Tehdit İstihbaratı Platformu

Kaspersky CyberTrace

kaspersky geleceği yakalayın

Kaspersky CyberTrace

Bir Tehdit İstihbaratı Platformu, analistlerin mevcut güvenlik operasyonu iş akışlarında tehdit istihbaratından daha etkili bir biçimde faydalanmasına yardımcı olmak üzere tehdit veri akışları ile SIEM çözümlerinin kusursuz entegrasyonunu sağlar.

Etkili uyarı saptaması ve analizinin mümkün kılınması

Siber güvenlik analistleri tarafından işlenen uyarıların sayısı katlanarak artıyor. Analiz edilen bu kadar veri içerisinde uyarıların etkili bir biçimde önceliklendirilmesi, saptanması ve doğrulanması neredeyse imkansızdır.

Çok sayıda güvenlik ürününden sayısız yanıp sönen ışık gelir. Dolayısıyla önemli uyarılar bu kalabalığın içerisinde kaybolur ve analistler sıkıntıya girer. SIEM'ler ve diğer güvenlik analiz araçları olayları ilişkilendirir ve uyarıların sayısını azaltmaya yardımcı olur, ancak güvenlik analistlerinin aşırı yükü devam etmektedir.

SIEM sistemleri

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

Tehdit veri akışları ile mevcut tehdit istihbaratı kaynaklarındaki sürekli büyüme, kuruluşların hangi bilgilerin ilgili olup olmadığını belirlemesini zorlaştırır. Tehdit istihbaratlarının farklı formatlarda olması ve çok sayıda Tehlike Belirtisi (IoC'ler) içermesi, SIEM veya ağ güvenliği kontrollerinin bu istihbaratı işlemesini daha zor bir hale getirir.

Entegrasyonlar

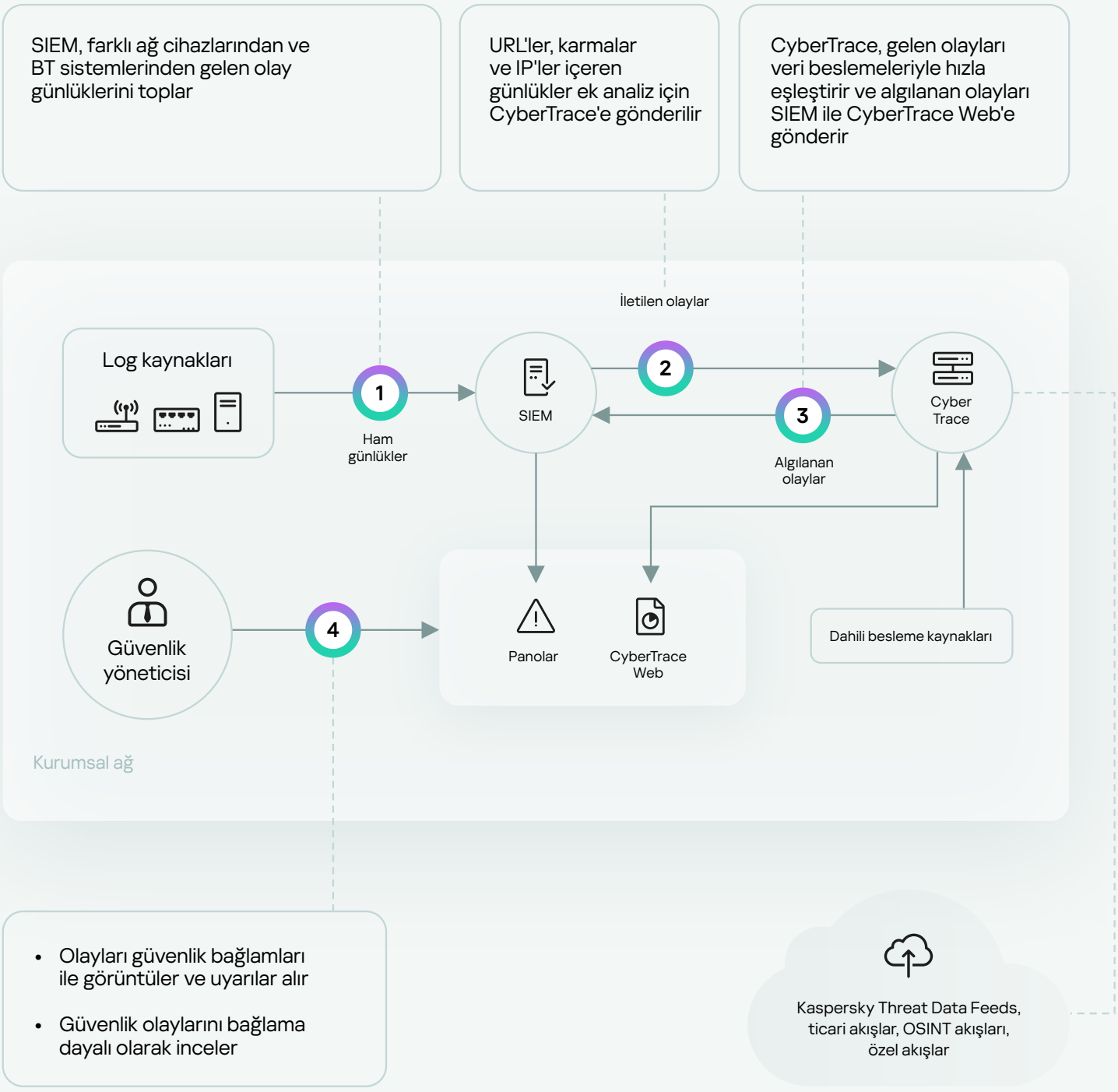
Kaspersky CyberTrace; JSON, STIX, XML ve CSV formatlarındaki tüm tehdit istihbaratı veri akışlarıyla entegre edilebilir:

1. Kaspersky tehdit istihbaratı veri akışları
2. Diğer markaların veri akışları
3. OSINT veya özel akışlarınız

Müşterilerin rahatlığı için CyberTrace, çok sayıda SIEM çözümü ve günlük kaynağı ile kullanıma hazır entegrasyonu destekler.

Kaspersky CyberTrace entegrasyon şeması

Kaspersky CyberTrace, SIEM iş yükünü önemli ölçüde azaltarak ek gelen veri ayrıştırma ve eşleştirme katmanı ile SIEM kapasitesini geliştirebilir. Olayları veri akışlarından gelen bilgilerle eşleştirmek, tehditleri belirlemeye ve tespit edilen olaylara değerli bir bağlam sağlanmasına yardımcı olur. Yüksek seviyeli çözüm entegrasyonu mimarisi aşağıdaki şekilde gösterilmiştir.



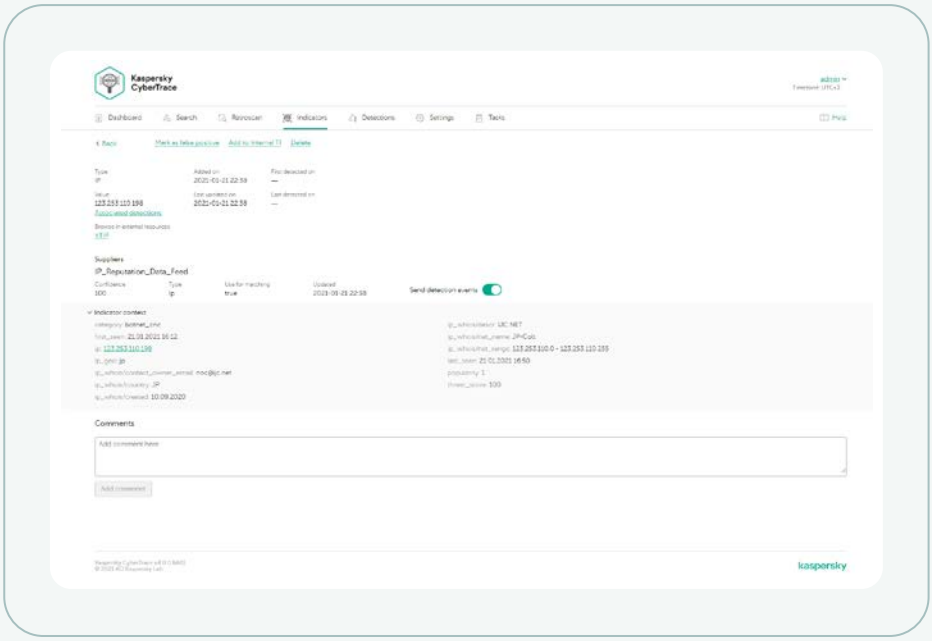
Ürün özellikleri

Kaspersky CyberTrace, etkili uyarı saptama ve ilk yanıt için tehdit istihbaratını işlevsel hale getiren bir dizi araç sunar:

Bir gösterge için tüm istihbarat sağlayıcılarından gelen ayrıntılı bilgiler

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. Sonuçları istihbarat sağlayıcılarına göre filtreleme, tehdit istihbaratı analizi sürecini basitleştirir.

