Kaspersky Tehdit İstihbaratı

kaspersky GELECEĞİ YAKALAYIN

Karşılaşılan zorluklar

Sürekli olarak gelişen BT güvenlik tehditlerinin takibi, analizi, yorumlanması ve azaltılması çok büyük bir girişimdir. Tüm sektörlerden kuruluşlar, BT güvenliği tehditleriyle ilişkilendirilen riskleri yönetmeye yardımcı olması için ihtiyaç duydukları güncel, alakalı verilerin eksikliğiyle karşılaşmaktadır.

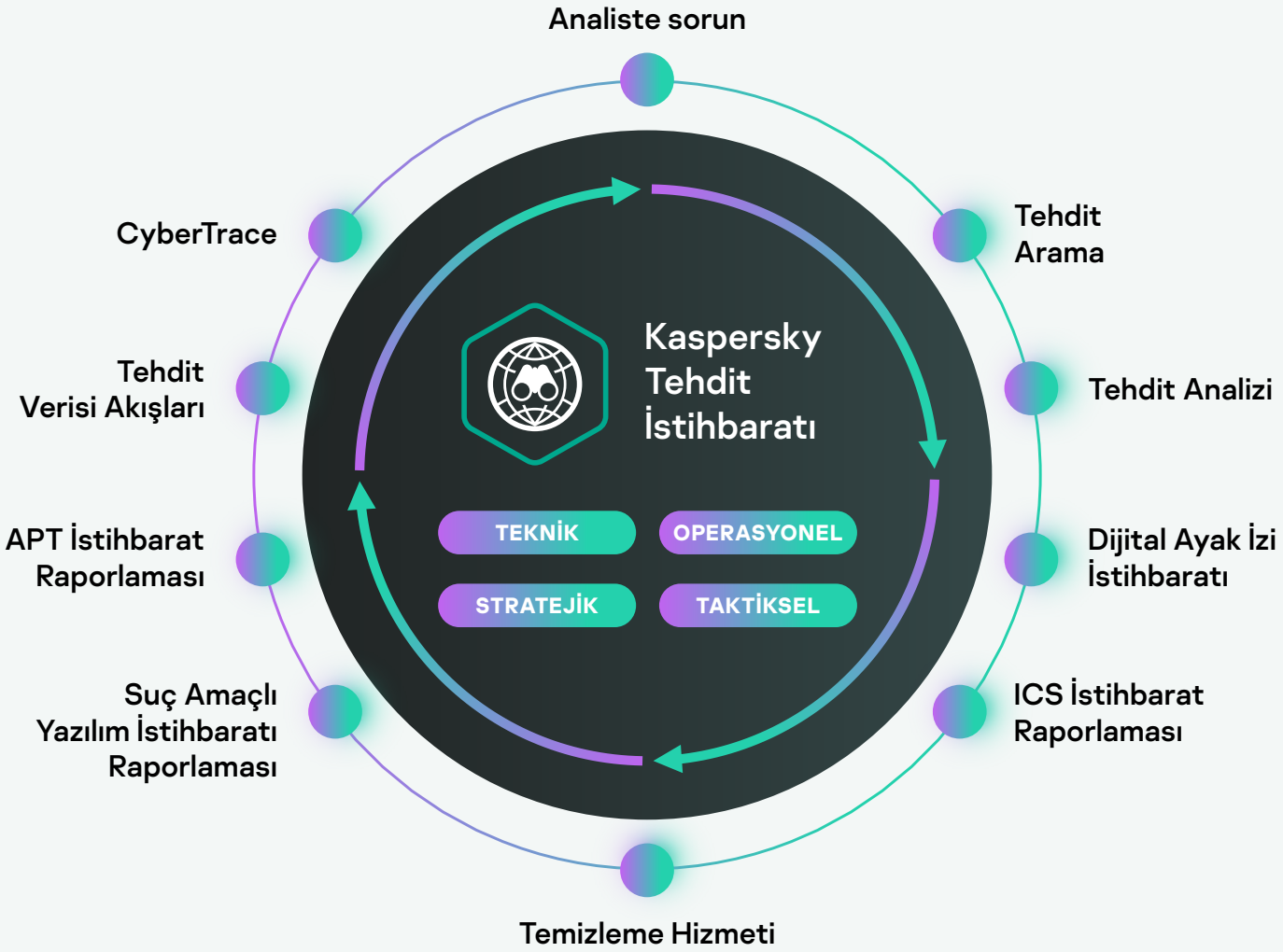
Kaspersky Tehdit İstihbaratı

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 dahil olmak üzere dünyanın önde gelen emniyet güçleri ve devlet mercileri tarafından güvenilir bir ortak olarak kabul edilmesini sağlamıştır. Kaspersky Tehdit İstihbaratı; teknik, taktiksel, operasyonel ve stratejik Tehdit İstihbaratına anında erişmenizi sağlar.

Kaspersky Tehdit İstihbaratı portföyünün içeriği

Tehdit Verisi Akışları, CyberTrace (bir Tehdit İstihbaratı Platformu), Tehdit Arama, Tehdit Analizi (Cloud Sandbox ve Cloud Threat Attribution Engine), çeşitli Tehdit İstihbaratı Raporlama seçenekleri ve talep üzerine tehdit istihbaratı uzmanlığı sunan hizmetler.



Kaspersky Threat Data Feeds

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

Güvenlik ekipleri, şüpheli ve tehlikeli IP'ler, URL'ler ve dosya karmaları ile ilgili bilgi içeren en güncel tehdit istihbaratı akışlarını SIEM, SOAR ve Tehdit İstihbarat Platformları gibi mevcut güvenlik sistemlerine entegre ederek ilk uyarı triyajı süreçlerini otomatikleştirebilir ve triyaj uzmanlarına, araştırılması veya daha fazla araştırma ve müdahale için olay müdahale ekiplerine bildirilmesi gereken uyarıları anında belirlemek için yeterli bağlamı sunar.

- IP TANINIRLIK AKIŞI
- KARMA VERİ AKIŞI (WIN/*nix/ MacOS / AndroidOS / iOS)
- URL AKIŞLARI (Kötü Amaçlı, Kimlik Avı ve C&C)
- FİDYE YAZILIMI URL AKIŞI
- APT IOC AKIŞLARI
- GÜVENLİK AÇIĞI AKIŞI
- PASİF DNS (pDNS) AKIŞI
- IoT URL AKIŞI
- İZİN VERİLENLER LİSTESİ AKIŞI
- ICS KARMA VERİ AKIŞI
- VE DAHA FAZLASI

Kaspersky Threat Data Feeds

Bağlamsal veriler

Her bir Veri Akışındaki her kayıt, eyleme geçirilebilir bağlamla (tehdit adları, zaman damgaları, coğrafi konum, virüs bulaşmış web kaynaklarının çözümlenmiş IP adresleri, karmalar, popülerlik vb.) zenginleştirilmiştir. Bağlamsal veriler, verilerin geniş kapsamlı kullanımını daha fazla doğrulayarak ve destekleyerek "büyük resmin" ortaya çıkarılmasına yardımcı olur. Veriler bağlama yerleştirildiğinde, saldırganları belirlemek ve hızlı karar alıp harekete geçmenize yardımcı olmak amacıyla "kim, ne, nerede, ne zaman" sorularını yanıtlamak için daha kolay bir şekilde kullanılabilir.

