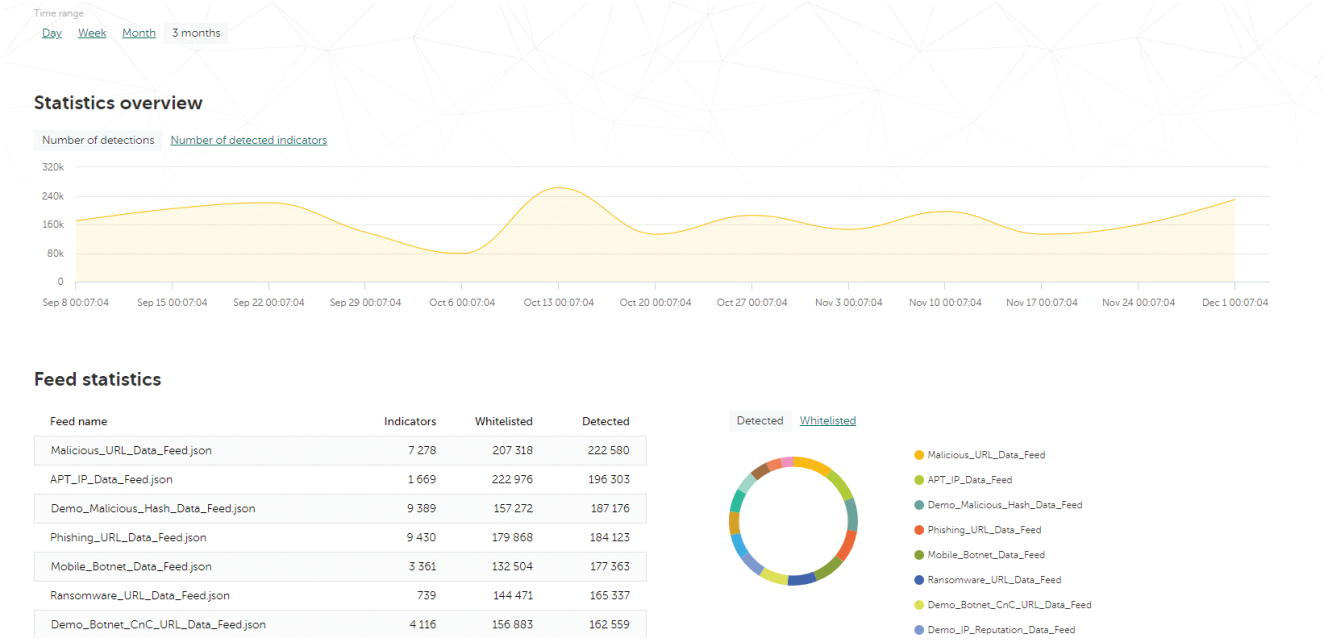
Kaspersky® CyberTrace

Güvenlik İşlemleri Merkezi'nin Katman 1 analistleri tarafından işlenen güvenlik uyarıları sayısı her gün artıyor. Böyle büyük miktarda veri analiz edilirken, etkili uyarı önceliği belirlemek, deneme yapmak ve doğrulamak neredeyse imkansızdır. Çeşitli güvenlik ürünlerinden sayısız sinyal geliyor, bu da önemli uyarıların arada kaynamasına ve analistin yorulmasına sebep oluyor. Güvenlik verilerini toplayan ve ilgili alarmları ilişkilendiren SIEM'ler, günlük yönetimi ve güvenlik analizi araçları, ek denetimler gerektiren uyarıların sayısını azaltmaya yardımcı olur, ancak Katman 1 uzmanları aşırı iş yüküne maruz kalmaya devam eder.