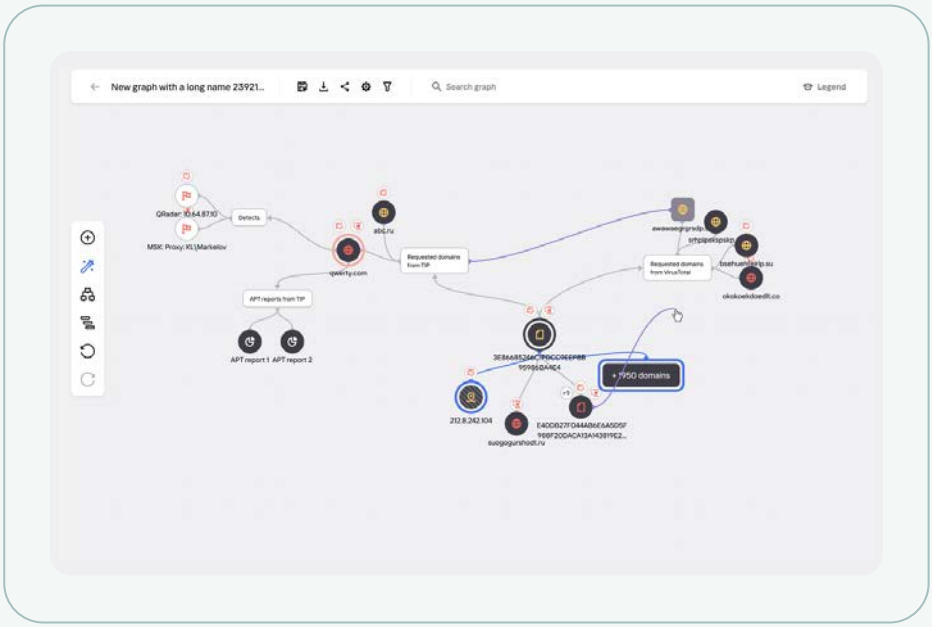
Ulusal/Devlet/Finansal Bilgisayar Acil Durum Müdahale Ekipleri (CERT'ler), TI satıcıları ve topluluklardan gelen e-posta abonelikleri ve PDF belgeleri CyberTrace için IoC kaynağı olarak kullanılabilir. IOC'lerin hem e-posta gövdesinden hem de ekinden (XML, CSV, JSON, PDF) çıkarılması mümkündür. IMAP/POP3 sunucuları ve PDF dosyalarından oluşan bir koleksiyona sahip yerel/paylaşılan klasörler besleme kaynağı olarak kullanılabilir.



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. Göstergelerin algılanması halinde algılama tarihleri hakkındaki bilgilerle algılanan gösterge listesi bağlantıları kullanıma sunulur.