Öne Çıkan Noktalar

Veri Akışları, dünya genelindeki bulgulara (Kaspersky Security Network, 213'ten fazla ülkedeki milyonlarca son kullanıcıyı kapsayan tüm internet trafiğinin önemli bir yüzdesine görünürlük sağlar) dayalı biçimde gerçek zamanlı ve otomatik olarak oluşturularak yüksek algılama oranları ve doğruluk sağlar

Uygulama kolaylığı. Tamamlayıcı belgeler, örnekler, özel bir teknik hesap yöneticisi ve Kaspersky teknik desteği, entegrasyon kolaylığı sağlamak için bir araya getirilir

Dünyanın her yerinden güvenlik analistleri ve GReAT ve Ar-Ge ekiplerinden dünyaca tanınmış güvenlik uzmanları dahil yüzlerce uzman, bu akışların oluşturulmasına katkıda bulunur. Güvenlik sorumluları, gereksiz gösterge ve uyarı yağmuruna tutulmadan en nitelikli verilerden oluşturulan kritik bilgiler ve uyarılar alır

Toplama ve işleme

Veri Akışları, Kaspersky Security Network ve kendi web tarayıcılarımız, Botnet İzleme hizmetimiz (botnetlerin, hedeflerinin ve etkinliklerinin 365 gün 7/24 izlenmesi), spam tuzaklarımız, araştırma ekiplerimiz ve iş ortaklarımız gibi birleştirilmiş, heterojen ve güvenilir kaynaklardan toplanır.

Ardından, toplanan tüm veriler, dikkatlice incelenir ve istatistiksel ölçütler, koruma alanları, sezgisel motorlar, benzerlik araçları, davranış profili çıkarma, analiz ekibi doğrulaması ve izin verilenler listesi doğrulaması gibi birden fazla ön işleme tekniği kullanılarak gerçek zamanlı olarak iyileştirilir.

FTP, HTTPS veya özel iletim mekanizmaları yoluyla basit ve hafif dağıtım biçimleri (JSON, CSV, OpenIoC, STIX), akışların güvenlik çözümlerine kolayca entegre edilmesini destekler

Tüm akışlar, sürekli kullanılabilirlik sağlayan, hataya yüksek ölçüde dayanıklı bir altyapı tarafından oluşturulur ve izlenir

Hatalı pozitif sonuçlarla dolu Veri Akışlarının değeri yoktur; bu nedenle %100 incelenmiş veriler sunmak amacıyla akışlar gönderilmeden önce çok kapsamlı testler ve filtreler uygulanır

Avantajlar

SIEM'ler, Güvenlik Duvarları, IPS/IDS, Güvenlik Proxy'si, DNS çözümleri, Anti-APT dahil ağ savunma çözümlerinizi, siber saldırılara ilişkin bilgi sunmak ve saldırganların niyetinin, kabiliyetlerinin ve hedeflerinin daha iyi anlaşılmasını sağlamak için sürekli güncellenen Güvenlik İhlal Göstergeleri (IOC'ler) ve eyleme geçirilebilir bağlamla destekleyin. Başlıca SIEM'ler (HP ArcSight, IBM QRadar, Splunk vb. dahil) ve TI Platformları tamamen desteklenir

Güvenlik analistlerinize, araştırılması veya daha fazla araştırma ve müdahale için olay müdahale ekiplerine bildirilmesi gereken uyarıları anında belirlemeleri için yeterli bağlam sağlarken ilk triyaj sürecini otomatikleştirerek olay müdahalesi ve adli delil toplama kabiliyetlerinizi geliştirin ve hızlandırın

Hassas varlıkların ve fikri mülkiyetin virüs bulaşmış makinelerden kuruluş dışına sızmasını önleyin. Marka itibarınızı korumak, rekabet avantajınızı sürdürmek ve iş fırsatlarını güvence altına almak için virüs bulaşmış varlıkları hızlı bir şekilde tespit edin

Bir Yönetilen Güvenlik Hizmeti Sağlayıcısı (MSSP) olarak, müşterilerinize üst düzey bir hizmet sunmak amacıyla sektör lideri tehdit istihbaratı sağlayarak işinizi büyütün. Bir Bilgisayar Acil Durum Müdahale Ekibi (CERT) olarak, siber tehdit algılama ve tanımlama kabiliyetlerinizi geliştirin ve genişletin

Kaspersky CyberTrace

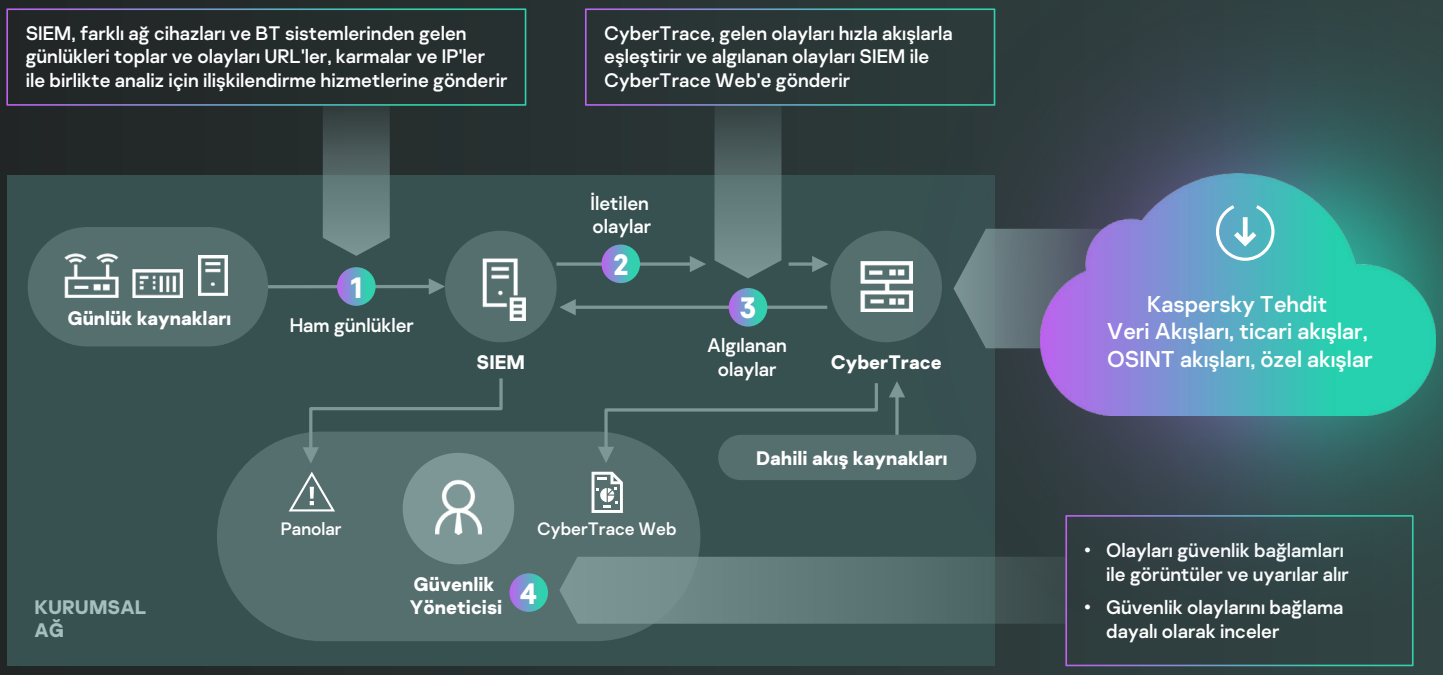
Güvenlik Operasyonu Merkezleri, SIEM sistemleri gibi makine tarafından okunabilen, en güncel tehdit istihbaratı ile mevcut güvenlik kontrollerini bir araya getirerek ilk saptama sürecini otomatikleştirebilir. Ayrıca incelenmesi veya daha ayrıntılı bir şekilde incelenmek veya yanıtlanmak üzere olay yanıt ekiplerine taşınması gereken uyarıları hemen tespit edebilmek üzere güvenlik analistlerine yeterli bağlamı sağlar. Bununla birlikte, tehdit veri akışları ile mevcut tehdit istihbaratı kaynaklarındaki sürekli büyüme, kuruluşların hangi bilgilerin ilgili olup olmadığını belirlemesini zorlaştırır. Tehdit istihbaratlarının farklı formatlarda sunulması ve çok sayıda Güvenlik İhlal Göstergesi (IoC'ler) içermesi, SIEM veya ağ güvenliği kontrollerinin bu istihbaratı işlemesini zorlaştırır.

