleri olarak dışa aktarın.

Kaspersky Threat Lookup faydaları

1. Saldırıları önceliklendirmenize ve işletmeniz için en çok risk teşkil eden tehditleri en aza indirmeye odaklanmanıza olanak tanıyan yüksek düzeyde doğrulanmış tehdit bağlamı ile tehdit göstergeleriyle ilgili ayrıntılı aramalar yapın
2. Ana bilgisayarlar ve ağ üzerindeki güvenlik olaylarını daha verimli ve etkili bir şekilde tanımlayıp analiz edin ve bilinmeyen tehditlere karşı dahili sistemlerden gelen sinyalleri önceliklendirin
3. Kritik sistemler ve veriler tehlikeye girmeden kill chain'i bozmak için olay müdahalesi ve tehdit yakalama yetkinliklerinizi geliştirin
4. Web tabanlı bir arabirimden veya RESTful API aracılığıyla tehdit göstergelerini arayabileceksiniz
5. Yeni şüpheli nesneleri bulmak için sertifikalar, sık kullanılan adlar, dosya yolları veya ilgili URL'ler dahil olmak üzere gelişmiş ayrıntıları inceleyebileceksiniz
6. Keşfedilen tehdit unsurunun yaygın veya özgün olup olmadığını kontrol edin ve bu tür bir unsurun neden kötü niyetli olarak ele alınması gerektiğini anlayın

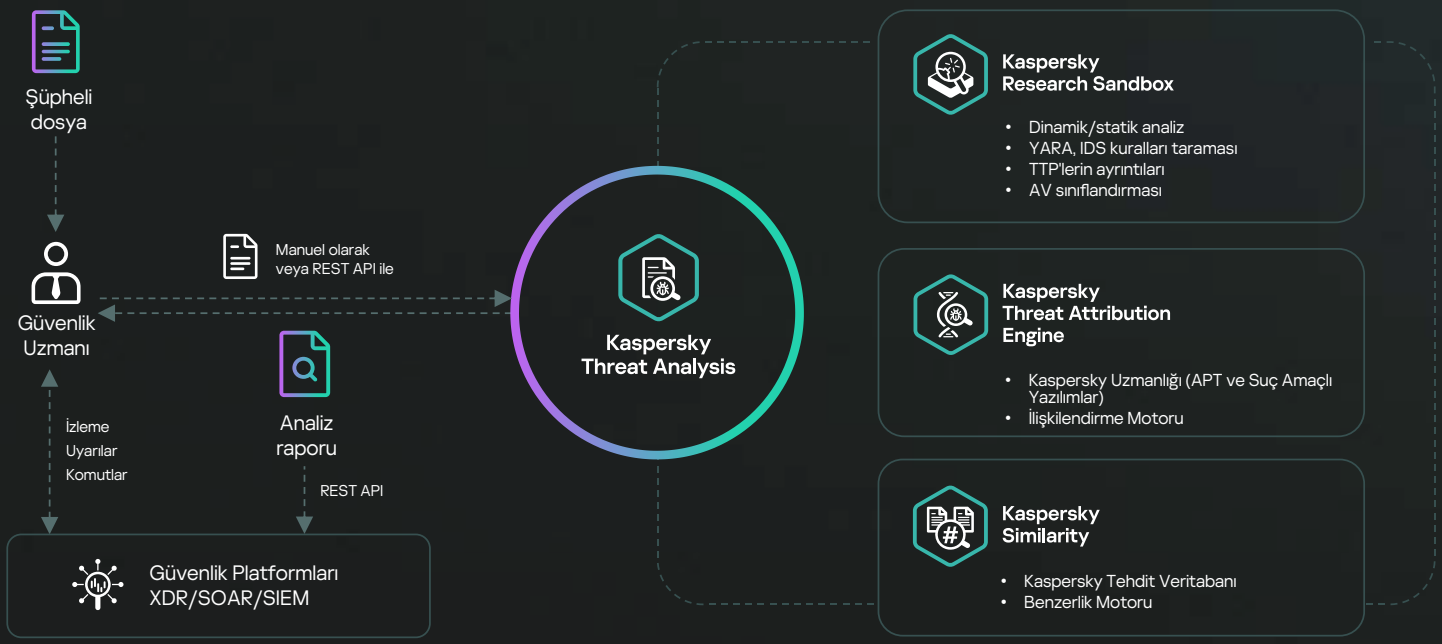
Kaspersky
Threat Analysis

Kaspersky Tehdit Analizi

Potansiyel bir siber tehditle karşı karşıya kaldığınızda, verdiğiniz kararlar ve bu kararları ne kadar iyi verebildiğiniz kritik öneme sahip olabilir. Günümüzün hedefli saldırılarını yalnızca geleneksel anti virüs araçlarıyla önlemek mümkün değildir. Anti virüs motorları sadece bilinen tehditleri ve bunların türevlerini durdurma kabiliyetine sahipken gelişmiş tehdit aktörleri otomatik tespiti atlatmak için ellerindeki tüm araçları kullanır. Her gün SOC'leri tarafından işlenen güvenlik uyarılarının sayısı katlanarak artıyor. Her gün üretilen kötü amaçlı yazılım örneklerinin miktarı göz önüne alındığında, etkili uyarı önceliklendirme, öncelik belirleme ve doğrulama neredeyse imkansız hale gelmektedir.

Kaspersky, güvenlik araştırmacılarının var olan ve yeni ortaya çıkan tehditler hakkında bilgi sahibi olmalarına yardımcı olmak için şüpheli dosyaların rutin analizini otomatikleştiren tek bir esnek çerçeve sunuyor. Kaspersky Tehdit Analizi, sandboxing gibi geleneksel tehdit analizi teknolojilerine ek olarak sizi en gelişmiş ilişkilendirme ve ilgili benzerlik teknolojileriyle donatır. Etkili tehdit analizi sağlayan bu hibrit yaklaşım, tamamen bilinçli kararlar verebilir ve böylece altyapınızı güvende tutabilirsiniz. Kaspersky Tehdit Analizi, hem birleşik web hem de RESTful arayüzleri aracılığıyla sağlanır.

