Kaspersky Threat Data Feeds

kaspersky geleceği yakalayın

Kaspersky Threat Data Feeds

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 zincirleri, saldırılar ve şirketinize yönelik geliştirdikleri Taktikler, Teknikler ve Prosedürler (TTP'ler) kullanır. Korunmak için tehdit istihbaratına dayalı yeni yöntemler gerektiği açıktır.

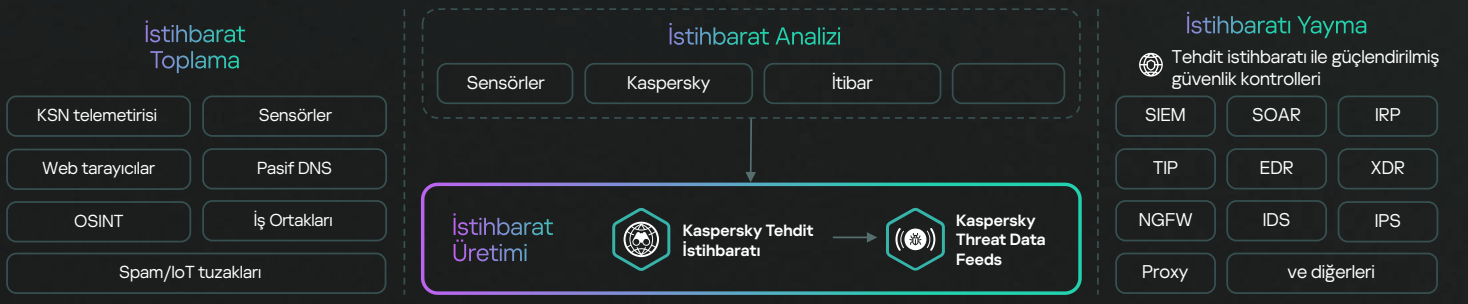
Güvenlik ekipleri, şüpheli ve tehlikeli IP'ler, URL'ler ve dosya karmaları ile ilgili bilgi içeren en güncel tehdit istihbaratı akışlarını SIEM, SOAR ve Tehdit İstihbaratı Platformları gibi mevcut güvenlik sistemlerine entegre ederek ilk uyarı triyajı süreçlerini otomatikleştirebilir ve triyaj uzmanlarına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

Bağlamsal veriler

Kaspersky tarafından sağlanan akışlardaki girişler, tehditleri hızlı bir şekilde onaylamanıza ve önceliklendirmenize yardımcı olan aşağıdaki bağlamsal verileri içerir:

- Tehdit adları
- Kötü amaçlı web kaynaklarının IP adresleri ve domain'leri
- Kötü amaçlı dosya grupları
- Savunmasız ve güvenliği ihlal edilmiş unsurlar
- MITRE ATT&CK sınıflandırmasına göre hazırlanmış saldırı taktikleri, teknikleri ve prosedürleri
- Zaman damgaları
- Coğrafi Konum
- Bilinirlik ve daha fazlası

Nasıl çalışır?



Kaspersky Threat Data Feeds, Kaspersky'nin birleştirilmiş, heterojen ve son derece güvenilir kaynaklarından toplanır:

Kaspersky SecurityNetwork

Büyük veri analitiği, makine öğrenimi ve insan uzmanlığından yararlanarak yeni tehditlere en hızlı yanıtı vermek için dünya çapında 400 milyondan fazla gönüllü katılımcıdan anonim siber tehdit verilerini toplayan ve analiz eden sofistike bulut altyapısı.

Web tarayıcılar

OSINT, Kaspersky analistlerinin araştırmaları ve kötü amaçlı yazılımlardan URL'leri çıkaran kendi otomatik işleme ve analiz sistemlerimiz gibi çeşitli kaynaklardan yeni kötü amaçlı yazılım ve yasal örnekler toplar.

BotFarm'lar

Özel botnet araştırma ekibi, değerli tehdit istihbaratı elde etmek için bot yapılandırmalarını çıkarır, iletişim protokollerini ters mühendisliğe tabi tutar ve komuta merkezlerinden gelen komutları izler.

Spam tuzakları

Kimlik avı önleme sistemlerimiz her yıl 500 milyondan fazla kimlik avı bağlantısı tıklamasını ve 160 milyondan fazla kötü amaçlı e-posta ekini önlüyor ve bunlardan veri akışlarımızı zenginleştirmek için ek veriler elde ediyoruz.

İş Ortakları

Kötü amaçlı örnekleri diğer satıcılar ve siber güvenlik kuruluşları ile paylaşmak için ortaklıklara katılıyoruz.