Kaspersky CyberTrace, analistlerin mevcut güvenlik operasyonu iş akışında tehdit istihbaratından daha etkili bir biçimde faydalanmasına yardımcı olmak üzere tehdit veri akışları ile SIEM çözümlerinin kusursuz entegrasyonunu sağlayan 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.

Kaspersky CyberTrace, tehdit istihbaratını etkili bir şekilde işlevsel hale getirmeye yönelik bir dizi araç sunar:

- Gelişmiş arama sorguları kullanarak arama özelliği ve tam metin arama özelliğine sahip gösterge veri tabanı, bağlam alanları da dahil olmak üzere tüm gösterge alanlarında karmaşık aramalar yapılmasına imkan sağlar
- Her göstergeye ait ayrıntılı bilgiler içeren sayfalar daha derin analizler sunar. Her sayfa, belirli bir gösterge için tüm istihbarat sağlayıcılarından gelen bilgilerin tamamını içerir (kopyaların önlenmesi), böylelikle analistler tehditleri yorumlar kısmında tartışabilir ve gösterge hakkındaki dahili tehdit istihbaratlarını ekleyebilir
- Bir Araştırma Grafiği, CyberTrace üzerinde depolanan verileri ve algılanan tehditleri görsel olarak keşfetmenizi ve tehdit benzerliklerini görmenizi sağlar
- Gösterge dışa aktarım özelliği, gösterge setlerinin ilke listeleri (engelleme listeleri) gibi güvenlik kontrollerine aktarılmasını ve tehdit verilerinin Kaspersky CyberTrace örnekleri veya diğer TI platformları arasında paylaşılmasına olanak verir
- IoC'lerin etiketlenmesi yönetimlerini kolaylaştırır. Herhangi bir etiket oluşturabilir, bu etiketin ağırlığını (önemini) belirleyebilir ve IoC'leri manuel olarak etiketlemek için bunu kullanabilirsiniz. Ayrıca bu etiketlere ve etiketlerin ağırlıklarına göre IoC'leri sınıflandırabilir ve filtreleyebilirsiniz
- Geçmişe yönelik ilişkilendirme özelliği (geçmişe yönelik tarama), geçmişte açığa çıkarılan tehditleri bulmak üzere en güncel akışları kullanarak önceden kontrol edilen olaylardan elde edilen gözlemlenebilir verileri analiz etmenizi sağlar
- Filtre, algılama olaylarını SIEM çözümlerine göndererek hem onlar hem de analistler üzerindeki yükü azaltır
- Çoklu kullanım desteği, MSSP'leri ve büyük kurumsal kullanım durumlarını destekler
- Entegre akışların ve akış kesişim matrislerinin etkinliğini ölçmek için kullanılan akış kullanım istatistikleri, en değerli tehdit istihbaratı sağlayıcılarının seçilmesine yardımcı olur
- HTTP RestAPI, tehdit istihbaratlarını aramanıza ve yönetmenize yardımcı olur

Araç, gelen verileri ayrıştırmak ve eşleştirmek için dahili bir sürece sahiptir ve bu da SIEM iş yükünü büyük oranda azaltır. Kaspersky CyberTrace gelen günlükleri ve olayları ayrıştırır, çıkan verileri akışlarla hızlıca eşleştirir ve tehdit algılama için kendi uyarılarını oluşturur. Yüksek seviyeli çözüm entegrasyonu mimarisi aşağıdaki şemada gösterilmiştir:



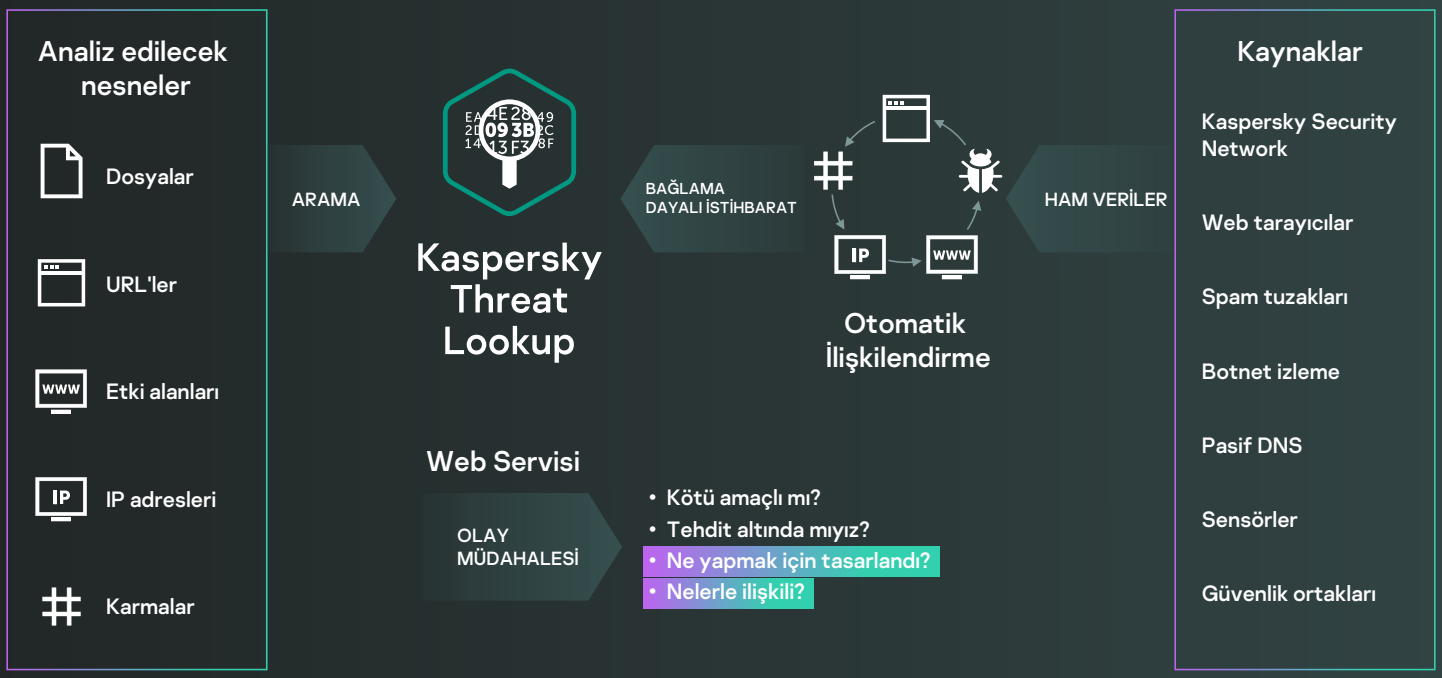
Kaspersky CyberTrace ve Kaspersky Tehdit Veri Akışları ile güvenlik analistleri şunları yapabilir:

- Çok büyük miktarlarda güvenlik uyarılarını etkili biçimde ayrıştırabilir ve önceliklendirebilir
- Öncelik belirleme ve ilk müdahale süreçlerini iyileştirebilir ve hızlandırabilir
- Kurum için kritik olan uyarıları hemen tespit ederek hangilerinin IR ekiplerine bildirileceği hakkında daha bilinçli kararlar verebilir
- Proaktif ve istihbarata dayalı bir savunma oluşturabilir

Kaspersky Threat Lookup

Siber suçlar sınır tanımamaktadır ve teknik kapasiteleri hızla gelişmektedir; siber suçlular hedeflerini tehdit etmek için dark web kaynaklarını kullanırken saldırıların giderek ne kadar gelişmiş hale geldiği görülmektedir. Savunmanızı tehlikeye atmak için yeni girişimler ortaya çıktıkça siber tehditlerin sıklığı, karmaşıklığı ve gizlenme taktikleri de sürekli artmaktadır. Saldırganlar, işletmenizin işleyişini aksatmak, varlıklarınızı çalmak veya müşterilerinize zarar vermek için karmaşık ölüm zincirleri ve özelleştirilmiş Taktikler, Teknikler ve Prosedürler (TTP'ler) kullanmaktadır.