Etkin uyarı öncelik belirlemesini ve analizini etkinleştirme

Güvenlik İşletim Merkezleri, SIEM sistemleri gibi, en güncel makine tarafından okunabilir tehdit istihbaratını mevcut güvenlik kontrollerine entegre ederek, soruşturulması veya daha derinlemesine araştırılması ve yanıtlanması için Olay Müdahale (IR) ekiplerine gönderilmesi gereken uyarıları anında tanımlamayı sağlamak için Katman 1 uzmanlarına yeterli bağlam sunarak ilk deneme sürecini otomatikleştirebilir. Ancak, tehdit veri akışları ve kullanılabilir tehdit istihbarat kaynakları sayısındaki durmak bilmeyen artış, kuruluşların hangi bilgilerin geçerli olduğunu belirlemesini zorlaştırır. Tehdit istihbaratı farklı formatlarda sağlanır ve çok sayıda Risk Göstergesi (IoC) içerir, bu da SIEm'lerin veya ağ güvenlik denetimlerinin bunları özetlemesini zorlaştırır.

Kaspersky CyberTrace; analizcilerin mevcut güvenlik operasyonları iş akışlarındaki tehdit istihbaratını daha etkili bir şekilde geliştirmelerine yardımcı olmak için SIEM çözümleriyle tehdit veri akışlarının sorunsuz entegrasyonunu sağlayan bir tehdit istihbarat füzyonu ve analiz aracıdır. Kullanmak istediğiniz herhangi bir tehdit istihbarat akışıyla (JSON, STIX, XML ve CSV formatlarında) (Kaspersky, diğer satıcılar, OSINT veya özel akışlarınız için tehdit istihbarat akışları) entegre olur ve çeşitli SIEM çözümleriyle ve günlük kaynaklarıyla entegrasyonu destekler. Kaspersky CyberTrace, günlük dosyalarını tehdit istihbarat akışlarıyla otomatik olarak eşleştirerek gerçek zamanlı 'durumsal farkındalık' sağlayarak Katman 1 analistlerinin zamanında ve daha bilgiye dayalı kararlar almasına olanak tanır.

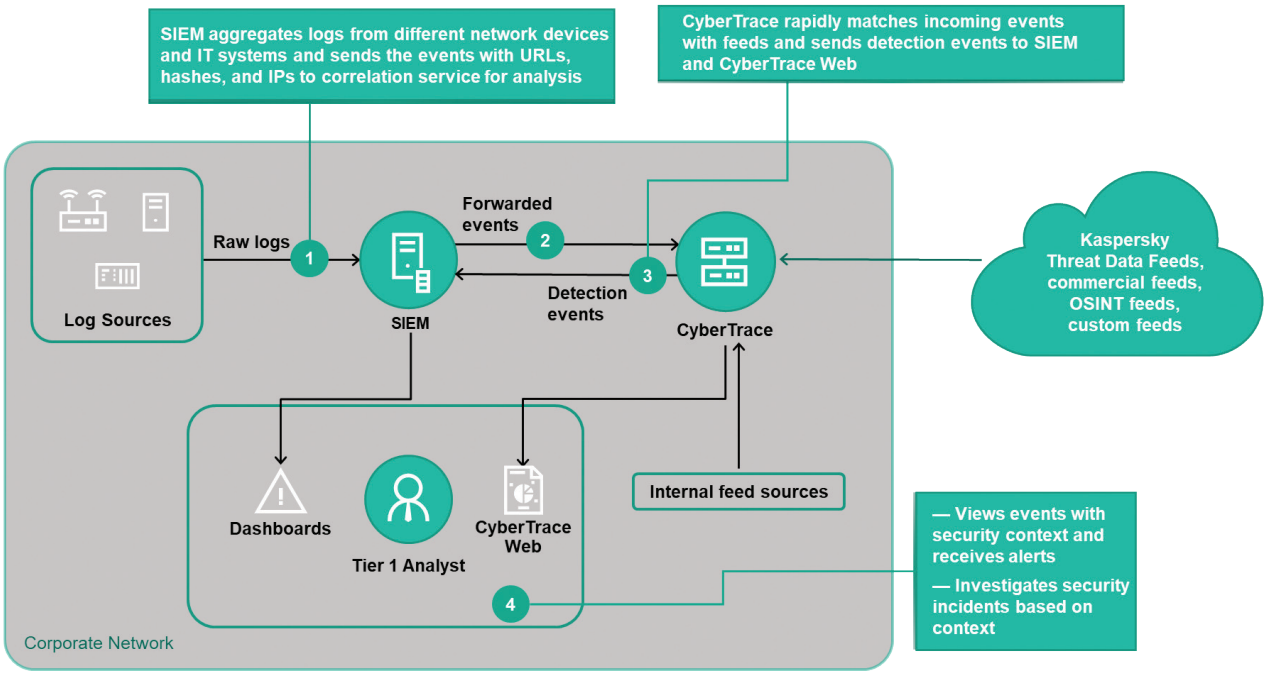


Şekil 1. Kaspersky CyberTrace istatistikleri

Kaspersky CyberTrace, etkin uyarı öncelik belirlemesi ve öncül yanıt yürütmesi için tehdit istihbaratını işlevselleştirmek üzere bir dizi araç sağlar:

- Kaspersky Lab ve OSINT akışlarından gelen demo tehdit veri akışları kullanıma hazır
- Tehdit algılamaları hakkında verileri görselleştirmek ve yönetmek için geniş SIEM çözümlerine yönelik SIEM konektörleri
- Entegre akışların etkinliğini ölçmek için akış kullanım istatistikleri
- Kapsamlı tehdit araştırması (karma, IP adresleri, etki alanları, URL'ler) için isteğe bağlı gösterge araması
- Veri görselleştirme, yapılandırmaya erişim, ilerleme yönetimi, günlük ayrıştırma kuralları, kara listeler ve beyaz listeler sağlayan bir web kullanıcı arabirimi
- Akışlar için gelişmiş filtreleme (tehdit türü, coğrafi konum, popülerlik, zaman damgaları ve daha fazlası dahil olmak üzere göstergelerin her biriyle sağlanan içeriğe göre) ve günlük olayları (özel koşullara dayalı)
- Diğer sistemlerle (güvenlik duvarları, ağ ve ana bilgisayar kimlikleri, özel araçlar) entegrasyon için veri akışlarıyla eşleşen arama sonuçlarının CSV biçiminde dışa aktarılması
- Günlüklerin ve dosyaların toplu taranması
- Windows ve Linux platformları için komut satırı arabirimi
- Kaspersky CyberTrace'in bir SIEM ile entegre olmadığı ancak ağ aygıtları gibi çeşitli kaynaklardan gelen günlükleri alıp ayrıştırdığı bağımsız mod
- İnternetten izole edilmesi gereken DMZ destekli senaryolarda kurulum.

Araç, gelen verileri ayrıştırmak ve eşleştirmek için SIEM iş yükünü önemli ölçüde azaltan bir içselleştirilmiş işlem kullanır. Kaspersky CyberTrace gelen günlükleri ve olayları ayrıştırır, ortaya çıkan verileri akışlarla hızlıca eşleştirir ve tehdit algılamasında kendi uyarılarını oluşturur. Yüksek düzeyde bir çözüm entegrasyonu mimarisi aşağıdaki şekilde gösterilmiştir:



Şekil 2. Kaspersky CyberTrace entegrasyon şeması

Kaspersky Lab ayrıca Kaspersky CyberTrace ile entegre edilebilen ve global tehdit görünürlüğü, siber tehditlerin zamanında algılanması, güvenlik uyarılarının önceliklendirilmesi ve bilgi güvenliği olaylarına etkili yanıt sağlayan bir dizi sürekli güncellenen tehdit veri akışı sunar:

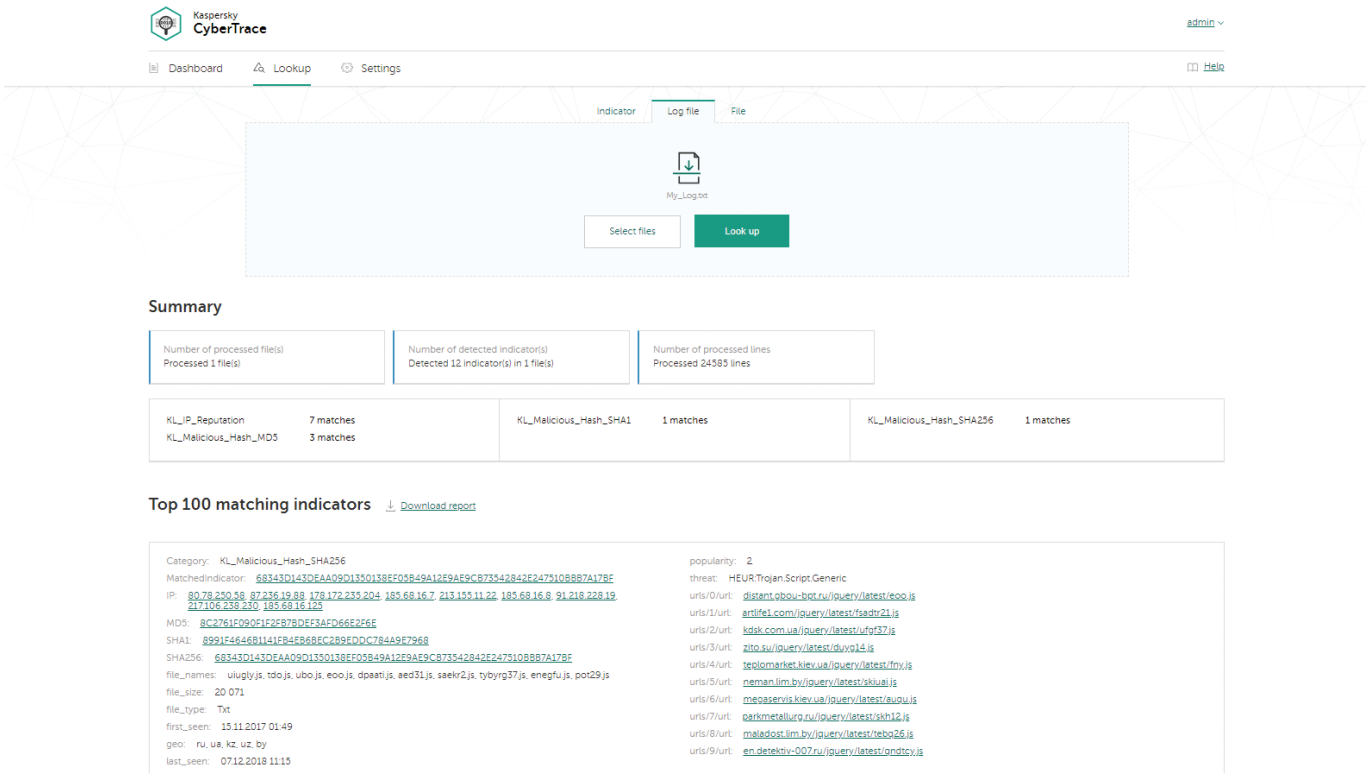
- IP bilinirlik akışı: farklı kategorilerden şüpheli ve kötü amaçlı ana bilgisayarları kapsayan IP adreslerinden oluşan bağlama sahip bir set
- Kötü Amaçlı ve Kimlik Avı URL Akışı: kötü amaçlı ve kimlik avı amaçlı bağlantıları ve web sitelerini kapsar
- Botnet Komuta ve Kontrol (C&C) URL Akışı: masaüstü botnet komuta ve kontrol sunucularını ve ilgili kötü amaçlı nesneleri kapsar
- Mobil Botnet Komuta Kontrol URL Akışı: mobil botnet komuta ve kontrol

sunucularını kapsar
- Fidye Yazılımı URL Akışı: fidye yazılımı nesnelerini barındıran veya bunlar tarafından erişilen bağlantıları kapsar
- APT IoC akışları – Düşmanlar tarafından APT saldırıları yapmak için kullanılan kötü amaçlı etki alanlarını, ana bilgisayarları, kötü amaçlı IP adreslerini ve kötü amaçlı dosyaları kapsar
- Pasif DNS (pDNS) akışı – etki alanları için DNS çözümlerinin sonuçlarını ilgili IP adreslerinde içeren bir kayıt kümesi[1]
- IoT URL akışı – IoT aygıtlarına bulaşan kötü amaçlı yazılımları yüklemek için kullanılan web sitelerini kapsar[2]
- Kötü Amaçlı Karma Akışı: en tehlikeli, yaygın ve yeni ortaya çıkan kötü amaçlı yazılımları kapsar
- Mobil kötü amaçlı yayın akışı – Android ve iOS mobil platformlarına bulaşan kötü amaçlı nesneleri kapsar
- P-SMS Truva Atı akışı: saldırganların SMS mesajlarını çalmasını, silmesini ve onlara yanıt vermesini sağlamanın yanı sıra mobil kullanıcılar için fazla ücrete neden olan SMS Truva Atları'nı kapsar
- Beyaz Liste veri akışı: yasal yazılımlar hakkında sistematik bilgi sağlayarak üçüncü taraf çözümleri ve hizmetleri sunar.