Kaspersky Tehdit Analizi bileşenleri



Kaspersky
Research Sandbox

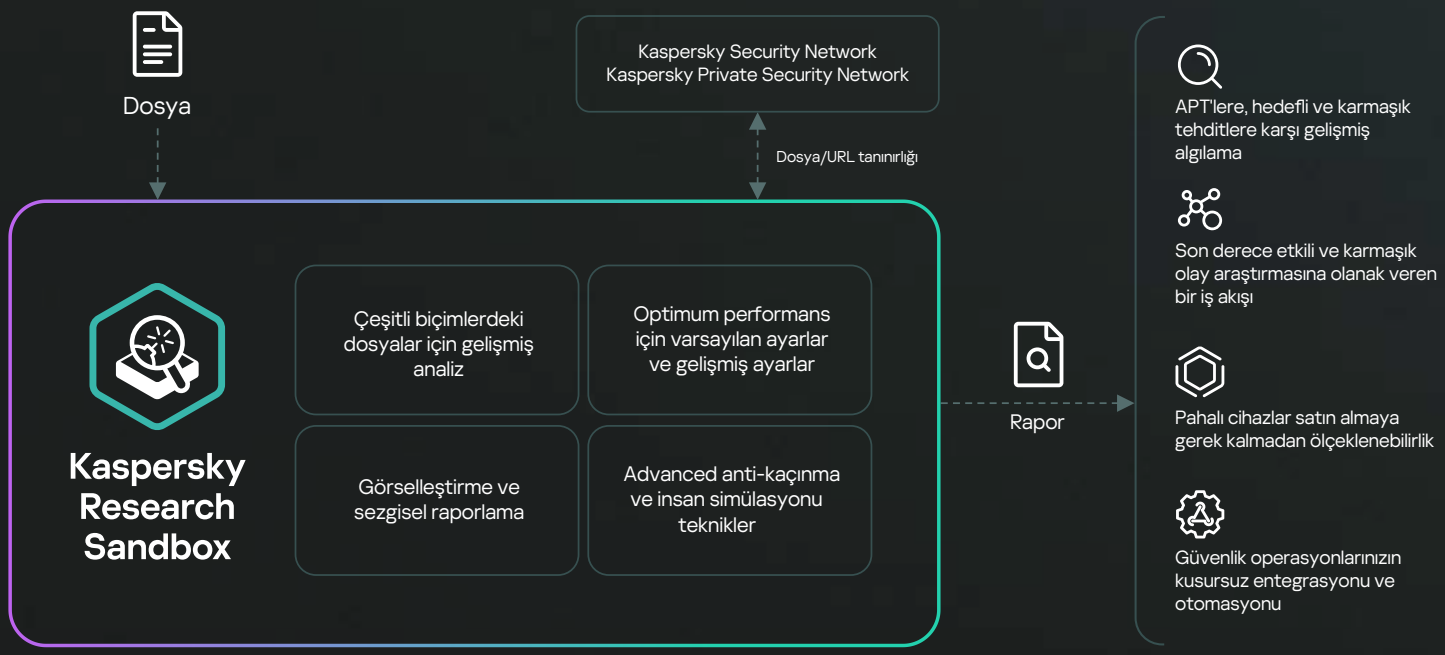
Kaspersky Research Sandbox

Kaspersky Research Sandbox, doğrudan yirmi yıldan fazla bir süredir gelişen bir teknoloji olan laboratuvar kullanımına yönelik korumalı alan kompleksimizden geliştirilmiştir. Kesintisiz tehdit araştırmalarımız boyunca edindiğimiz kötü amaçlı yazılım davranışları hakkındaki tüm bilgileri bir araya getirirken aynı zamanda her gün 420.000'den fazla yeni kötü amaçlı nesneyi tespit etmemizi sağlar.

Kaspersky Research Sandbox, dosya örneklerinin kökenlerini araştırmanıza, davranış analizine dayalı IOC'ler toplamanıza ve daha önce görülmemiş kötü amaçlı unsurları tespit etmenize olanak tanır. Davranışsal analiz ve sarsılmaz atlatma karşıtı tekniklerini, otomatik tıklayıcı, belge kaydırma ve sahte süreçler gibi insan simülasyonu teknolojileriyle birleştiren hibrit bir yaklaşım sunar.

Tesislerde kullanıldığında bu teknoloji, verilerin kuruluş dışında açığa çıkarılmasını da önler. Kaspersky Research Sandbox, analiz için gerçek ortamlara uyarlanmış özel yürütme ortamları oluşturmaya da olanak tanıyarak tehdit tespitinin doğruluğunu ve araştırma hızını artırır.

Nasıl çalışır?



Ürün özellikleri

- Patentli teknoloji
- Windows, Linux ve Android ortamlarında otomatik hâle getirilmiş nesne analizi
- Ayrıntılı analiz raporları ile 200'den fazla dosya türü için analiz desteği
- MITRE ATT&CK tarafından TTP'lerin çıkarılması için 1000'den fazla benzersiz av
- Gelişmiş atlatma karşıtı teknikler ve insan simülasyonlu teknolojiler
- Dosya yürütme sırasında elde edilen ölçümler ve verilere dayalı tehdit puanı, analiz edilen nesnenin tehlike düzeyini gösterir
- Dosya yürütme sırasında oluşan ağ trafiğini incelemek için önceden yapılandırılmış Suricata kuralları
- Manuel örnek yükleme ve otomatik iş akışlarıyla entegrasyon için geliştirilmiş REST API