Kaspersky Tehdit Arama, Kaspersky'nin siber tehditler ve bunların ilişkileri konusunda elde ettiği bilgi birikiminin tamamını tek ve güçlü bir web hizmetinde sunar. Amaç, güvenlik ekiplerinize mümkün olduğunca fazla veri sağlayarak siber saldırıları kuruluşunuzu etkilemeden önce önlemektir. Platform; URL'ler, etki alanları, IP adresleri, dosya karmaları, 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.



Öne Çıkan Noktalar

Güvenilir İstihbarat: Kaspersky Tehdit Arama'nın önemli bir özelliği, eyleme geçirilebilir bağlamla zenginleştirilmiş tehdit istihbaratı verilerimizin güvenilirliğidir. Kaspersky, kötü amaçlı yazılım testlerinde[1] alanında lider konumundadır ve sıfıra yakın hatalı pozitif sonuçla en yüksek algılama oranlarını elde ederek güvenlik istihbaratımızın benzersiz kalitesini gösterir

Tehdit avlama: 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

Olay araştırmaları: Bir Araştırma Grafiği, Tehdit Aramada depolanan verileri ve algılanan tehditleri görsel olarak incelemenize olanak tanıyarak olay araştırmalarını destekler. Bir olayın tam kapsamını daha iyi anlayabilmeniz ve temel nedenini belirleyebilmeniz için URL'ler, etki alanları, IP'ler, dosyalar ve diğer bağlamlar arasındaki ilişkinin grafik şeklinde bir görselleştirmesini sunar.

Ana arama: Tek ve güçlü bir arabirimde tüm aktif tehdit istihbaratı ürünlerinde ve harici kaynaklarda (OSINT IoCs, Dark Web ve Surface Web dahil) bilgi arayın.

Kullanımı kolay Web arabirimi veya RESTful API: Tercihinize bağlı olarak bir web arabirimi yoluyla (bir web tarayıcısı üzerinden) hizmeti manuel modda kullanın veya basit bir RESTful API üzerinden hizmete erişim sağlayın

Çok çeşitli dışa aktarma biçimleri: 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

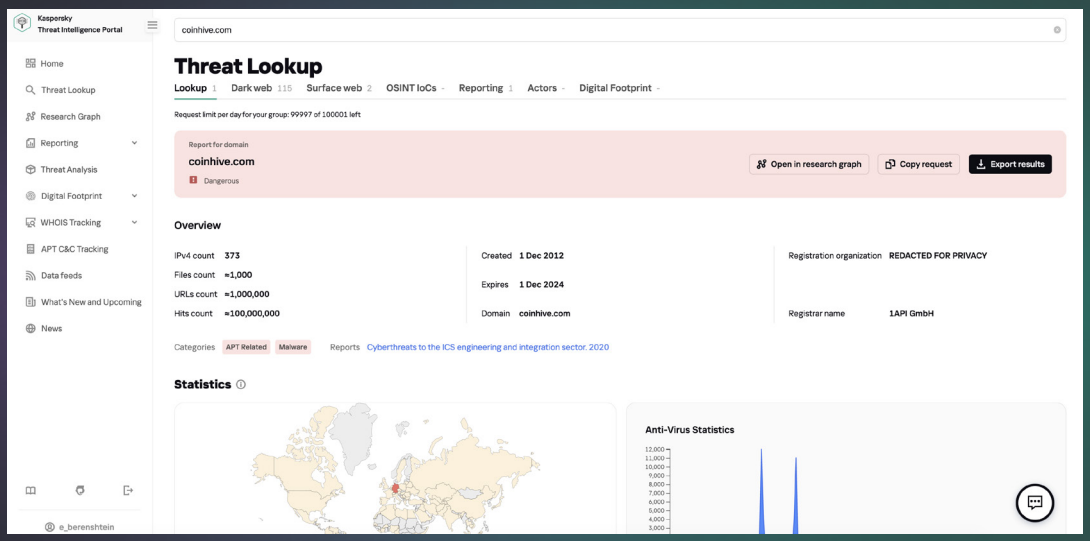
Avantajlar

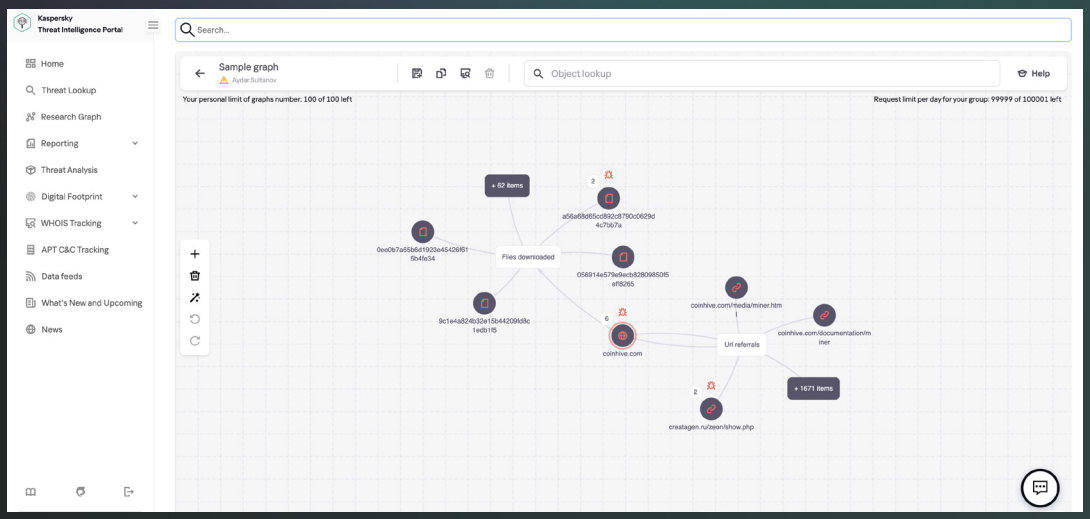
Saldırıları önceliklendirmenize ve işletmeniz için en çok risk teşkil eden tehditleri en aza indirmeye odaklanmanıza olanak tanıyan yüksek düzeyde doğrulanmış tehdit bağlamı ile tehdit göstergeleriyle ilgili ayrıntılı aramalar yapın

Ana bilgisayarlar ve ağ üzerindeki güvenlik olaylarını daha verimli ve etkili bir şekilde tanılayıp analiz edin ve bilinmeyen tehditlere karşı dahili sistemlerden gelen sinyalleri önceliklendirin

Kritik sistemler ve veriler tehlikeye girmeden ölüm zincirini bozmak için olay müdahalesi ve tehdit avlama kabiliyetlerinizi geliştirin

[1] kaspersky.com/top3





Artık;

Web tabanlı bir arabirimden veya RESTful API aracılığıyla tehdit göstergelerini arayabileceksiniz

Yeni şüpheli nesneleri bulmak için sertifikalar, sık kullanılan adlar, dosya yolları veya ilgili URL'ler dahil olmak üzere gelişmiş ayrıntıları inceleyebileceksiniz