Veri akışları; Kaspersky Security Network ve siber tehditlere ilişkin verilerini gönüllü olarak bizimle paylaşan 100 milyon+ global kullanıcısı, kendi web gezintilerimiz, botnet izleme sistemi (365 gün 7/24 bilinen bütün botnetleri, bu botnetlerin hedeflerini ve etkinliklerini izler), spam tuzakları, tehdit araştırma ekipleri ve güvenilir ortakları dahil olmak üzere, heterojen ve son derece güvenilir kaynakların kaynaştırılmış bir kombinasyonundan oluşturulmaktadır.

Daha sonra toplanan veriler gerçek zamanlı olarak denetlenir ve sadeleştirilir. Bu işlemler için istatistik kriterleri, Kaspersky Lab Uzman Sistemleri (koruma alanları, sezgisel motorlar, çoklu tarayıcılar, benzerlik araçları ve davranış profili oluşturma) analist doğrulaması ve beyaz liste onayı gibi birçok ön işleme tekniği kullanılır.

Veri akışlarındaki her kayıt, eyleme geçirilebilir bağlam (tehdit puanlama, coğrafi konum, tehdit adları, tarih damgaları, virüslü web kaynaklarının çözülmüş IP adresleri, karmalar, popülerlik vb.) ile zenginleştirilmiştir.



Şekil 3. Kaspersky Tehdit Veri Akışları bağlamı

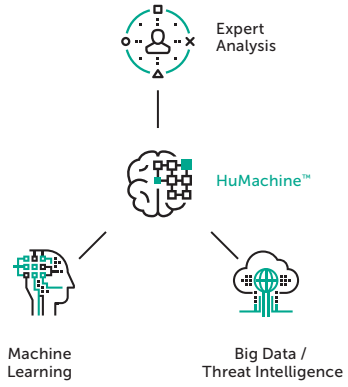
1 Entegrasyon 2019'da desteklenecektir

2 Entegrasyon 2019'da desteklenecektir

Bu bağlamsal veriler, verinin çeşitli kullanım alanlarını geçerli hale getirerek ve destekleyerek "büyük resmin" açığa çıkmasına yardımcı olur. Veriler bağlam içinde değerlendirildiğinde kim, ne, nerede, ne zaman sorularını daha kolay cevaplamak için kullanılabilir. Bu soruların cevapları düşmanlarınızı tanımlamanızı sağlayarak doğru kararlar almanıza yardımcı olabilir.

Kaspersky CyberTrace ve Kaspersky Tehdit Veri Akışları ayrı kullanılabilir; ancak birlikte kullanıldıklarında tehdit tespit yeteneklerinizi önemli ölçüde güçlendirirler ve güvenlik operasyonlarınızı siber tehditlere karşı global görünürlük sayesinde güçlendirir. Kaspersky CyberTrace ve Kaspersky Tehdit Veri Akışları ile, Güvenlik Operasyonları Merkezi analistleri şunları yapabilir:

- Sayısız güvenlik uyarısını etkili bir şekilde ayrıştırmak ve önceliklendirmek
- Öncelik belirleme ve öncül yanıt süreçlerini geliştirmek ve hızlandırmak
- Kuruluş için önemli uyarıları hemen tanımlamak ve hangi durumlarda Olay Müdahale ekiplerine yöneltilmesi gerektiği hakkında daha bilinçli kararlar vermek
- İleriye dönük ve istihbarat odaklı bir savunma oluşturun.



Kaspersky Lab
Kurumsal Siber Güvenlik: **www.kaspersky.com.tr/enterprise**
Siber Tehdit Haberleri: **www.securelist.com**
BT Güvenliğiyle İlgili Haberler: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com.tr