Kaspersky
Threat Attribution
Engine

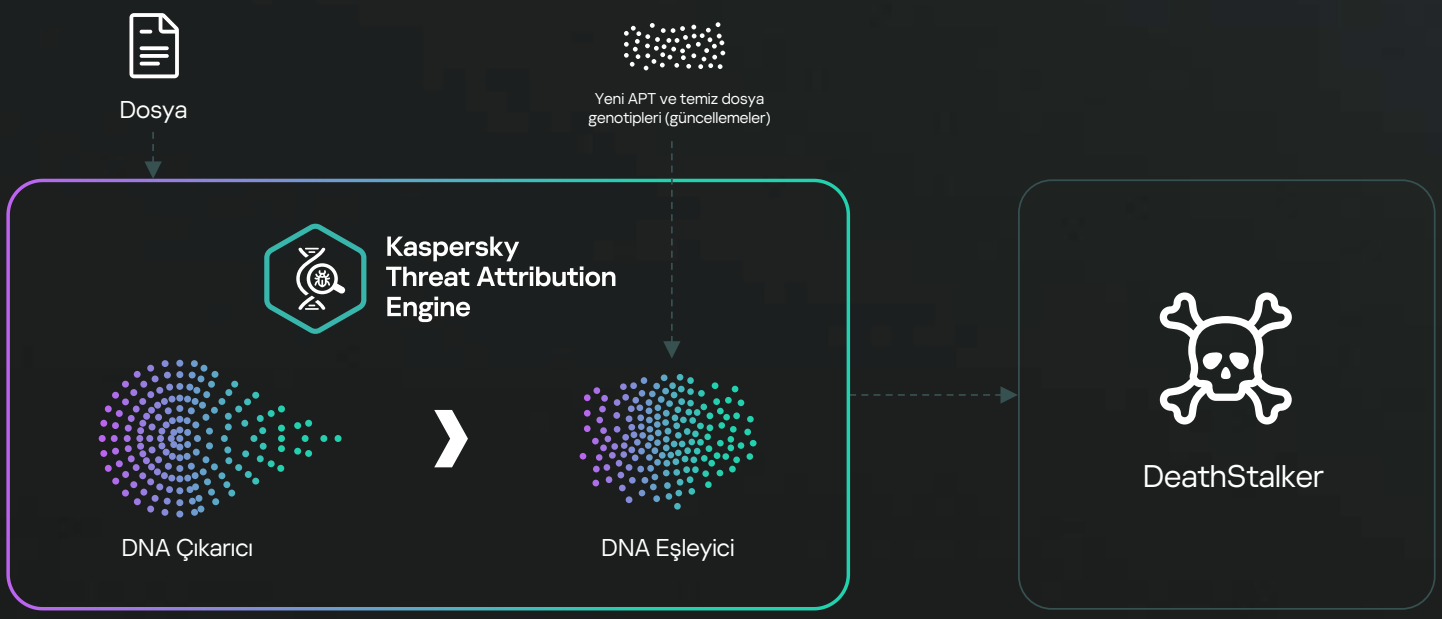
Kaspersky Threat Attribution Engine

Kaspersky Threat Attribution Engine, yüksek profilli kötü amaçlı yazılımların kaynağı ve olası yazarları hakkında derinlemesine bilgi sağlayan benzersiz bir tehdit analiz aracıdır. Benzersiz bir algoritma ve APT kötü amaçlı yazılım örnekleri ile Kaspersky uzmanları tarafından son 25 yılda toplanan sektörün en büyük temiz dosya koleksiyonunu içeren özel bir veritabanı kullanarak şüpheli bir dosyayı bilinen APT tehditlerine, aktörlerine, kampanyalarına hızlı bir şekilde bağlar.

1100'den fazla tehdit aktörünü ve saldırılarını takip ediyor ve yılda 200'den fazla tehdit istihbarat raporu yayınlıyoruz. Sürmekte olan araştırmalarımız 100.000'den fazla dosya içeren bir APT koleksiyonunu desteklemekte ve otomatik araçların kullanımıyla birlikte olağanüstü doğrulukta ilişkilendirme seviyesi elde edilmektedir.

Ürün, sıfıra yakın yanlış pozitif oranları sağlarken, benzer numuneleri karşılaştırmak için de benzersiz bir yaklaşım sunar. Herhangi bir yeni saldırı, bilinen APT kötü amaçlı yazılımları, önceki hedefli saldırılar ve bilgisayar korsanı grupları ile hızlı bir şekilde ilişkilendirilebilir, bu da yüksek riskli tehditleri daha az ciddi olaylardan ayırt etmenize yardımcı olur. Böylece bir saldırganın sisteminizde bir yer edinmesini önlemek için zamanında koruyucu önlemler alabilirsiniz. Kaspersky Threat Attribution Engine, 3. tarafların işlenmiş bilgilere ve gönderilen tehdit unsurlara erişimini önlemek için güvenli ve ayrı ortamlarda kurulabilir. Kurum içi dağıtım, özel koleksiyonunuzdaki dosyalara benzer örnekleri tespit etmek için kendi aktörlerinizi ve örneklerinizi eklemenin yanı sıra altyapınızdaki benzer dosyalar için daha fazla otomatik arama ve üçüncü taraf çözümlerle entegrasyon sağlamak üzere YARA kurallarını dışa aktarmak için ek işlevsellik sağlar.

Nasıl çalışır?



Tescilli arama yöntemi

Kaspersky Threat Attribution Engine, kötü amaçlı yazılımları ilişkilendirme varlıklarına bağlamak için dosyalar arasındaki benzerlikleri arayan benzersiz bir tescilli yöntem kullanır. Bu yöntem şunları içermektedir:

1

Kodundan yola çıkarak aşağıdaki hususları ortaya koyup bir örneğin genetiğini analiz etme:

- Genotipler — ikili kodun ayırt edici parçaları.
- Dizeler — ayırt edici karakter dizeleri.

2

Analiz edilen dosyalarda, daha önce analiz edilen APT örneklerinin genotiplerine ve dizelerine benzeyen veya zaten ilişkilendirilmiş varlıklarla bağlantılı olan genotiplerin ve dizelerin otomatik olarak aranması.

3

APT örneklerinde bulunan benzer genotiplere ve dizelere dayanarak, analiz edilen örneğin kökeni, ilişkilendirilen varlıklar ve bu örnek ile bilinen APT örnekleri arasındaki benzerlikler hakkında bir rapor sunar.

Ürünün öne çıkan özellikleri

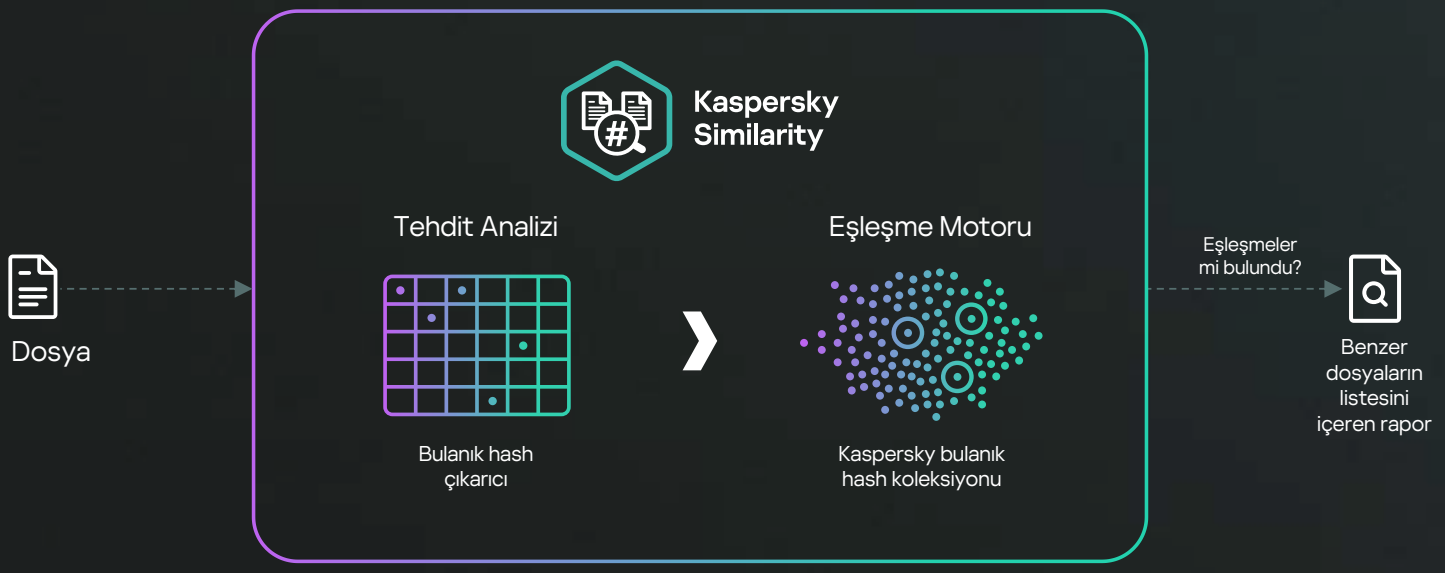
- Patentli teknoloji
- Yüzlerce APT aktörü, örneği ve kampanyasıyla ilgili düzenlenen verileri içeren bir depoya anında erişim sunar
- Manuel örnek yükleme ve otomatik iş akışlarıyla entegrasyon için geliştirilmiş REST API
- Parola korumalı arşivleri özel parolalarla açmak için işlevsellik
- Güvenlik günlüklerinin daha fazla otomatik analizi veya üçüncü taraf çözümleri ile entegrasyon için STIX 2.1 biçimine aktarma yapın (TXT ve JSON biçimleri de desteklenir)
- Amazon Web Services (AWS) gibi bulut altyapılarında dağıtımı destekleyerek hızlı ürün kurulumu sağlar ve önceden donanım yatırımı yapmaya gerek olmadığından maliyet tasarrufu sağlar

