kaspersky GELECEĞİ YAKALAYIN

Kaspersky CyberTrace

Her gün bilgi güvenliği analistleri tarafından işlenen güvenlik uyarılarının 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 tükenmişliğe girer. Güvenlik verilerini toplayan ve ilgili uyarılar arasında ilişki kuran SIEM'ler, günlük yönetimi ve güvenlik analizi araçlarının tamamı ek inceleme gerektiren uyarı sayısını azaltmaya yardımcı olsa da güvenlik analistlerinin üzerindeki aşırı yük azalmaz.

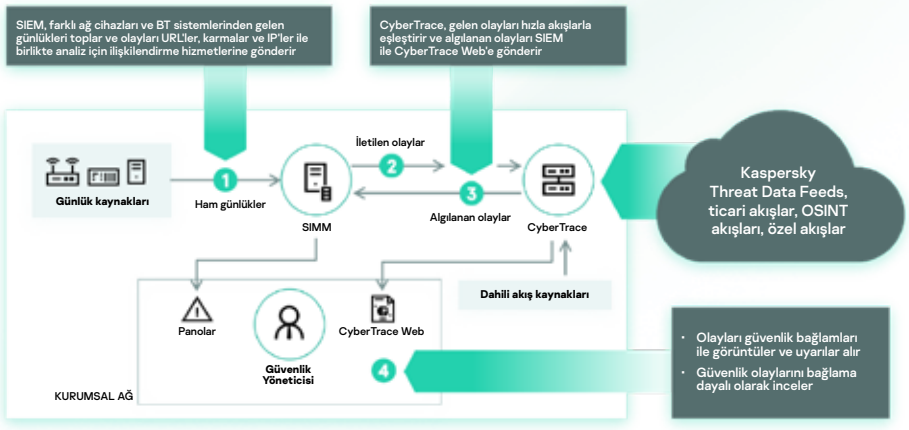
Tehdit istihbaratlarının farklı formatlarda olması ve çok sayıda Tehlike Belirtisi (IoC'ler) içermesi, SIEM veya ağ güvenliği kontrollerinin bu istihbaratı işlemesini daha zor bir hale getirir.

Etkili uyarı saptaması ve analizinin mümkün kılınması

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 olması ve çok sayıda Tehlike Belirtisi (IoC'ler) içermesi, SIEM veya ağ güvenliği kontrollerinin bu istihbaratı işlemesini daha zor bir hale getirir.

Kaspersky CyberTrace, analistlerin mevcut güvenlik operasyonu iş akışlarında tehdit istihbaratından daha etkili bir biçimde faydalanmasına yardımcı olmak üzere tehdit veri akışları ile SIEM çözümlerinin kusursuz entegrasyonunu sağlayan bir Tehdit İstihbaratı Platformudur. Kullanmak isteyebileceğiniz JSON, STIX, XML ve CSV formatındaki her türlü tehdit istihbaratı akışı (Kaspersky'den, diğer satıcılardan ve OSINT'ten gelen tehdit istihbaratı akışları veya özel akışlarınız) ile entegre olur ve çok sayıdaki SIEM çözümü ve günlük kaynağıyla kullanıma hazır entegrasyonu destekler.

