Saldırganlara karşı nasıl savunma yapacağınızı bilin. Kuruluşunuzun gerçek tehdit alanını ortaya çıkarın

Tehdit Ortamı Kaspersky Threat Intelligence Portal'da

kaspersky geleceği yakalayın

Kaspersky Threat Intelligence Portal

Kaspersky Threat Intelligence Portal'da kurumunuz için Tehdit Ortamı

Küresel tehdit alanı sürekli olarak gelişmekte, her gün yeni saldırı yöntemleri ortaya çıkmakta ve bilinen yöntemler daha karmaşık hale gelmektedir. Günümüzde, bilgi güvenliği ekiplerinin hızlı bir şekilde yanıt verilmesi gereken tehditleri etkili bir şekilde önceliklendirebilmeleri giderek daha önemli hale gelmektedir. Ancak işletmeniz, sektörünüz ve bölgenizle en alakalı tehditlere nasıl odaklanabilirsiniz?

Kaspersky Threat Intelligence Portal

Kullanıcılar, belirli bir sektörü ve bölgeyi hedef alan saldırganlar hakkında bilgi sağlamak için özel olarak tasarlanan ve algılama teknolojilerini küresel tehdit istihbaratıyla birleştiren Tehdit Alanı bölümünde tehdit ortamlarını değerlendirmek için eşsiz bir fırsata sahiptir. Bu, potansiyel düşmanlarınızla ilişkili tehditler, onların taktikleri, teknikleri ve prosedürleri (TTP'ler) hakkında eksiksiz ve güncel bir bağlam sağlar.

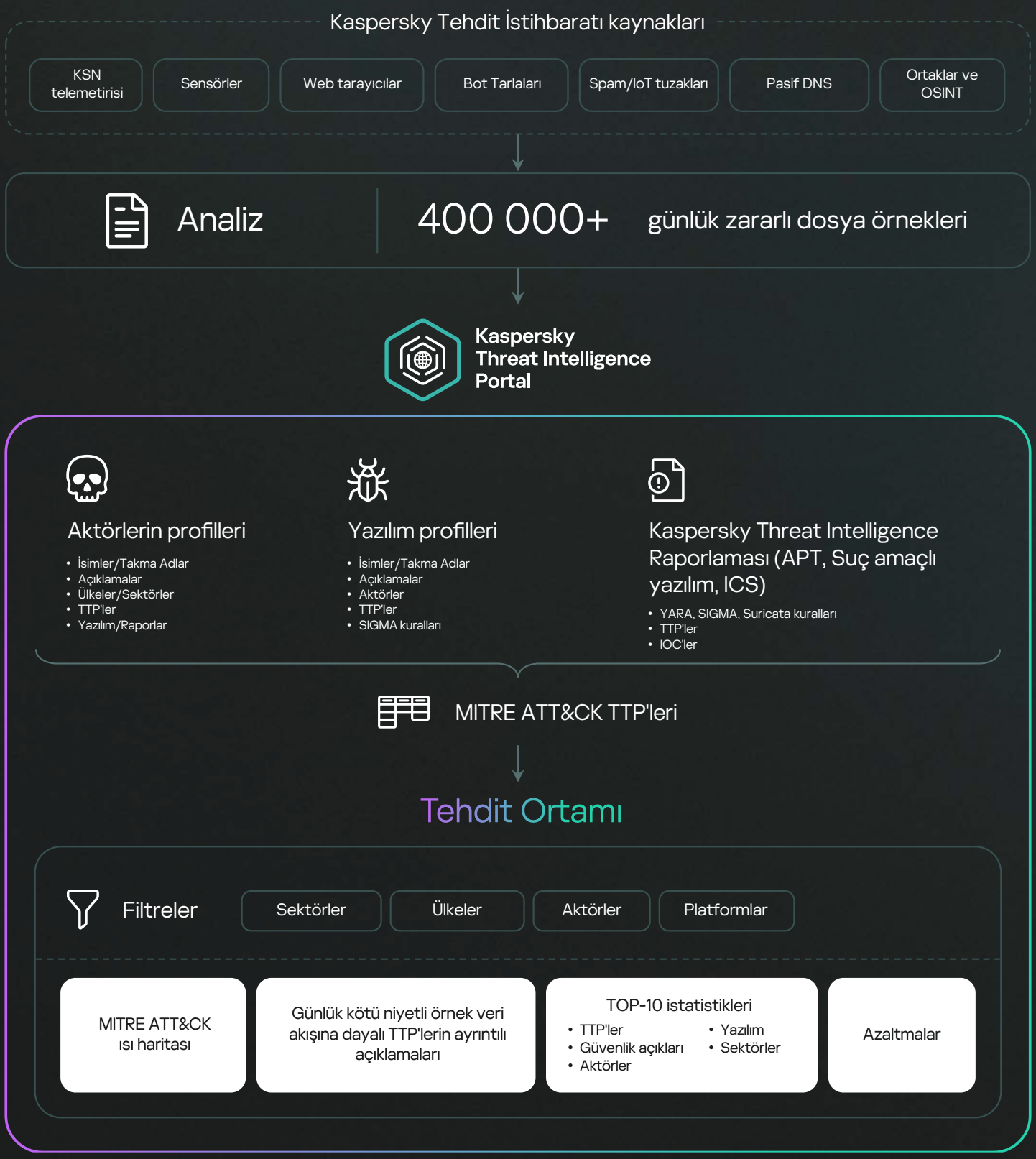
Tehdit Alanı, aşağıdakilerle ilişkili tehditler hakkında bilgi sağlar:

- coğrafya
- endüstri
- tehdit türleri
- tehdit aktörleri
- teknikleri, taktikleri ve prosedürleri (TTP'ler)
- kullandıkları kötü amaçlı yazılımlar
- ilgili güvenlik ihlali göstergeleri (IoC'ler)

Tehdit istihbaratı verileri, Kaspersky'nin 25 yılı aşkın süredir siber suçlarla mücadele etmek için kullandığı çeşitli uzman sistemler kullanılarak gerçek zamanlı olarak toplanıyor. Bunlardan biri olan Kaspersky Security Network, dünya çapında milyonlarca kullanıcıdan anonim veriler alır ve her gün milyonlarca dosyayı, web tarayıcılarını, bot çiftliklerini, spam tuzaklarını, sanal sunucuları, sensörleri, pasif DNS'leri, açık ve karanlık web kaynaklarını ve iş ortaklarını otomatik olarak işler. Bu verileri son çeyrek yüzyıldır kendimiz kullanıyoruz ve bağımsız testlerde ve harici incelemelerde en yüksek puanları alıyoruz. Elde edilen veriler Kaspersky tehdit araştırma ekipleri tarafından dikkatle analiz edilir ve korumalı alanlar, sezgisel motorlar ve benzerlik araçları gibi modern otomatik sistemler tarafından işlenerek garantili, doğrulanmış ve güncel bilgilere dönüştürülür.

Daha fazla bilgi edinin

Nasıl çalışır?