Kaspersky Intelligence Reporting

Kaspersky Similarity

Kaspersky Similarity, bilinmeyen ve gizli tehditlere karşı koruma sağlamak için Kaspersky uzmanları tarafından geliştirilen teknolojiye dayanan benzer işlevselliğe sahip dosyaları tanımlamak için kullanışlı bir araçtır. Bu teknoloji, sonuçların en yüksek doğruluk ve güvenilirliğini sağlamak için 50'den fazla benzersiz özel karma türünü ve Kaspersky tarafından 25 yıl boyunca biriktirilen ve milyonlarca kötü amaçlı dosya içeren kötü amaçlı yazılım örneklerinden oluşan bir veritabanını kullanır.

Kaspersky Similarity, benzer (örneğin kaçamak) kötü amaçlı yazılım örneklerini bulmanızı ve bunları altyapıda aramanızı sağlayarak, örnek üzerinde düşman tarafından yapılan küçük bir değişikliğin bile güvenlik radarınızda olduğundan emin olmanızı sağlar.



Benzerlik raporları

Kaspersky uzmanları, bu özniteliklere dayanarak farklı dosyalar arasındaki benzerlikleri belirlemek için bir dizi karma oluşturdu.

Kaspersky Similarity, kullanıcıların şüpheli bir dosya göndermesine, karmalarını çıkarmasına ve bunları Kaspersky tehdit veritabanında bulunan dosyaların karmalarıyla karşılaştırmasına olanak tanır. Eşleşmelerin bulunması durumunda, Kaspersky tarafından zaten bilinen ve benzerlik puanına göre sıralanan TOP benzer kötü amaçlı dosyalar için karma listesi oluşturur. Rapor, her benzer dosya için meta verilerle birlikte ek bağlam içerir:

- Benzerlik güveni
- Dosya durumu (kötü amaçlı yazılım, reklam yazılımı veya diğer)
- Tehdit adı
- İlk ve son tespitin zaman damgaları
- İsabet sayısı (tespitler)
- Dosya karması
- Dosya türü
- Dosya boyutu

Öne Çıkan Noktalar

- Patentli teknoloji
- En yüksek karşılaştırma doğruluğu için maksimum kapsam sağlayan, 25 yıldan uzun süredir toplanmakta olan kötü amaçlı ve temiz dosyalardan oluşan sektördeki en büyük veritabanlarından birini kullanır
- Manuel örnek yükleme ve otomatik iş akışlarıyla entegrasyon için geliştirilmiş REST API
- Bu teknoloji, Kaspersky uzmanları tarafından, bağımsız testler tarafından düzenli olarak en yüksek oranlarla onaylanan ürünlerimizde daha da yüksek tehdit koruması sağlamak amacıyla yeni tehditleri keşfetmek için uzun süredir kullanılmaktadır:

Daha fazla bilgi edinin

Kaspersky Threat Lookup faydaları

1

Kaspersky Research Sandbox ile olaylara müdahale ve adli tıp faaliyetlerinizi güçlendirin. 0 gün tehditleri ve MITRE ATT&ACK TTP'leriyle eşleştirilmiş sonuçları bulma becerisine sahip şüpheli dosyaların en son dinamik analizini sağlar.

2

Kaspersky Threat Attribution Engine ile doğru ve zamanında ilişkilendirme, tehdit aktörünü TTP'lerin tam listesine göre tanımlamaya yardımcı olarak saldırı vektörünün kapsamlı bir görünümünü ve olay müdahale sürelerini aylardan dakikalara indirmeyi sağlayan belirgin hafifletme adımlarını sunar.

3

Geleneksel kötü amaçlı yazılımdan koruma teknolojilerini atlatmak için özel olarak oluşturulmuş kötü amaçlı örnekleri bulmayı sağlayan Kaspersky Similarity ile sinsi tehditleri ortaya çıkarın, bu sayede takip edilmeden yıllarca sürebilen en karmaşık APT saldırılarını tespit edebilirsiniz.

Kaspersky Intelligence Reporting

Kaspersky Tehdit İstihbaratı Raporlaması

Modern siber tehditlerle mücadele etmek için tehdit aktörleri tarafından kullanılan taktik, teknik ve prosedürlerin her yönüyle bilinmesi gerekir. Saldırılarda kullanılan C&C'ler ve araçlar sık sık değişirken saldırganların saldırıyı gerçekleştirme davranışlarını ve yöntemlerini değiştirmeleri zordur. Bu şablonların derhal tespit edilmesi etkin savunma mekanizmalarını önceden uygulayarak siber suçluların gücünü azaltmaya ve saldırı yapısını bozmaya yardımcı olur.

Kaspersky Tehdit İstihbaratı Raporlama'ya abone olarak araştırmalarımıza sürekli özel erişim sağlayabilir, en tehlikeli tehditler hakkında güncel bilgiler edinebilir, sizin ve güvenlik ekibinizin saldırıları zamanında tespit etmek için proaktif olarak etkili bir strateji uygulayabilmesini ve benzer tehditlerden kaynaklanan zararı en aza indirebilmesini sağlayabilirsiniz.