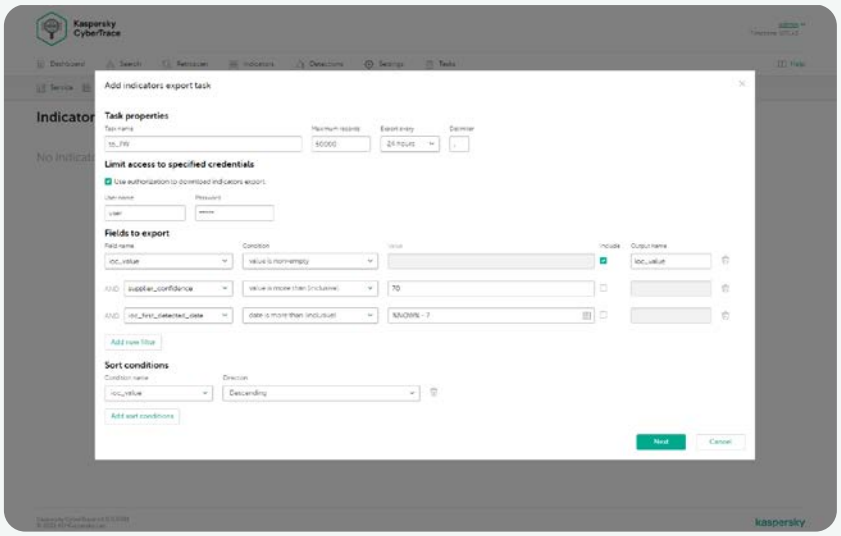
Araştırma Grafiği

Araştırma Grafiği, CyberTrace üzerinde depolanan verileri ve algılamaları görsel olarak keşfetmenizi ve tehdit benzerliklerini görmenizi sağlar. Aynı zamanda araştırmalar sırasında karşılaşılan URL'ler, etki alanları, IP'ler, dosyalar ve diğer bağlamlar arasındaki ilişkinin grafik olarak görselleştirilmesini sağlar. Grafik, şu özellikleri içermektedir: dönüştürmeler, mini grafik, düğümleri gruplandırma, manuel olarak bağlantı ekleme, gösterge ekleme ve grafikte düğüm arama. VirusTotal'dan Araştırma Grafiği üzerinde IoC zenginleştirmesi desteklenir.



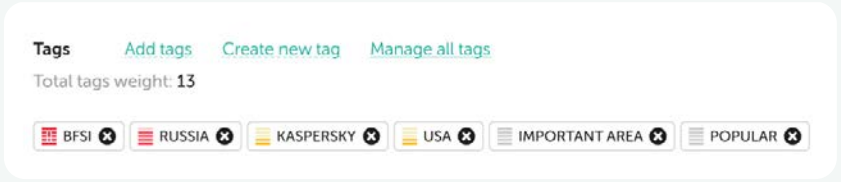
Göstergeleri dışa aktarım görevi

Göstergele dışa aktarım özelliği, dışa aktarılan IoC'lerin ilke listeleri (engelleme listeleri) gibi üçüncü taraf güvenlik kontrolleriyle yerel entegrasyonunu ve tehdit verilerinin Kaspersky CyberTrace örnekleri arasında veya diğer TI Platformlarıyla paylaşılmasını destekler.



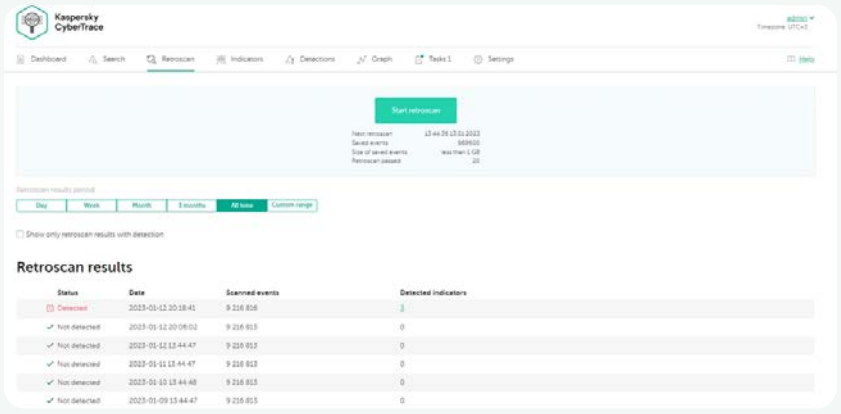
IoC etiketleri

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.



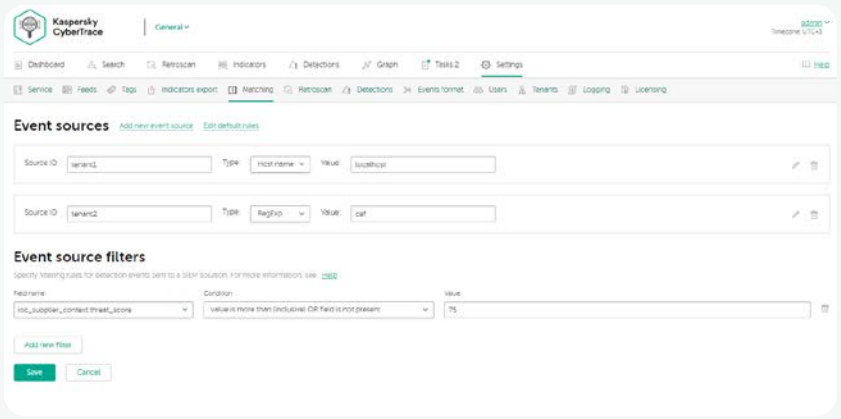
Geriye dönük tarama özelliği

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. Gelecek incelemeler için geçmişe yönelik tüm algılamalar rapora dahil edilir.