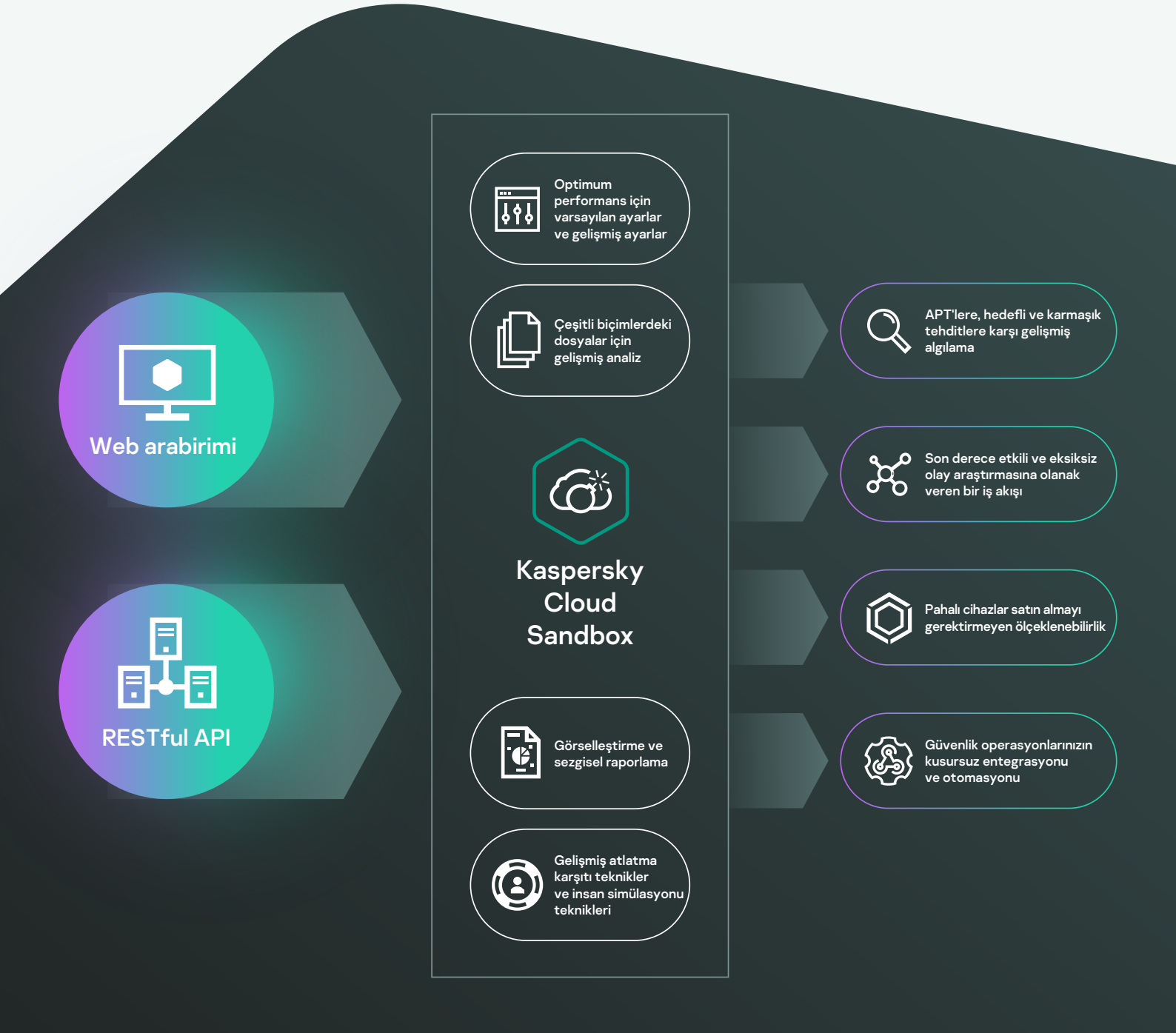
Bulduğunuz nesnenin yaygın mı yoksa benzersiz mi olduğunu kontrol edebileceksiniz

Bir nesnenin neden kötü amaçlı olarak değerlendirilmesi gerektiğini anlayabileceksiniz

Kaspersky Cloud Sandbox

Günümüzün hedefli saldırılarını sadece geleneksel AV araçlarıyla önlemek imkansızdır. Antivirüs motorları sadece bilinen tehditleri ve bunların türevlerini durdurma kabiliyetine sahipken gelişmiş tehdit aktörleri otomatik algılamayı atlatmak için ellerindeki tüm araçları kullanır. Bilgi güvenliği olaylarından kaynaklanan kayıplar katlanarak artmaya devam etmektedir; bu da önemli bir hasar oluşmadan önce hızlı müdahale etmek ve tehditlere karşı koymak için anında tehdit algılama kabiliyetlerinin artan önemini vurgulamaktadır.

Bir dosyanın davranışına dayalı akıllı bir karar verirken eş zamanlı olarak işlem belleğini, ağ etkinliğini vb. analiz etmek, karmaşık hedefli ve özelleştirilmiş olan en son tehditleri anlamak için en iyi yaklaşımdır. İstatistiksel verilerde, yakın zamanda değiştirilen kötü amaçlı yazılımlar hakkında bilgi eksiği olsa da, korumalı alan teknolojileri; dosya örneklerinin kaynaklarını araştırılmasına, davranışsal analize dayalı IOC'lerin toplanmasına ve daha önce görülmemiş kötü amaçlı nesnelerin algılanmasına olanak veren güçlü araçlardır.



Kapsamlı raporlama

- Yüklü ve çalıştırılan DLL'ler
- Alan adları ve IP adresleriyle harici bağlantılar
- Oluşturulan, değiştirilen ve silinen dosyalar
- Ortaya çıkarılan her güvenlik ihlal göstergesi (IOC) için eyleme geçirilebilir bağlamla ayrıntılı tehdit istihbaratı
- İşlem belleği dökümleri ve ağ trafiği dökümleri (PCAP)
- HTTP ve DNS istekleri ve yanıtları
- Oluşturulan karşılıklı dışlamalar ("mutex"ler)
- RESTful API
- Değiştirilen ve oluşturulan kayıt defteri anahtarları
- Yürütülen dosya tarafından oluşturulan işlemler
- Ekran görüntüleri
- **ve çok daha fazlası**

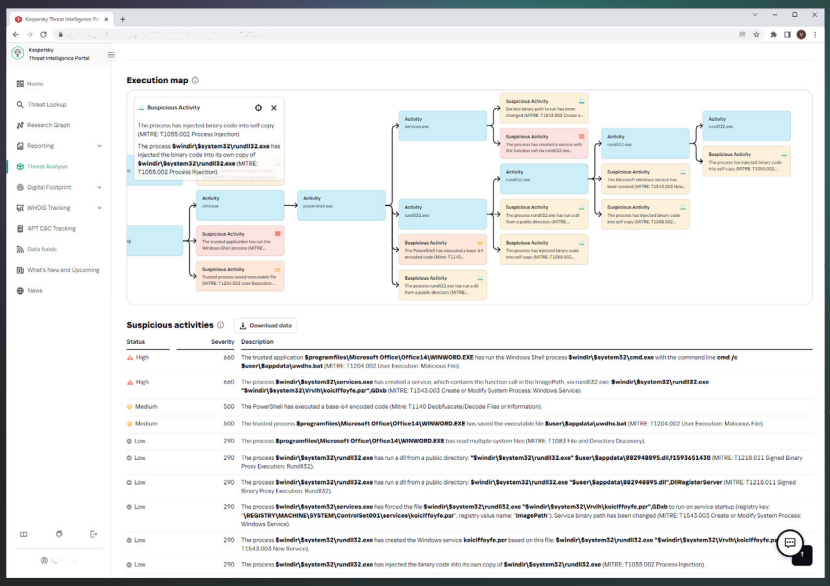
Proaktif tehdit algılama ve azaltma

Kötü amaçlı yazılımlar, çalıştıklarının algılanmasını engellemek için çeşitli yöntemler kullanır. Sistem gerekli parametreleri karşılamıyorsa kötü amaçlı program hemen hemen her zaman kendini yok edecek ve hiçbir iz bırakmayacaktır. Kötü amaçlı kodun yürütülebilmesi için korumalı ortamın normal son kullanıcı davranışını doğru bir şekilde taklit edebilmesi gerekir.

Kaspersky Cloud Sandbox, petabaytlarca istatistiksel veriden (Kaspersky Security Network ve diğer tescilli sistemler sayesinde) toplanan tehdit istihbaratını, davranışsal analizi ve son derece sağlam atlatma önleme özelliğini otomatik tıklayıcı, belgede gezinme ve sahte işlemler gibi insan davranışlarını simüle eden teknolojilerle birleştiren hibrit bir yaklaşım sunar.

Bu ürün, kurum içi korumalı alan laboratuvarımızda, on yılı aşkın bir değişim sürecinin sonunda geliştirilmiştir. Bu teknoloji, 20 yıl boyunca devam eden tehdit araştırmaları sonucunda edindiğimiz tüm kötü amaçlı yazılım davranışı bilgimizi içermektedir. Bu da, müşterilerimize sektör lideri güvenlik çözümleri sunmak için her gün 360.000'den fazla yeni kötü amaçlı nesneyi tespit etmemize olanak vermektedir.