Araştırmalarımızın yalnızca küçük bir yüzdesi kamuya açıklanırken, Kaspersky Intelligence Reporting size en son tehditlerle ilgili en güncel bilgilere ayrıcalıklı erişim sağlar. Uzmanlarımız siber suçluların faaliyetlerini sürekli olarak izleyerek en sofistike ve tehlikeli hedefli saldırıları, siber casusluk kampanyalarını, kötü amaçlı yazılım ve şifreleme örneklerini ve dünyadaki en son siber suç trendlerini tespit etmektedir.

200+	300+	500+	2500+	170 000+
yıllık bazda özel rapor	tehdit aktörleri	kampanya	YARA kuralları	IOC'ler

Analiz raporlarına şunlar dâhildir:

Tehdit aktörü profilleri

MITRE ATT&CK'e eşleme

Yönetici özeti (C-düzeyi odaklı bilgiler)

Derin teknik analize şunlar dâhildir:

- Saldırı yöntemleri
- Kullanılan açıklardan yararlanma yöntemleri
- Kötü amaçlı yazılım açıklaması
- C&C altyapı ve protokollerinin açıklaması
- Kurban analizi
- Veri sızdırma analizi
- İlişkilendirme

Güvenlik İhlal Göstergeleri (IOC'ler) ve YARA/SIGMA/ Suricata kuralları

Kaspersky uzmanlarından öneriler

İhtiyaçlarınıza ve kuruluşunuzun özelliklerine göre farklı ticari raporlama yolları sunuyoruz:

Kaspersky APT Intelligence Reporting

Genellikle iyi organize olmuş ve iyi finanse edilen gruplardan kaynaklanan sofistike, uzun vadeli hedefli siber tehditler hakkında içgörü sağlar. Dünya çapındaki çeşitli APT grupları ve bunların taktikleri, teknikleri ve prosedürlerinin (TTP'ler) yanı sıra hedefledikleri sektörler ve bölgeler hakkında bilgiler içerir. Bu raporlama yolu, tedarik zinciri saldırılarından hacktivist ve yıkıcı faaliyetlere kadar uzanan casusluk faaliyetlerine odaklanmaktadır. Bu raporlar, kuruluşunuz büyük bir şirket, devlet kurumu veya kritik altyapıyla ilgili bir kuruluş ise idealdir ve özellikle devlet kurumlarının ilgi alanına girebilecek hassas verilere sahip kuruluşlar için de uygundur.

Kaspersky Crimeware Intelligence Reporting

Öncelikli hedefi mali kazanç olan saldırı ve kampanyalara odaklanır. Darkweb'de satılan çalıntı veriler, finansal dolandırıcılık, fidye yazılımları ve ATM/PoS kötü amaçlı yazılımları da kapsayan siber suçlardaki son trendler hakkında bilgiler içerir. Yeni suç yazılımı çeşitleri, dağıtım yöntemleri ve hedefledikleri veri türleri hakkında ayrıntılar sağlarlar. Bu raporlama yolu, özellikle kuruluşunuz önemli miktarda çevrimiçi iş yapıyorsa veya örneğin bir finans kurumu veya e-ticaret platformu olarak hassas müşteri verilerine sahipseniz önemlidir.

Kaspersky ICS Threat Intelligence

Endüstriyel kuruluşları hedef alan kötü niyetli kampanyalar hakkında derinlemesine istihbarat ve daha fazla farkındalık sağlamanın yanı sıra en popüler endüstriyel kontrol sistemlerinde ve temel teknolojilerde bulunan zayıf noktalar hakkında bilgi sağlar Bu raporlama yolu, 2016 yılında kurulan ICS tehdit ve güvenlik açığı araştırması, olay müdahalesi ve güvenlik analizi konularında 30'dan fazla yüksek nitelikli uzmandan oluşan özel bir ekip olan Kaspersky ICS CERT tarafından sunulmaktadır. Bu raporlar, yazılım ve donanım bileşenleri de dâhil tüm kritik varlıklarınızı korumak ve teknolojik süreçlerinizin güvenliğini ve sürekliliğini sağlamak için eyleme geçirilebilir içgörüler ve rehberlik sağlar.

Aşağıdaki ilgili Kaspersky ICS Tehdit İstihbaratı hizmetlerini göz önünde bulundurmak isteyebilirsiniz:

ICS Tehdit İstihbaratı Raporlaması

Endüstriyel siber güvenlik tehditleri ve güvenlik açıkları hakkındaki düzenli yayınlarımıza abonelik:

- 0 gün tehditleri hakkında uyarılar
- Detaylı teknik raporlar
- Aylık değerlendirmeler
- Güvenlik açığı azaltımlarına ilişkin öneriler
- İstatistikler ve eğilimler

ICS Tehdit Veri Akışları

Endüstriyel siber güvenlik tehditleri ve güvenlik açıkları hakkında makine tarafından okunabilir veri akışları.

HTTPS, TAXII ve bilgi güvenliği çözümlerine entegrasyon için özel dağıtım yöntemleri aracılığıyla basit veri dağıtım formatları (JSON, CSV, OpenIoC, STIX).

Ask the Analyst hizmeti

Kaspersky ICS CERT uzmanları ile danışmanlık alarak endüstriyel siber güvenlik tehditleri ve güvenlik açıkları, tehdit istatistikleri ve alanı, endüstri standartları vb. konularda size en uygun tavsiyeleri alabilirsiniz.

Kaspersky Tehdit İstihbaratı Raporlaması size şunları sunar:

Ayrıcalıklı erişim

Çeşitli nedenlerle, yüksek profilli tehditlerin tamamı hakkında kamuya bilgi verilmez. Ancak, bu tür özel bilgileri müşterilerimize soruşturma sürecinde, hatta resmi kamuoyu duyurusundan önce sağlıyoruz.

Teknik verilere erişim

OpenIOC veya STIX'i de içeren standart formatlardaki genişletilmiş bir IOC listesine ve YARA/Sigma/Suricata kurallarımıza erişim dâhildir

Tehdit aktörü profilleri

Şüpheli kaynak ülke ve ana faaliyet, kullanılan kötü amaçlı yazılım aileleri, hedeflenen sektörler ve coğrafyalar ve MITRE ATT&CK ile eşleme ile birlikte, kullanılan tüm TTP'lerin açıklamaları dâhildir.

MITRE ATT&CK

Raporlarda açıklanan tüm TTP'ler, MITRE ATT&CK ile eşlenerek ilgili güvenlik izleme kullanım durumlarının geliştirilmesi ve önceliklendirilmesi, açıklık analizlerinin yapılması ve mevcut savunmaların ilgili TTP'lere karşı test edilmesi yoluyla daha iyi algılama ve müdahale sağlar.

Geriye dönük analiz

Abonelik döneminiz boyunca, önceden hazırlanan tüm özel raporlara erişim olanağı sunulur.