Sensörler

Sanal sunucular, sinkhole'lar ve ITW saldırılarını engellemeye yönelik diğer yöntemler. Örneğin (IoT cihazları, savunmasız sistemler, yazılım vb). Kaspersky analistleri, saldırganların saldırı girişimlerini ve yöntemlerini araştırır, tehlikeye girme göstergelerini çıkarır ve bunları diğer veri kaynaklarıyla ilişkilendirir.

Pasif DNS

Veriler, barındırma kuruluşları ve İnternet Servis Sağlayıcıları gibi güvenilir üçüncü taraflardan küresel olarak toplanır.

OSINT

Saldırgan veriler; haber kaynakları, sosyal medya, kamu raporları, karanlık web vb. gibi kamuya açık kaynaklardan otomatik olarak toplanır. Bu verileri, düşmanın altyapısını keşfeden yeni kötü amaçlı örnekleri aramak ve bilgi tabanımıza sürekli olarak eklemek için kullanıyoruz.

Algılanan her gösterge, yanlış pozitifleri ayıklamak için güven ve itibar teknolojilerini ve yüz milyonlarca gerçek güvenilir ve kötü amaçlı dosyadan alınan örnekler üzerinde eğitilmiş makine öğrenimi modellerini kullanan otomatik bir işleme sisteminde çok aşamalı bir tarama sürecinden geçer. Her bir gösterge aynı zamanda TTP'ler, ağ davranışı, işletim sistemi davranışı ve bir dizi başka ilişki gibi düzinelerce ek özelliğin çıkarıldığı birden fazla korumalı alanda analiz edilir.

Tüm bunlar Kaspersky Threat Intelligence'ı, tehdit izleme merkezlerinizi güçlendirebilecek ve kuruluşunuzun ön saflarındaki düşmanları tespit edebilecek güçlü bir taktiksel düzeyde istihbarat kaynağına dönüştürür.

Öne Çıkan Noktalar

Veri Akışları, dünya genelindeki bulgulara dayalı olarak gerçek zamanlı olarak otomatik olarak oluşturulur ve yüksek tespit oranları ve doğruluk sağlar.

Ek belgeler, örnekler, özel bir teknik müşteri yöneticisi ve Kaspersky'nin teknik desteği ile uygulama kolaylığı sağlanır ve bunların tümü kolay entegrasyon sağlamak için bir araya getirilir.

FTP, HTTPS veya özel iletim mekanizmaları yoluyla basit ve hafif dağıtım biçimleri (JSON, CSV, OpenIoC, STIX), akışların güvenlik çözümlerine kolayca entegre edilmesini destekler Önde gelen SIEM'ler ve TI Platformları tam olarak desteklenmektedir.

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

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

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

Avantajlar

1

SIEM'ler, Güvenlik Duvarları, NGFW, IPS/IDS, Güvenlik Proxy'si, DNS çözümleri, Anti-APT dâhil 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.

2

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.

3

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 enfekte olmuş varlıkları hızlı bir şekilde tespit eder.

4

Bir Yönetilen Güvenlik Hizmeti Sağlayıcısı (MSSP) olarak, müşterilerinize üst düzey bir hizmet sunmak amacıyla sektör lideri tehdit istihbaratı sağlayarak işinizi büyütün.

5

Bilgisayar Acil Durum Müdahale Ekibi (CERT) olarak sahip olduğunuz siber tehdit algılama ve tanımlama yetkinliğini geliştirin ve genişletin.

Kaspersky Tehdit İstihbaratı

Kaspersky Threat Intelligence, birinci sınıf analistlerimiz ve araştırmacılarımız tarafından toplanan geniş bir bilgi yelpazesine erişim sağlar. Bu veriler, kuruluşunuzun günümüzün siber tehditlerine etkili bir şekilde karşı koymasına yardımcı olacaktır.

Şirketimiz, siber tehdit araştırmalarında derin bilgi birikimine, kapsamlı deneyime ve siber güvenliğin tüm yönlerine ilişkin benzersiz içgörülere sahiptir ve güncel taktiksel, operasyonel ve stratejik tehdit istihbaratı sağlar. Bu, bizi Interpol ve çeşitli CERT birimleri de dâhil olmak üzere dünyanın dört bir yanındaki kolluk kuvvetleri ve devlet kuruluşlarının güvenilir bir ortağı haline getirdi. Ve tüm bunlar Kaspersky Threat Intelligence Portal aracılığıyla ilgili, eyleme geçirilebilir veriler olarak size sunulur.

Kaspersky Threat Intelligence

Daha fazla bilgi edinin

www.kaspersky.com.tr

#kaspersky
#geleceğiyakalayın