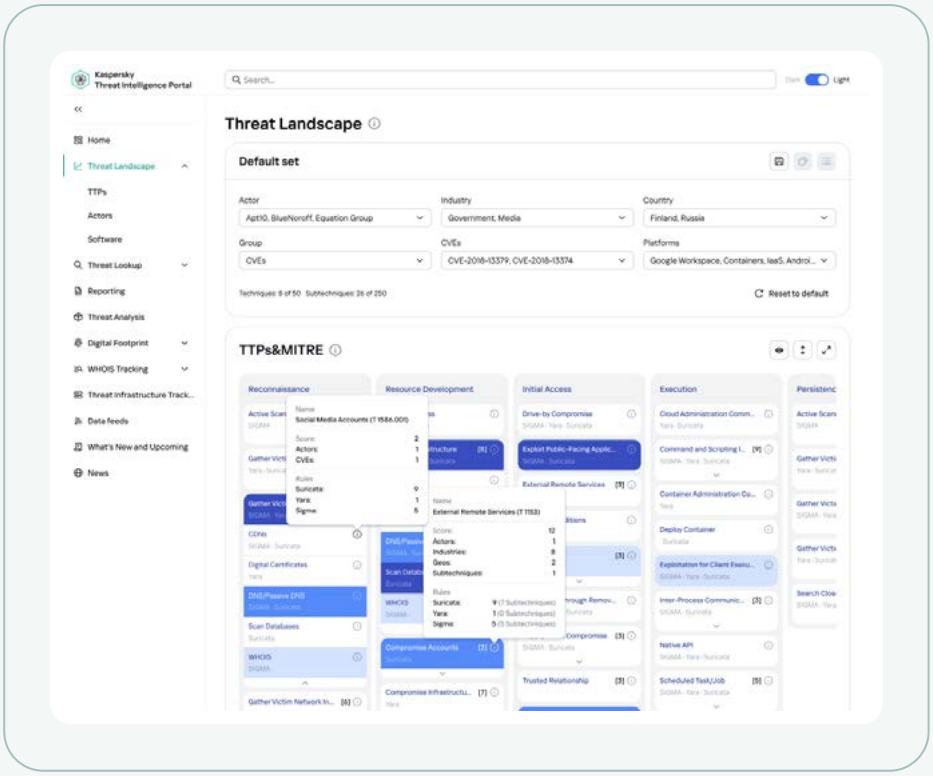


Her gün yüz binlerce kötü amaçlı dosya örneğini işleyerek coğrafi konum ve sektör verilerini çıkarırız, ardından Kaspersky dahili sistemleri ilişkili TTP'leri çıkarır ve dosyaları zaten bilinen siber suç grupları ve kötü amaçlı yazılımlarla ilişkilendirir. Tehdit Alanı bölümü de uzman araştırma ekiplerimizden aldığımız ve dünyanın dört bir yanından gelen gerçek olay verilerine dayanmaktadır.

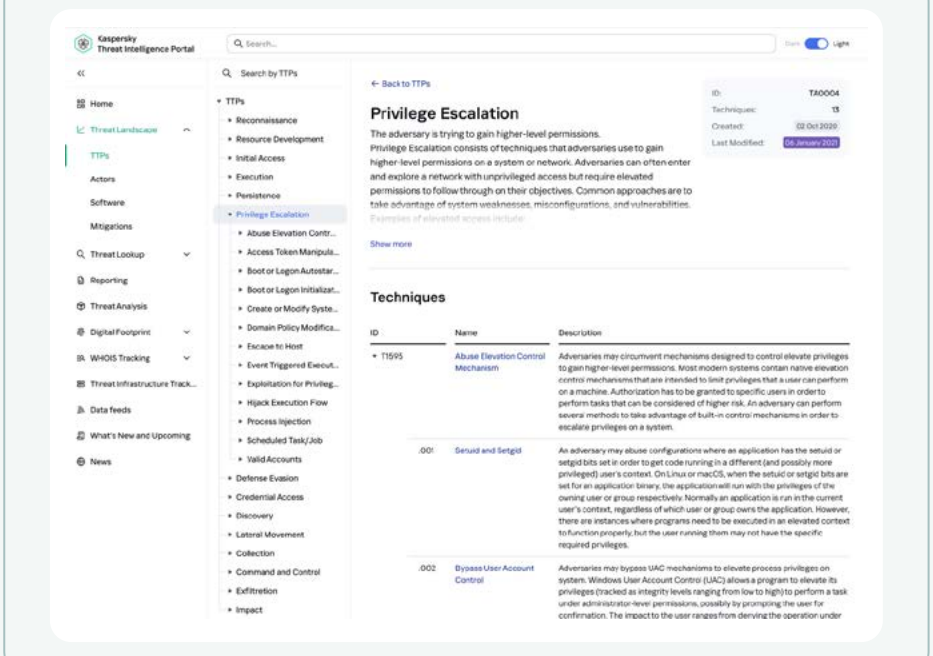
Filtreleri uygulayan Kaspersky Threat Intelligence Portal kullanıcıları, potansiyel düşmanları hakkında, MITRE ATT&CK çerçevesine uygun olarak en güncel bilgileri elde eder ve kendi tehdit alanlarını oluşturabilirler. Saldırı için kullanılması en muhtemel teknikleri, taktikleri ve prosedürleri ve bununla birlikte aktörlerin, kötü amaçlı yazılımların ve kullandıkları TTP'lerin ayrıntılı açıklamaları, saldırıların ayrıntılı açıklamasını içeren raporları ve son olarak bir tekniğin başarılı bir şekilde uygulanmasını önlemek üzere kullanılabilecek belirli öneriler içeren azaltmaları elde ederler.