RESTful API desteği

Güvenlik iş akışlarınızın sorunsuz entegrasyonu ve otomasyonu.

Kaspersky
Digital Footprint
Intelligence

Kaspersky Dijital Ayak İzi İstihbaratı

İşletmeniz büyüdükçe, BT ortamlarınızın karmaşıklığı ve dağılımı da artar. Bunun sonucunda, geniş çapta dağılmış dijital varlığınızı doğrudan kontrol edebilme ve koruma sorunu ortaya çıkarır. Dinamik ve birbirine bağlı ortamlar, şirketlerin önemli avantajlar elde etmesine olanak verir. Ancak sürekli artan bağlanabilirlik, saldırı yüzeyini de genişletir. Siber saldırganlar daha becerikli hale geldikçe, sadece kuruluşunuzun çevrimiçi varlığının doğru bir genel görünümünü elde etmek değil, aynı zamanda şirketinizde meydana gelen değişiklikleri izlemek ve saldırılara açık dijital alanlarla ilgili güncel bilgileri anında kullanabilmek de onlar için önemli hale gelir.

Kuruluşlar, güvenlik operasyonlarında çok çeşitli güvenlik araçları kullanır ancak hala ortaya çıkabilecek dijital tehditlere karşı bazı özel önlemler almak gerekir. Bu önlemlere, veri sızıntılarını tespit etmek ve azaltmak, dark web forumlarında bulunan siber suçluların planlarını ve saldırı şemalarını izlemek vb. örnek verilebilir. Kaspersky, güvenlik analistlerinizin, saldırganların şirketinizin kaynaklarına nasıl yaklaştıklarını anlamalarına, kullanabilecekleri potansiyel saldırı vektörlerini anında keşfetmelerine ve savunmalarını buna göre ayarlamalarına yardımcı olmak için Kaspersky Dijital Ayak izi İstihbaratı'nı geliştirdi.

Kaspersky Dijital Ayak İzi İstihbaratı şunları sunar:

Tehdit Algılama

Şirketin itibarına zarar verebilecek ve/veya müşterileri aldatabilecek dolandırıcılık faaliyetlerinin izlenmesi.

Ağ keşifleri

Bir saldırı için potansiyel giriş noktası olan müşteri ağ kaynaklarının ve açıkta kalan hizmetlerinin tanımlanması. CVSS taban puanına, genel kullanıma açık yapılardaki açıklardan yararlanılabilirliğe, sızma testi deneyimine ve ağ kaynağının konumuna (barındırma/altyapı) dayalı daha fazla puanlama ve kapsamlı risk değerlendirmesiyle mevcut güvenlik açıklarının söz konusu müşteriye özel analizi.

Dark Web izlemesi

Dark web kaynaklarının (forumlar, fidye yazılım blogları, mesajlaşma uygulamaları, tor siteleri vb.) sürekli olarak izlenmesi, şirketiniz, müşterileriniz ve ortaklarınızla ilgili her türlü referans ve tehdidin tespit edilmesi. Herhangi bir aktif hedefli saldırının veya planlanan saldırının veya şirketinizi, sektörünüzü veya bölgenizi hedef alan APT saldırılarının analizi.

Veri sızıntılarının bulunması

Saldırı gerçekleştirmek için kullanılabilecek veya şirketiniz için itibar riski oluşturabilecek çalışanlarınıza, iş ortaklarınıza ve müşterilerinize ait gizliliği ihlal edilmiş kimlik bilgilerinin, banka kartlarının, telefon numaralarının ve diğer hassas bilgilerin tespiti.

Çoklu kullanım desteği

Yönetilen güvenlik hizmeti sağlayıcıları (MSSP'ler) ve çok şubeli bir yapıya sahip büyük kuruluşlar için geliştirilmiş yetenekler.

İstihbarat kaynakları

Şirketinizin güvenlik uygulamalarının karşıdan nasıl gözüktüğü hakkında kapsamlı bilgi sahip olmanız çok önemlidir. Kaspersky güvenlik analistleri, bu bilgileri sağlamak için aşağıdaki istihbarat kaynaklarından bilgi toplar ve bir araya getirir:

Yapılandırılmamış verileriniz

- IP adresleri
- Şirket etki alanları
- Marka adları
- Anahtar kelimeler
- Ağ menzilleri
- BIN/IIN kart numaraları
- Çalışan bilgileri

Ağ çevresi envanteri

Surface, deep ve dark web araması

Kaspersky Bilgi Tabanı araması

Tehdit uyarıları

Kaspersky kaynaklarına ek olarak surface ve dark web kaynaklarında gerçek zamanlı arama

Analiz raporları*

Nasıl çalışır?

Yapılandır	Topla	Filtrele	Bildirim
Şirketin dijital varlıkları hakkında bilgi keşfi	Surface, deep and dark web'den ve Kaspersky bilgi bankasından otomatik veri toplama	Analistler tarafından yönetilen tehdit tespiti, analizi ve önceliklendirmesi	Kaspersky Threat Intelligence Portal'da veya API aracılığıyla hızlı tehdit bildirimleri sağlanması

* Eklenti hizmeti

Dijital Ayak İzi İstihbaratı iş değerleri

Kaspersky Dijital Ayak İzi İstihbaratı, kuruluşunuza güçlü avantajlar ve önemli bir artı değer sunar:

Tehdit algılama

Marka itibarınızı korumak, müşterilerinizin güvenini muhafaza etmek, finansal kayıp riskini en aza indirmek ve iş operasyonlarının zarar görmesini engellemek için potansiyel tehditleri gerçek zamanlı olarak tespit edin.

Siber riskleri azaltın

Mevcut BT yapınızdaki boşlukları ve bunların doğurduğu riskleri ortaya çıkararak kilit paydaşlarınızı (CxO ve Yönetim Kurulu) siber güvenlik harcamalarını nereye odaklamanız gerektiği konusunda bilgilendirin

Daha hızlı tepki verin

Güvenlik uyarıları için tanımlayacağınız ek bağlamlar, olay müdahalesini iyileştirir ve Ortalama Yanıt Verme Sürenizi (MTTR) azaltır

Saldırı yüzeyinizi azaltın

Bir saldırıda kullanılabilecek saldırı vektörlerini ve güvenlik açıklarını en aza indirmek için şirketinizin dijital varlığını yönetin ve harici ağ kaynaklarını denetleyin.

Siber düşmanlarınızı anlayın

Erken kalkan çabuk yol alır - siber suçluların dark web'de şirketiniz hakkında neler planladığını ve konuştuğunu önceden bilin ki bunlara karşı hazırlıklı olun.