Threat Intelligence Portal'ımızın bir parçası olan Cloud Sandbox, tehdit istihbaratı iş akışınızdaki önemli bileşendir. Tehdit Arama URL'ler, etki alanları, IP adresleri, dosya karmaları, tehdit adları, istatistiksel/davranışsal veriler, WHOIS/DNS verileri vb. hakkında en güncel, ayrıntılı tehdit istihbaratını alırken, Cloud Sandbox bu bilgiyi analiz edilen örnek tarafından oluşturulan IOC'lere bağlar.



Artık, tehdidin yapısını hemen anlayarak ve noktaları, birbiriyle ilişkili tehdit göstergelerinin ayrıntılarını ortaya çıkaracak şekilde birleştirerek, son derece etkili ve karmaşık olay istihbaratlarını yürütebilirsiniz.

Denetim, özellikle çok aşamalı saldırılar söz konusu olduğunda çok yoğun kaynak kullanımı gerektirebilir. Kaspersky Cloud Research Sandbox, pahalı cihazlar satın almanıza veya sistem kaynakları hakkında endişelenmenize gerek kalmadan, size dosyaları otomatik olarak işlemek için ölçeklenebilirlik sağlayarak olaylara müdahalenizi ve adli bilişim faaliyetlerini destekler.

Kaspersky APT İstihbarat Raporlaması

Kaspersky APT İstihbarat Raporlaması müşterileri, keşfedilen her APT ile ve kesinlikle kamuya açıklanmayacak tehditlerle ilgili tüm teknik veriler (çeşitli biçimlerde) dahil olmak üzere incelemelerimize ve keşiflerimize benzersiz bir sürekli erişim olanağına sahip olur. Raporlar, güvenlik araştırmacılarına, kötü amaçlı yazılım analistlerine, güvenlik mühendislerine, ağ güvenliği analistlerine ve APT araştırmacılarına tehditlere karşı hızlı ve doğru müdahale edilmesini sağlayan eyleme geçirilebilir veriler sunmak için ilgili APT ile birlikte APT'nin ilgili IOC'leri ve YARA kurallarını içeren ayrıntılı bir teknik açıklamasını sunan C düzeyi odaklı ve anlaşılması kolay bilgiler veren bir yönetici özeti içerir.

Uzmanlarımız siber suçlu gruplarının taktiklerinde tespit ettikleri herhangi bir değişiklik konusunda da sizi anında uyaracaktır. Güvenlik savunmanızın başka bir güçlü araştırma ve analiz bileşeni olan, Kaspersky'nin eksiksiz APT raporları veri tabanına da erişiminiz olacaktır.

Avantajlar

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

Genel kullanıma açık olmayan APT'ler hakkında bilgi
Çeşitli nedenlerle, yüksek profilli tehditlerin tamamı hakkında kamuya bilgi verilmez. Fakat bunları müşterilerimizle paylaşırız

Ayrıcalıklı erişim
Kamuya açıklanmadan önce, devam eden araştırmalar sırasında tespit edilen en son tehditler hakkında teknik açıklamalar alın

Geriye dönük analiz
Abonelik döneminiz boyunca, önceden hazırlanan tüm özel raporlara erişim olanağı sunulur

Teknik verilere erişim
OpenIOC veya STIX'i de içeren standart biçimlerde sunulan genişletilmiş bir IOC listesine ve YARA kurallarımıza erişim dahildir

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 dahildir

Sürekli APT kampanya izleme
Araştırma sırasında eyleme dönüştürülebilir istihbarata erişim (APT dağıtımı, IOC'ler, komut ve kontrol altyapıları vb. hakkında bilgi).

RESTful API
Güvenlik iş akışlarınızın sorunsuz entegrasyonu ve otomasyonu

Kaspersky Digital Footprint Intelligence

İşletmeniz büyüdükçe, BT ortamlarınızın karmaşıklığı ve dağıtımı da artarak, geniş çapta dağıtılmış dijital varlığınızı doğrudan kontrol veya sahiplik olmadan koruma sorununu ortaya çıkarır. Dinamik ve birbirine bağlı ortamlar, şirketlerin önemli avantajlar elde etmesine olanak verir. Ancak sürekli artan bağlanabilirlik, saldırı yüzeyini de genişletir. Saldırganlar daha becerikli hale geldikçe, sadece kuruluşunuzun çevrimiçi varlığının doğru bir genel görünümünü elde etmek değil, aynı zamanda onda meydana gelen değişiklikleri izlemek ve saldırılara açık dijital varlıklarla ilgili güncel bilgilere yanıt vermek de büyük önem taşır.

Kuruluşlar, güvenlik operasyonlarında çok çeşitli güvenlik araçları kullanır ancak hala ortaya çıkabilecek dijital tehditlere karşı, içeriden kişilerin faaliyetlerini, siber suçluların dark web forumlarındaki planlarını ve saldırı hazırlıklarını algılama ve azaltma kabiliyetlerine sahip olmak gibi yollarla önlemler alınması gerekir. Kaspersky, güvenlik analistlerinin saldırganların şirket kaynaklarına bakış açısını keşfetmelerine, kullanabilecekleri potansiyel saldırı vektörlerini anında keşfetmelerine ve savunmalarını buna göre ayarlamalarına yardımcı olmak için Kaspersky Digital Footprint Intelligence'yi yarattı.

Kuruluşunuza karşı bir saldırı başlatmanın en iyi yolu nedir? Size saldırmanın en düşük maliyetli yolu nedir? İşletmenizi hedef alan bir saldırganın elinde hangi bilgiler var? Altyapınız bilginiz olmadan ele mi geçirildi?

Uzmanlarımız girişim için zayıf noktaları tespit edip geçmiş, mevcut ve hatta gelecekteki planlı saldırıların kanıtlarını ortaya çıkararak saldırı durumunuzun kapsamlı bir resmini sunduğundan, Kaspersky Digital Footprint Intelligence, bu soruları ve daha fazlasını yanıtlar.

Ürün şunları sağlar:

- İstenmeden çevrede bırakılmış yönetim arabirimleri veya yanlış yapılandırılmış hizmetler, cihazların arabirimleri vb. gibi, saldırı için potansiyel bir giriş noktası olan müşteri ağ kaynaklarını ve saldırıya açık hizmetleri belirlemek için müdahaleci olmayan yöntemler kullanan ağ çevresi envanteri.
- 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 özelleştirilmiş analizi.
- Herhangi bir aktif hedefli saldırının veya planlanan saldırının veya şirketinizi, sektörünüzü veya bölgenizi hedef alan APT kampanyalarının belirlenmesi, izlenmesi ve analizi.
- Kendi virüs bulaşmış sistemleri daha sonra size saldırmak üzere kullanılabilecek müşterilerinizi, iş ortaklarınızı ve abonelerinizi hedef alan tehditlerin belirlenmesi.
- Ele geçirilmiş hesapları, bilgi sızıntılarını veya kuruluşunuza yönelik planlanan ve tartışılan saldırıları keşfetmek için pastebin sitelerinin, genel forumların, blogların, anlık mesajlaşma kanallarının, kısıtlı çevrimiçi yeraltı forumlarının ve toplulukların, tedbirli bir şekilde izlenmesi.