Öne Çıkan Noktalar

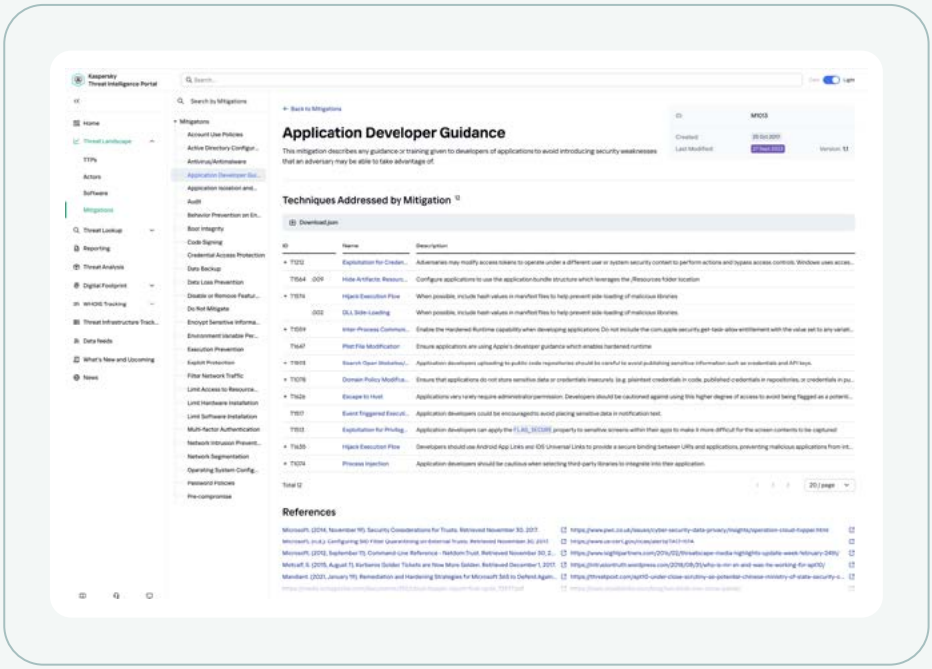
Kuruluşunuz için gerçek zamanlı olarak benzersiz bir tehdit alanı oluşturmak amacıyla MITTRE ATT&CK ısı haritası. Filtreleri uygulayarak kullanıcı, sistemlerimiz ve uzmanlarımız tarafından sürekli araştırma yoluyla elde edilen, son 24 saatteki güncellemeler de dâhil olmak üzere en güncel verilere erişebilir. Uluslararası kuruluşlar için katman kaydetme yeteneği.