Bilinmeyeni bilin

Siber saldırılara karşı koyma ve şirketiniz bünyesindeki güvenlik ekiplerinin yetki alanı dışındaki tehditleri tespit etme becerinizi geliştirin.

Hizmet sunumu verimliliği

Çoklu kullanıcı modunda hızlı başlangıç ve kolay ölçeklendirme, hem yönetilen güvenlik hizmeti sağlayıcıları (MSSP) ve müşterileri hem de çok ortaklı büyük kuruluşlar için zaman kazandırır.

Kaspersky Takedown Service

Kaspersky Takedown Hizmeti

Siber suçlular, şirketinize ve markalarınıza saldırmak için kullanılan, kötü amaçlı ve kimlik avına yönelik etki alanları oluşturur. Bu tehditlerin tespit edilip hızla ortadan kaldırılamaması, gelir kaybına, markanızın zarar görmesine, müşteri güveninin yitirilmesine, veri sızıntılarına ve daha fazlasına yol açabilir. Ancak bu alanların kaldırılmasını yönetmek, uzmanlık ve zaman gerektiren karmaşık bir süreçtir.

Kaspersky Takedown Hizmeti, kötü amaçlı ve kimlik avına yönelik domain'lerin yol açtığı tehditleri markanız ve işletmeniz herhangi bir zarar görmeden önce hızla azaltır. Bütün sürecin uçtan uca yönetimi müşterilere değerli zaman ve kaynak tasarrufu sağlar. Bu hizmet küresel olarak sunulur.

Kaspersky, her gün 15.000'den fazla kimlik avı/sahtekarlık amaçlı URL'yi ve bu tür URL'lere tıklamaya yönelik bir milyonun üzerinde girişimi engeller. Kötü amaçlı ve kimlik avına yönelik domain'leri analiz etme konusunda yıllar boyu edindiğimiz deneyim, bu domain'lerin kötü amaçlı olduğunu göstermek için gerekli tüm kanıtları nasıl toplayacağımızı bildiğimiz anlamına gelmektedir. Ekibinizin diğer öncelikli görevlerine odaklanabilmesini sağlamak amacıyla etki alanı kaldırma yönetiminizi biz üstleneceğiz ve dijital riskinizi en aza indirgemek için hızla harekete geçme olanağı sağlayacağız.

Kaspersky, uluslararası kuruluşlar, ulusal ve bölgesel emniyet teşkilatları (örn. INTERPOL, Europol, Microsoft Dijital Suçlar Birimi, Hollanda Polisinin Ulusal Yüksek Teknoloji Suç Birimi (NHTCU) ve Londra Şehir Polisi) ve dünya genelindeki Bilgisayar Acil Yanıt Ekipleri (CERT'ler) ile birlikte çalışarak, müşterilerine çevrimiçi hizmetleri için etkili koruma ve itibar sağlar.

Tam görünürlük

Talebinizin kaydedilmesinden ilgili tehdidin başarılı bir şekilde kaldırılmasına kadar, sürecin her aşamasında size bilgi vereceğiz

Uçtan uca yönetim

Bütün kaldırma sürecini yöneterek sizin katılımınızı en aza indireceğiz

Küresel kapsam

Bir kötü amaçlı veya kimlik avına yönelik domain'in nerede kayıtlı olduğu önemli değildir; Kaspersky, ilgili yasal yetkiye sahip bölgesel kuruluştan bu alanın kaldırılmasını talep edecektir

Nasıl çalışır?

Taleplerinizi kurumsal müşteri destek portalımız olan Kaspersky Şirket Hesabı üzerinden gönderebilirsiniz. Gerekli tüm belgeleri hazırlayarak kaldırma talebini, domain'i kapatmak için gerekli yasal haklara sahip olan ilgili yerel/bölgesel makama (CERT, kayıt kurumu vb.) göndereceğiz. İstenen kaynak başarıyla kaldırılana kadar sürecin her adımında bilgilendirileceksiniz.

Kolay koruma

Kaspersky Takedown Hizmeti, kötü amaçlı ve kimlik avına yönelik domain'lerin oluşturduğu tehditleri markanız ve işletmeniz herhangi bir zarar görmeden önce hızla azaltır. Bütün sürecin uçtan uca yönetimi size değerli zaman ve kaynak tasarrufu sağlar.

Kaspersky
Ask the Analyst

Kaspersky Ask the Analyst Hizmeti

Siber suçlular, işletmelere saldırmak için sürekli olarak karmaşık yöntemler geliştiriyorlar. Günümüzün değişken ve hızla büyüyen tehdit ortamı, giderek daha çevik hale gelen siber suç tekniklerine tanıklık ediyor. Kurumlar; kötü amaçlı yazılım içermeyen saldırılar, dosyasız saldırılar, programların kontrolünü ele geçirmeye yönelik saldırılar, sıfırıncı-gün güvenlik açıkları ve bu saldırıların toplu olarak oluşturduğu karmaşık tehditler, APT benzeri ve hedefli saldırıların yol açtığı karmaşık olaylarla karşılaşmaktadır.

İşletmeleri zor duruma sokan siber saldırıların yaşandığı bir çağda siber güvenlik uzmanları her zamankinden daha önemlidir, ancak bu uzmanları bulmak ve şirket bünyesine katmak kolay değildir. Sağlam bir siber güvenlik ekibiniz olsa bile uzmanlarınızın her zaman karmaşık tehditlerle yalnız başlarına mücadele etmelerini bekleyemezsiniz — ekibiniz, uzman üçüncü taraflardan yardım isteyebilmelidir. Dışarıdan temin edilecek uzmanlık, olası karmaşık saldırıları veya APT yöntemlerine ışık tutabilir ve bunları ortadan kaldırmanın en istikrarlı yolları hakkında eyleme dönüştürülebilir tavsiyeler sağlayabilir.

Sürekli tehdit araştırması, Kaspersky'nin siber saldırganların ve suçluların uğrak yeri olan dünya çapındaki kapalı topluluklar ve karanlık forumları bulması, denetlemesi ve bunlara sızmasını sağlar. Analistlerimiz, önceden tedbirler alarak en zarar verici ve bilinen tehditlerin yanı sıra belirli kurumları hedef alan tehditleri tespit etmek ve incelemek için bu erişimden faydalanırlar.

Kaspersky Ask the Analyst, Tehdit İstihbaratı portföyümüzü genişleterek size, karşılaştığınız veya ilgilendiğiniz tehditlerle ilgili rehberlik ve geri bildirim talep etme olanağı sunar. Hizmet, Kaspersky'nin güçlü tehdit istihbaratını ve araştırma yetkinliğini özel ihtiyaçlarınıza göre uyarlayarak kuruluşunuzu hedef alan tehditlere karşı dayanıklı savunmalar oluşturmanızı sağlar.