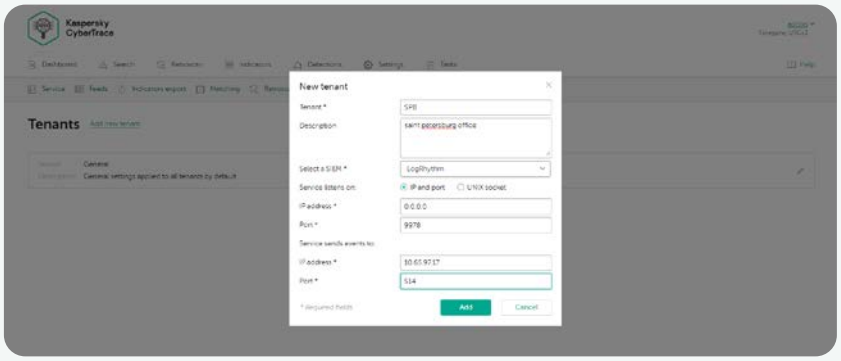
Olay kaynağı filtreleri

Algılama olaylarını SIEM çözümlerine göndermede kullanılan filtre, uyarı yorgunluğu ile mücadele eden analistler ve bu çözümler üzerindeki yükü hafifletir. Yalnızca olay olarak işlenmesi gereken, en tehlikeli algılamaları SIEM sistemine göndermenize olanak tanır. Tüm diğer algılamalar, dahili veri tabanına kaydedilir ve temel neden analizi veya tehdit avlama için kullanılabilir.



Çoklu kullanım desteği

Çoklu Kullanım özelliği, hizmet sağlayıcılarının (merkez ofis) farklı şubelerden (kullanıcı) gelen olayları ayrı ayrı işlemeleri gereken durumlarda büyük kurumların kullanımlarını veya MSSP'leri destekler. Bu özellik, tek bir Kaspersky CyberTrace örneğinin farklı kullanıcılara ait birden çok SIEM çözümüne bağlanmasına izin verir. Ayrıca her kullanıcı için hangi akışların kullanılacağını yapılandırabilirsiniz.



Gösterge istatistikleri ve akış kesişim matrisi

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

Rest API kullanılarak Kaspersky CyberTrace, otomasyon ve düzenleme için karmaşık ortamlara kolayca entegre edilebilir. Kaspersky'nin olay izleme, analiz ve müdahale platformu ile entegrasyon mümkündür.

Diğer ürün özellikleri

- Algılanan tehditlere ilişkin verileri yönetmek ve görselleştirmek üzere çok çeşitli SIEM çözümleri için SIEM konektörleri
- Derinlemesine tehdit incelemesi için talep üzerine gösterge arama (karmalar, IP adresleri, etki alanları, URL'ler)
- Akışlar için gelişmiş filtreleme
- Günlükler ve dosyalar için toplu tarama
- Windows ve Linux platformları için komut satırı arayüzü
- Kaspersky CyberTrace'in ağ cihazları gibi farklı kaynaklardan gelen günlükleri aldığı ve ayrıştırdığı bağımsız mod
- Ve çok daha fazlası

Kaspersky CyberTrace ve Kaspersky Threat Data Feeds ayrı ayrı kullanılabilir ancak birlikte kullanıldıklarında tehdit algılama kapasitenizi büyük oranda geliştirir ve siber tehditlerle ilgili küresel görünürlük sağlayarak güvenlik operasyonlarınıza güç katarlar.

Kaspersky CyberTrace ve Kaspersky Threat Data Feeds ile kuruluşların yapabilecekleri:

Güvenlik uyarıları etkili biçimde ayrıştırılabilir ve önceliklendirilebilir.

Analistlerin iş yükü azaltılarak tükenmişlik durumunun önüne geçilebilir.

Kritik uyarılar hemen tespit edilerek hangilerinin olay yanıt ekiplerine taşınacağı hakkında daha bilinçli kararlar verilebilir

Proaktif ve istihbarata dayalı bir savunma oluşturulabilir.

Kaspersky CyberTrace

Daha fazla bilgi edinin

www.kaspersky.com.tr

#kaspersky
#geleceğiyakalayın