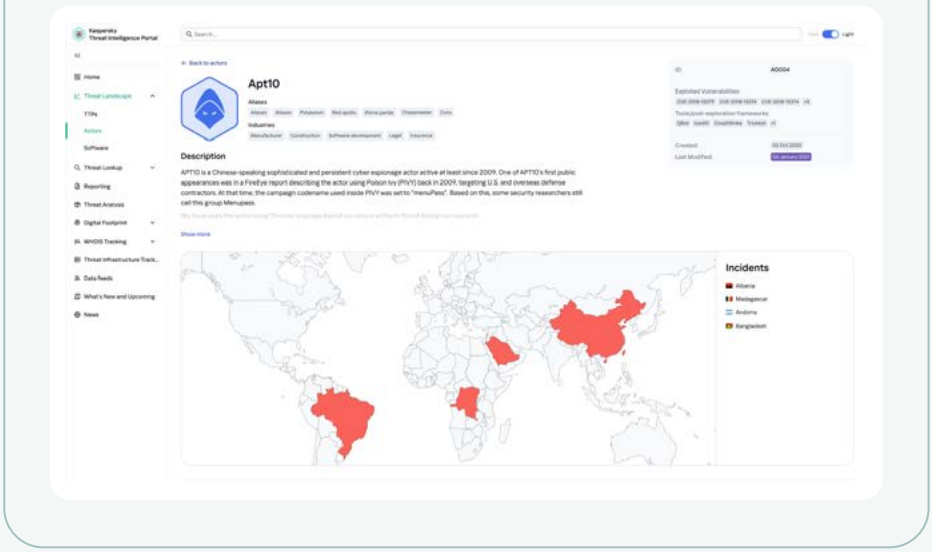
Kaspersky uzman sistemlerine dayalı olarak saldırganların teknikleri, taktikleri ve prosedürleri hakkında gerçek zamanlı canlı bilgiler.



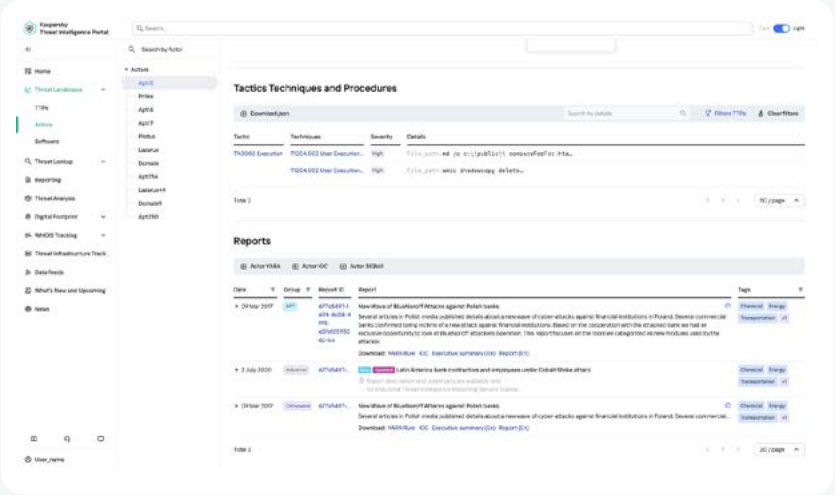
Azaltmalar bölümü, kuruluşların güvenlik açıklarından kaçınmaları için önleyici ve koruyucu tedbirlerin ayrıntılı açıklamalarını sağlar.



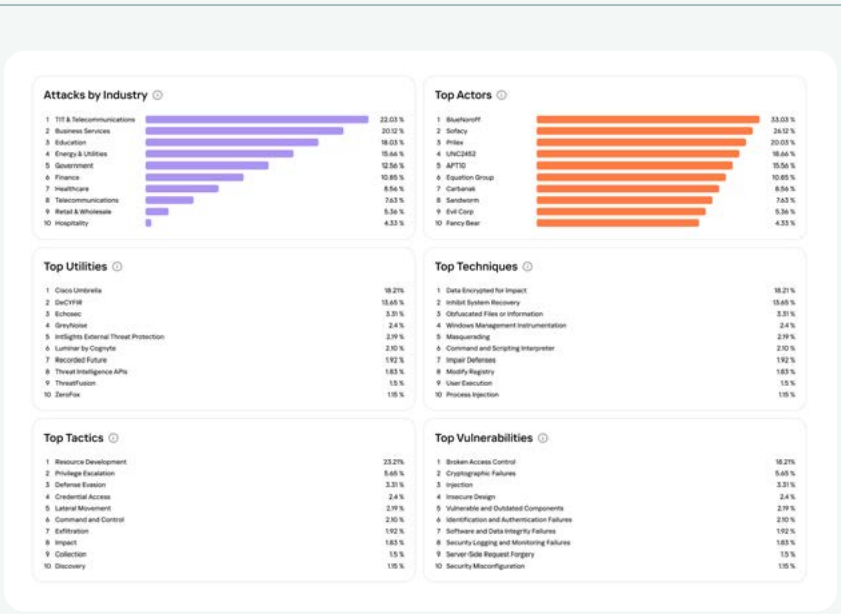
Kaspersky uzmanları tarafından derlenen ayrıntılı açıklamalarla sektörün en kapsamlı aktör ve kötü amaçlı yazılım profilleri havuzuna erişim.