Kaspersky Ask the Analyst Çıktıları (Birleşik talebe dayalı abonelik)

APT ve Suç Yazılımları

Yayınlanan raporlar ve devam eden araştırmalar ile ilgili ek bilgiler (APT veya Suç Amaçlı Yazılım İstihbarat Raporlama hizmetine ek olarak)

Tehdit, güvenlik açığı ve tehlike belirtileriyle ilgili açıklamalar

- Belirli bir kötü amaçlı yazılım ailesinin genel açıklaması
- Tehditlere yönelik ek bağlam (ilgili veriler, URL'ler, CnC'ler vb.)
- Belirli güvenlik açıkları hakkında bilgiler (ne kadar önemli olduğu ve Kaspersky ürünlerindeki bu sorunla ilgili koruma mekanizmaları)

ICS ile ilgili istekler

- Yayınlanmış raporlarla ilgili ek bilgiler
- ICS Güvenlik açığı bilgileri
- ICS tehdit istatistikleri ve bölge / sektör trendleri
- Yönetmelikler veya standartlarla ilgili ICS Kötü Amaçlı Yazılım bilgileri

Dark Web istihbaratı

- Belirli olgular, IP adresleri, domain isimleri, dosya isimleri, e-postalar, bağlantılar veya görüntüler ile ilgili Dark web araştırması
- Bilgi araması ve analizi

Kötü amaçlı yazılım analizi

- Kötü amaçlı yazılım örneği analizi
- İlave düzeltme eylemleri hakkında öneriler

Nasıl çalışır?

Kaspersky Ask the Analyst, ayrı olarak veya tehdit istihbaratı hizmetlerimizin herhangi birine ek olarak satın alınabilir. Taleplerinizi kurumsal müşteri destek portalımız olan Kaspersky Şirket Hesabı üzerinden gönderebilirsiniz. Size e-posta yoluyla dönüş yapacağız ancak gerekirse ve kabul ederseniz bir konferans görüşmesi ve/veya ekran paylaşımı oturumu da düzenleyebiliriz. Talebiniz kabul edildikten sonra işlenmesi için gereken tahmini zaman hakkında size bilgi verilecektir.

Kullanım senaryoları

1. Önceden yayınlanan tehdit istihbaratı raporlarındaki tüm bilgileri açıklığa kavuşturun
2. Zaten sunulan tehlike belirtilerine dair ek istihbaratı elde edin
3. Güvenlik açıklarına ilişkin bilgiler ve bu açıkların kötü etkilerine karşı nasıl korunabileceğinize dair öneriler alın
4. İlgilendiğiniz Dark Web etkinliklerine dair ek bilgiler edinin
5. Kötü amaçlı yazılım davranışı, olası etkisi ve Kaspersky'nin gözlemlediği ilgili siber aktivite hakkındaki bilgileri de içeren, ilgili kötü amaçlı yazılım ailesine genel bakış raporu alın
6. Kısa raporlar aracılığıyla sağlanan ilgili IoC'ler için ayrıntılı bağlamsal bilgiler ve sınıflandırma ile uyarıları/olayları etkin bir şekilde öncelikli hâle getirin
7. Tespit edilen olağandışı aktivitenin bir APT veya suç yazılımı ile ilgili olup olmadığını belirlemek için yardım talep edin
8. Sağlanan örnek(lerin) davranışını ve işlevselliğini anlamak amacıyla kötü amaçlı yazılım dosyalarını kapsamlı analiz için gönderin

Kaspersky Ask the Analyst faydaları

Uzmanlığınızı artırın

Bulması zor tam zamanlı siber güvenlik uzmanları aramak ve onları işe almak için yatırım yapmak zorunda kalmadan sektördeki uzmanlara talebiniz üzerine erişme olanağı elde edin

İncelemeleri hızlandırın

Özel ve detaylı bağlam bilgilerine dayanarak olayları etkili bir şekilde araştırın ve önceliklendirin

Hızlı müdahale edin

Bilinmeyen vektörler aracılığıyla gelen saldırıları engellemek için rehberimizi kullanarak tehditlere ve güvenlik açıklarına hızlı bir şekilde müdahale edin

Bilginizi ve kaynaklarınızı genişletin

Kaspersky Ask the Analyst, vaka bazlı olarak Kaspersky araştırmacılarından oluşan temel bir gruba erişmenizi sağlar. Bu hizmet, uzun yıllara dayanan bilgi birikimimiz ve kaynaklarımızı kullanarak mevcut yetkinliklerinizi artırmak için uzmanlarımız ve sizin arasında kapsamlı bir iletişim sağlar.

Sonuç

Günümüzün siber tehditleriyle mücadele edebilmek için tehdit aktörleri tarafından kullanılan taktiklerin ve araçların 360 derece görülebilmesi gerekir. Bu istihbaratı oluşturmak ve en etkili karşı önlemleri saptamak için sürekli olarak çalışmak ve yüksek uzmanlık düzeyi gerekir. Kaspersky olarak, işlenecek petabaytlarca zengin tehdit verisi, gelişmiş makine öğrenimi teknolojileri ve dünyanın çeşitli noktalarında ikamet eden uzman havuzumuz ile, müşterilerimizin, önceden görülemeyen siber saldırılara karşı bile bağışıklıklarını sürdürmesine yardım ederek dünyanın dört bir yanından elde edilen en güncel tehdit istihbaratını sizlere sağlıyoruz.

Temel avantajlar

Tehdidin küresel çapta görünür hale gelmesini, siber tehditlerin zamanında tespit edilmesini, güvenlik uyarılarının önceliklendirilmesini ve bilgi güvenliği olaylarına etkili bir şekilde yanıt verilebilmesini sağlar

Farklı sektörler ve bölgelerdeki tehdit aktörleri tarafından kullanılan taktikler, teknikler ve prosedürlere ilişkin benzersiz analizler, hedefli ve karmaşık tehditlere karşı proaktif koruma sağlar

Azaltma stratejileriyle ilgili eyleme geçirilebilir tavsiyelerle güvenlik yapınıza dair sunulan kapsamlı bir genel bakış, savunma stratejinizi birincil siber saldırı hedefleri olarak belirlenen alanlara odaklamanıza olanak tanır

Analistlerin mesleki tükenmişlik yaşamasını engelleyerek iş gücünüzün özgün tehditlere odaklanmasını sağlar

İyileştirilmiş ve hızlandırılmış olay müdahalesi ve tehdit yakalama yetkinliği, saldırı “bekleme süresinin” azaltılmasına ve olası hasarın önemli oranda azaltılmasına yardımcı olur

Kaspersky Threat Intelligence

Daha fazla bilgi edinin

www.kaspersky.com.tr

#kaspersky
#geleceğiyakalayın