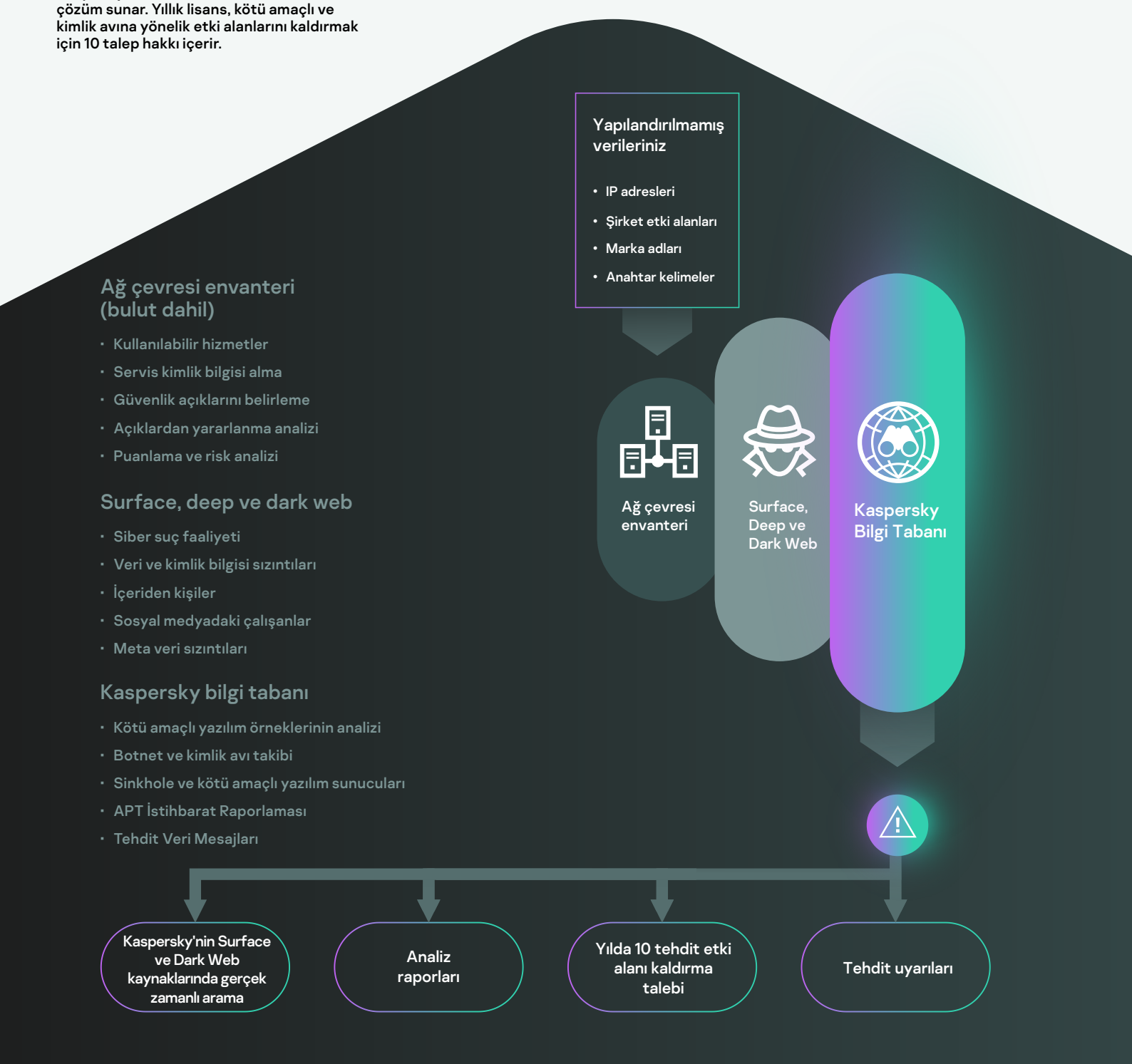
Öne Çıkan Noktalar

Kaspersky Digital Footprint Intelligence, eyleme geçirilebilir fikirler ve tavsiyeler sunmak için Surface, Deep ve Dark Web'in otomatik ve manuel analizi ile birleştirilmiş OSINT tekniklerinin yanı sıra dahili Kaspersky bilgi tabanını kullanır.

Ürüne Kaspersky Threat Intelligence Portalı'ndan erişilebilir. Yıllık gerçek zamanlı tehdit uyarıları içeren dört adet üç aylık rapor veya altı ay boyunca etkin olan uyarılar içeren tek bir rapor satın alabilirsiniz.

Varlıklarınızı tehdit eden küresel güvenlik olayları hakkında neredeyse gerçek zamanlı bilgiler ve kısıtlı yeraltı toplulukları ve forumlarda ifşa edilen hassas verilere ulaşmak için Surface ve Dark Web'de arama yapın. Yıllık lisans, harici kaynaklarda ve Kaspersky bilgi tabanında günde 50 aramayı içerir.

Kaspersky Digital Footprint Intelligence, Kaspesky Takedown Hizmeti ile tek bir çözüm sunar. Yıllık lisans, kötü amaçlı ve kimlik avına yönelik etki alanlarını kaldırmak için 10 talep hakkı içerir.



Kaspersky ICS Tehdit İstihbaratı Raporlaması

Kaspersky ICS Tehdit İstihbaratı Raporlaması endüstriyel kuruluşları hedef alan kötü amaçlı kampanyalar hakkında derinlikli istihbarat ve daha fazla farkındalığın yanı sıra en popüler endüstriyel kontrol sistemlerindeki ve temel teknolojilerdeki güvenlik açıkları hakkında bilgi sağlar. Raporlar web tabanlı bir portal yoluyla sunulur; böylece hizmeti hemen kullanmaya başlayabilirsiniz.

Aboneliğinize dahil olan raporlar

1. **APT raporları.** Endüstriyel kuruluşları hedef alan yeni APT ve yüksek hacimli saldırı kampanyaları hakkında raporlar ve aktif tehditlere ilişkin güncellemeler.
2. **Tehdit alanı.** Endüstriyel kontrol sistemleri için tehdit alanındaki önemli değişikliklere, ICS güvenlik seviyelerini etkileyen yeni keşfedilmiş kritik faktörlere ve bölgesel, ülkeye ve sektöre özel bilgiler dahil, ICS'nin tehditlere maruz kalması hakkında raporlar.
3. **Bulunan güvenlik açıkları.** Endüstriyel kontrol sistemlerinde, endüstriyel nesnelerin internetinde ve çeşitli sektörlerdeki altyapılarda kullanılan en popüler ürünlerde Kaspersky tarafından belirlenen güvenlik açıkları hakkında raporlar.
4. **Güvenlik açığı analizi ve azaltma.** Bilgilendirmelerimiz altyapınızdaki güvenlik açıklarını belirlemeye ve azaltmaya yardımcı olmak için Kaspersky uzmanlarından eyleme geçirilebilir tavsiyeler sunar.

Tehdit istihbaratı sayesinde

Tespit edin ve önleyin

Yazılım ve donanım bileşenleri dahil olmak üzere kritik varlıkları korumak ve teknolojik sürecin güvenliğini ve devamlılığını sağlamak için bildirilen tehditleri tespit edin ve önleyin

İlişkilendirin

Endüstriyel ortamlarda tespit ettiğiniz kötü niyetli ve şüpheli etkinlikleri Kaspersky'nin araştırma sonuçlarıyla ilişkilendirerek tespitinizi söz konusu kötü amaçlı kampanyaya bağlayın, tehditleri belirleyin ve olaylara anında müdahale edin

Değerlendirme yapın

Yama yönetimi konusunda bilinçli kararlar vermek ve Kaspersky tarafından tavsiye edilen diğer önleyici eylemleri gerçekleştirmek için güvenlik açığının kapsamı ve ciddiyetiyle ilgili doğru değerlendirmelere dayalı olarak endüstriyel ortamlarınız ve varlıklarınız için bir güvenlik açığı değerlendirmesi yapın

Destek alın

Şu amaçlarla, saldırı teknolojileri ve prosedürleri, yeni keşfedilmiş güvenlik açıkları ve diğer önemli tehdit alanı değişiklikleriyle ilgili bilgilerden destek alın:

- Bildirilen tehditlerin ve diğer benzer tehditlerin oluşturduğu riskleri belirlemek ve değerlendirmek
- Üretim güvenliğini ve teknolojik sürecin sürekliliğini sağlamak için endüstriyel altyapıdaki değişiklikleri planlamak ve tasarlamak
- Personel eğitim senaryoları hazırlamak ve kırmızı takıma karşı mavi takım alıştırmaları planlamak için gerçek yaşam senaryolarının analizine dayalı güvenlik farkındalığı aktiviteleri yürütmek
- Siber güvenliğe yatırım yapmak ve operasyonların esnekliğini sağlamak için bilinçli stratejik kararlar almak

Kaspersky Ask the Analyst

Siber suçlular, işletmelere saldırmak için sürekli olarak karmaşık yöntemler geliştiriyorlar. Günümüzdeki kısa süreli ve hızlı şekilde büyüyen tehdit ortamında gitgide daha hızlı bir hâl alan siber suç teknikleri görülmektedir. Kurumlar; kötü amaçlı yazılım olmayan saldırılar, dosyasız saldırılar, programların kontrolünü ele geçirmeye yönelik saldırılar, sıfır gün güvenlik açıkları ve bu saldırıların toplu olarak oluşturduğu karmaşık tehditler, APT benzeri ve hedeflenmiş saldırıların yol açtığı karmaşık olaylarla karşılaşmaktadır.