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

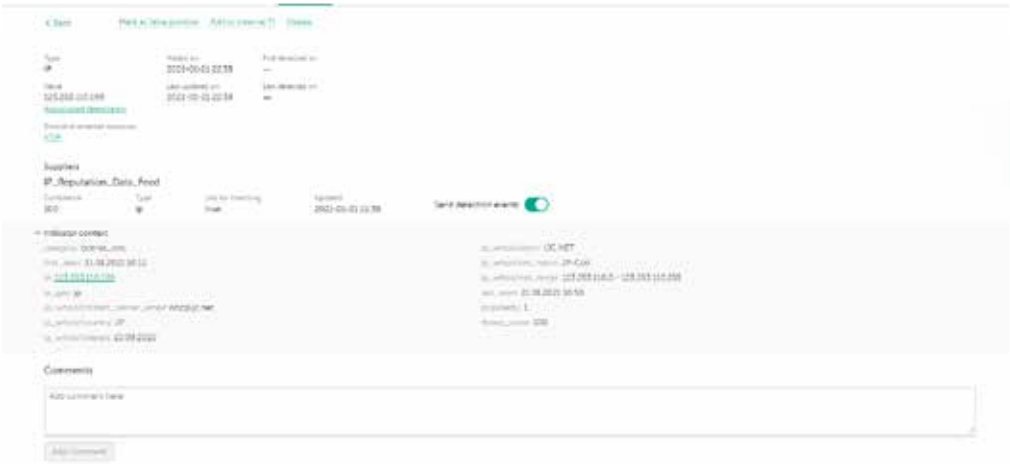


Şekil 1. Kaspersky CyberTrace entegrasyon şeması

Ürün özellikleri

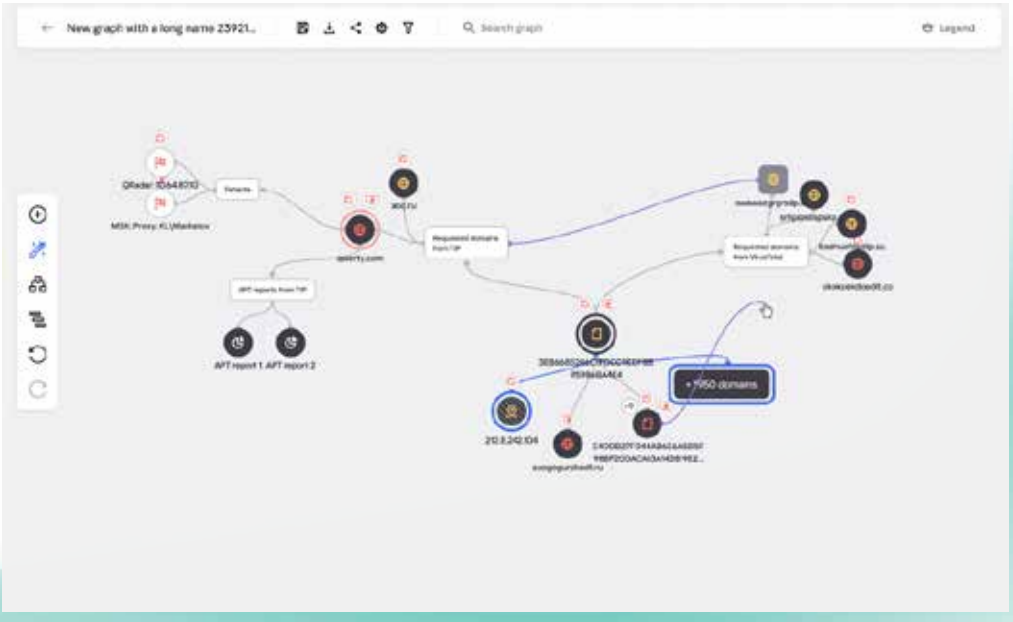
Kaspersky CyberTrace, etkili uyarı saptama ve ilk yanıt için tehdit istihbaratını işlevsel hale getiren bir dizi araç sunar:

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



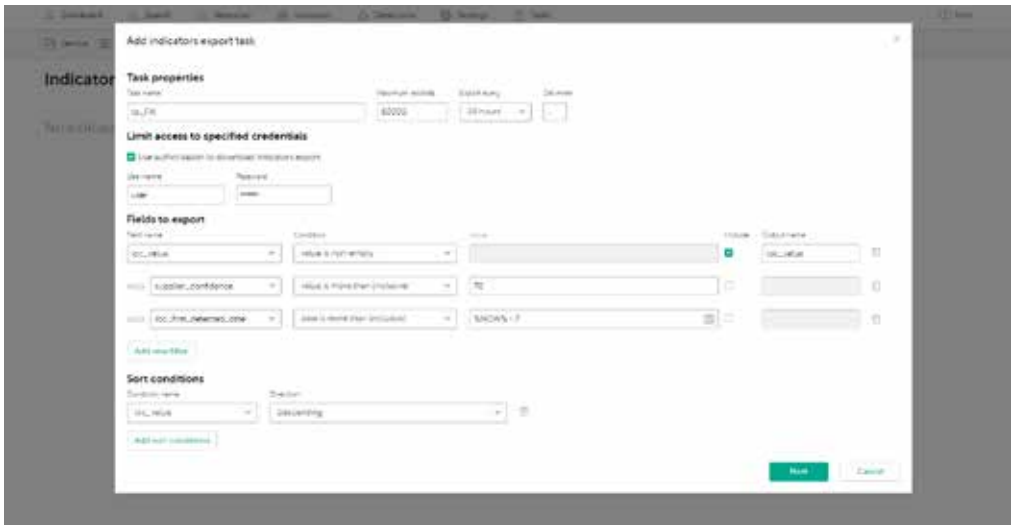
Şekil 2. Bir gösterge için tüm istihbarat sağlayıcılarından gelen ayrıntılı bilgiler

- 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.



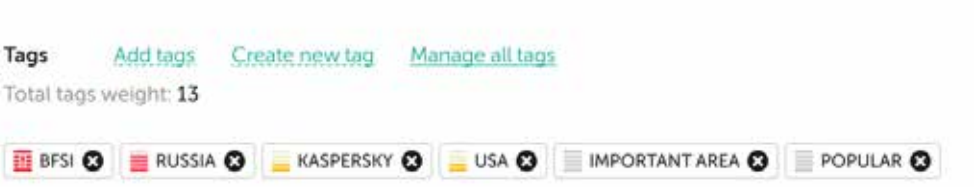
Şekil 3. Araştırma Grafiği

- 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 paylaşılmasını destekler.