Kuruluşunuzla ilgili tehditleri tespit etmek için MITRE ATT&CK teknikleri, taktikleri ve prosedürleri ile ilgili Sigma/Yara/Suricata kurallarına erişim.



Sektörler, aktörler, TTP'ler, güvenlik açıkları ve yazılımlar hakkında TOP-10 istatistikleri.



Günümüzde siber tehditlerin sürekli gelişen dünyası, çeşitli ürün ve hizmetler aracılığıyla erişilebilen çok sayıda Tehdit İstihbaratı verisi içermektedir. Kuruluşlar kendi tehdit ortamlarını anlayarak, ilgili saldırılara karşı proaktif bir şekilde savunmak için stratejik olarak makul adımlar atabilirler.

Kullanım faydaları

Proaktif savunma yaklaşımı

Etkili bir savunma stratejisi oluşturmak için kurum için en olası saldırı vektörlerinin anlaşılması

Saldırı yüzeyi izleme

Güvenlik açıklarının saldırganlar tarafından istismar edilmeden önce tespit edilmesi

İlgili tehditlere odaklanılması

İşletmenizi, sektörünüzü ve bölgenizi etkileme olasılığı en yüksek olan tehditlere odaklanabilme becerisi

Stratejik planlama

Yatırımların planlanması ve koruma araçlarının/yöntemlerinin geliştirilmesi için tehdit ortamı bilgilerinin kullanılması

Bilgi güvenliği departmanlarının verimliliğinin artırılması

İlgili tehditler ve küresel trendler hakkındaki bilgilere erişim yoluyla personel verimliliğinin artırılması ve personel maliyetlerinin azaltılması

Tehdit farkındalığı

Etkin savunma için en son tehditler ve bunların küresel eğilimleri hakkında farkındalık

Düşmanı ve kendinizi tanırsanız yüz savaşın sonucundan korkmanıza gerek kalmaz. Kendinizi tanır ama düşmanınızı tanımazsanız kazandığınız her bir zafer için bir de yenilgiye uğrarsınız. Eğer ne düşmanı ne de kendinizi tanıyorsanız her savaşta yenik düşersiniz.

Sun Tzu

Savaş Sanatı eserinden

Kaspersky Tehdit İstihbaratı

Kaspersky Threat Intelligence, birinci sınıf analistlerimiz ve araştırmacılarımız tarafından toplanan çeşitli bilgilere erişim sağlar. Bu veriler, her kuruluşun 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. Bu, Kaspersky'yi Interpol ve çeşitli CERT birimleri de dâhil olmak üzere dünyanın dört bir yanındaki kolluk kuvvetleri ve devlet kuruluşlarının güvenilir bir ortağı haline getirdi. Kaspersky Tehdit İstihbaratı güncel taktiksel, operasyonel ve stratejik tehdit istihbaratı sağlar.

Kaspersky Threat Intelligence

Daha fazla bilgi edinin

www.kaspersky.com.tr

© 2024 AO Kaspersky Lab.
Tescilli ticari markalar ve hizmet markaları, ilgili sahiplerine aittir.

#kaspersky
#geleceğiyakalayın