Sürekli tehdit araştırması

Kaspersky'nin saldırganların ve siber 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

İşletmeleri zor duruma sokan siber saldırıların yaşandığı 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 isteyebilme imkânına ihtiyaç duyar.** Haricî uzmanlık, karmaşık saldırıların veya APT'lerin olası yollarına ışık tutabilir ve bunları ortadan kaldırmanın en istikrarlı yolu hakkında eyleme dönüştürülebilir tavsiyeler sağlayabilir.

Ask the Analyst'ten Elde Edilenler

(Birleştirilmiş talep bazlı abonelik)

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

APT ve Suç Yazılımları

Yayınlanan raporlar ve devam eden araştırmalarla ilgili ek bilgiler (APT veya Suç Yazılım İstihbarat Raporlaması hizmetine ek olarak)[1]

Kötü Amaçlı Yazılım Analizi

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

Tehdit, güvenlik açıkları ve ilgili IoC'lerin açıklamaları

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

Karanlık Ağ İstihbaratı[2]

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

ICS ile ilgili istekler

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

[1] Yalnızca etkin APT ve/veya Suç Yazılım İstihbarat Raporlaması'na sahip müşteriler tarafından kullanılabilir

[2] Kaspersky Digital Footprint Intelligence aboneliğine dâhildir

HİZMET AVANTAJLARI

Uzmanlığınızı geliştirin

Bulması zor tam zamanlı uzmanlar aramak ve onları işe almaya yatırım yapmak zorunda kalmadan sektördeki uzmanlara talep üzerine erişme olanağı elde edin

İncelemeleri hızlandırın

Özel olarak hazırlanan ve ayrıntılı bağlamsal bilgilere dayanarak olayların önemini ve önceliğini etkili bir şekilde belirleyin

Hızlı müdahale edin

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

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 düzenleyebiliriz. Talebiniz kabul edildikten sonra işlenmesi için gereken tahmini zaman hakkında size bilgi verilecektir.

Hizmet kullanım durumları:

- Önceden yayınlanmış tehdit istihbaratı raporlarındaki bilgilere açıklık getirin
- Sağlanan IoC'ler için ilave istihbarat alın
- Güvenlik açıkları-na ilişkin bilgiler ve bu açıkların kötü etkilerine karşı na-sıl korunabileceği-nize dair öneriler edinin
- İlgilendiğiniz belirli Karanlık Ağ faaliyetleri hakkında ilave bilgiler edinin
- Kötü amaçlı yazılım davranışı, olası etkisi ve Kaspersky'nin gözlemlediği ilgili etkinlik hakkındaki bilgileri içeren, kötü amaçlı yazılım ailesine genel bakış raporu alın
- Kısa raporlar aracılığıyla sağlanan ilgili IoC'ler için ayrıntılı bağlamsal bilgiler ve sınıflandırma ile uyarıları/ olayları etkin bir şekilde öncelikli hâle getirin
- Tespit edilen sıra dışı faaliyetin bir APT veya suç yazılım etmeni ile ilgili olup olmadığını belirleme konusunda yardım talep edin
- Sağlanan örneklerin davranışını ve işlevselliğini anlamak amacıyla kötü amaçlı yazılım dosyalarını kapsamlı analiz için gönderin

Bilgi birikiminizi ve kaynaklarınızı genişletin

Kaspersky Ask the Analyst, vaka bazlı olarak Kaspersky araştırmacılarından oluşan temel bir gruba erişmenizi sağlar. Bu hizmet, eşsiz bilgi birikimimiz ve kaynaklarımızla mevcut yeteneklerinizi artırmak için uzmanlar arasında kapsamlı bir iletişim sağlar.

Kaspersky Takedown Hizmeti

Zorluk

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

Çözüm

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 etki alanlarını analiz etme konusunda yıllar boyu edindiğimiz deneyim, bu etki alanlarının kötü amaçlı olduğunu göstermek için gerekli tüm kanıtları nasıl toplayacağımızı bildiğimiz anlamına gelir. Ekibinizin diğer öncelikli görevlere odaklanabilmesi için dijital riskinizi en aza indirgemek üzere etki alanı kaldırma yönetiminizi üstlenerek 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.

Nasıl çalışır?

Taleplerinizi kurumsal müşteri destek portalımız olan Kaspersky Şirket Hesabı üzerinden gönderebilirsiniz. Gerekli tüm belgeleri hazırlayarak kaldırma talebini, etki alanını 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 etki alanlarının oluşturduğu tehditleri markanız ve işletmeniz herhangi bir zarar görmeden önce hızla azaltır. Bütün sürecin uçtan uca yönetimi size değerli zaman ve kaynak tasarrufu sağlar.

Hizmet avantajları

Küresel kapsam

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

Uçtan uca yönetim

Bütün kaldırma sürecini yöneterek sizin katılımınızı en aza indireceğiz.

Tam görünürlük

Talebinizin kaydedilmesinden etki alanının başarılı bir şekilde kaldırılmasına kadar, sürecin her aşamasında size bilgi vereceğiz.

Dijital Ayak İzi İstihbaratı ile Entegrasyon

Hizmet, markanıza/kuruluşunuza zarar vermek, onu kötüye kullanmak veya taklit etmek için tasarlanmış kimlik avı ve kötü amaçlı yazılım etki alanları hakkında gerçek zamanlı bildirimler sağlayan Kaspersky Dijital Ayak İzi İstihbaratı ile entegre olur. Tek bir çözüm, kapsamlı bir siber güvenlik stratejisinin önemli bir bileşenidir.

Temel avantajlar

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

Analistlerin mesleki tükenmişlik yaşamasını engelleyerek iş gücünüzün özgün tehditlere odaklanmasını 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

İyileştirilmiş ve hızlandırılmış olaya müdahale ve tehdit avlama kabiliyetleri, saldırı "bekleme süresinin" azaltılmasına ve olası hasarın önemli oranda azaltılmasına yardımcı olur

Sonuç

Günümüzün siber tehditleriyle mücadele etmek için tehdit aktörleri tarafından kullanılan taktikler ve araçların 360 derece görünümü gerekir. Bu istihbaratı oluşturma ve en etkili karşı önlemleri saptama, sürekli bağlılık ve yüksek uzmanlık düzeyi gerektirir. Kaspersky olarak, işlenecek petabaytlarca zengin tehdit verileri, gelişmiş makine öğrenimi teknolojileri ve tüm dünyadan eşsiz uzman havuzu ile, müşterilerimizin, önceden görülemeyen siber saldırılara karşı bile bağışıklıklarını sürdürmesine yardım ederek dünyanın dört bir yanından elde edilen en güncel tehdit istihbaratını sizlere sağlamaya çalışıyoruz.

FORRESTER®

Kaspersky, Forrester Wave'de Lider olarak konumlandırıldı: Dış Tehdit İstihbaratı Hizmetleri, 2021

Kaspersky Threat Intelligence

Daha fazla bilgi

www.kaspersky.com.tr