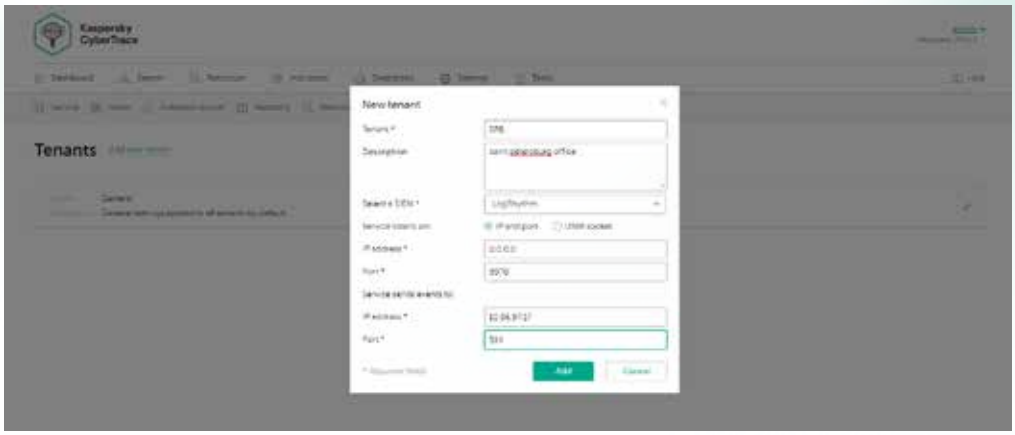
Şekil 4. Göstergeleri dışa aktarım görevi

- 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.



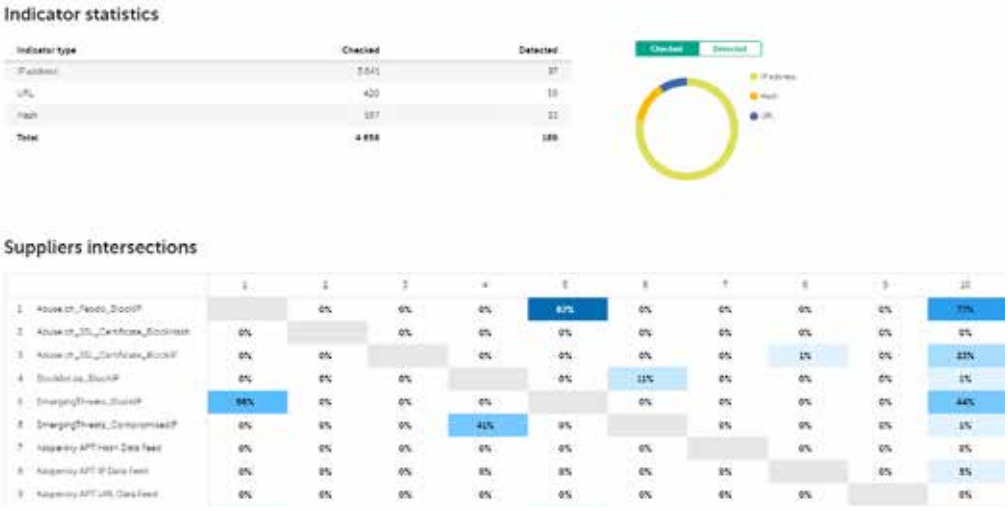
Şekil 5. IoC etiketleri

- 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.
- 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 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.



Şekil 6. Yeni kullanıcı oluşturma

- Entegre akışların ve akış kesişim matrislerinin etkinliğini ölçmek için kullanılan akış kullanım istatistikleri, en değerli tehdit istihbaratı sağlayıcılarının seçilmesine yardımcı olur.



Şekil 7. Gösterge istatistikleri ve akış kesişim matrisi

- HTTP RestAPI, tehdit istihbaratlarını aramanıza ve yönetmenize yardımcı olur. Kaspersky CyberTrace, RestAPI kullanılarak otomasyon ve düzenleme için kolaylıkla karmaşık ortamlara entegre edilebilir.
- Web UI entegrasyonu da dahil (tek kullanıcı arayüzü) Kaspersky Unified Monitoring and Analysis (KUMA) Platformu ile entegrasyonu destekler.

Kaspersky CyberTrace ve Kaspersky Tehdit Veri Akışları 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 Tehdit Veri Akışları 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.

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

Siber Tehdit Haberleri: www.securelist.com
BT Güvenliği Haberleri: business.kaspersky.com
KOBİ'ler için BT Güvenliği: kaspersky.com.tr/business
Kurumlar için BT Güvenliği: kaspersky.com.tr/enterprise
Tehdit İstihbaratı Portalı: opentip.kaspersky.com

www.kaspersky.com.tr

Kanıtlanmış başarılara sahibiz. Bağımsızız. Şeffafız. Teknolojinin hayatlarımızı geliştirdiği, daha güvenli bir dünya oluşturmakta kararlıyız. Bu nedenle teknolojiyi, sunduğu sonsuz sayıdaki fırsattan herkes yararlanabilsin diye daha güvenli hale getiriyoruz. Daha güvenli bir gelecek için siber güvenliğe önem verin.

kaspersky.com/transparency adresini ziyaret ederek daha fazla bilgi alın

Proven.
Transparent.
Independent.