# Karmaşıklıkla mücadele edin

Modern sofistike tehditlerin sebep olduğu karmaşık siber olaylarla başa çıkmanın yolları

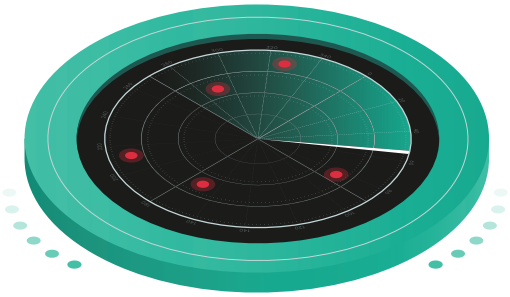
kaspersky GELECEĞİ YAKALAYIN

Bir tehdidi her zaman güvenlik çeperine girmeden önce durdurmak mümkün olmayabilir, ancak saldırının yayılmasını önlemek ve yol açabileceği hasarı sınırlandırmak veya saf dışı bırakmak kesinlikle mümkün. Konu karmaşık veya hedefli saldırılar olduğunda olay çözümleme hızı kritik önem taşıyor.

Bununla birlikte karmaşık olayların kendine has zorlukları var, çünkü saldırı altındaki işletmenin altyapısına ilişkin pek çok unsuru ilgilendiriyorlar. Bu bir anlamda bir ikilem doğuruyor: Her şey en az diğeri kadar önemliyken nereden başlayacağımızı nasıl bileceğiz?

Bu bültende başarılı bir karmaşık olay çözümlemenin önündeki beş önemli engeli ele alacağız. Ancak öncelikle, karmaşıklık kavramının kendisini ve siber güvenlik uzmanları için anlamını sorgulayarak başlayalım.

## Karmaşık bir olay tam olarak nedir?



Karmaşık olay, basit bir olayla karşılaştırılarak daha net bir şekilde tanımlanabilir. Küresel Covid-19 salgınının da ülkeler, kuruluşlar (devletler ve işletmeler), topluluklar, okullar, sektörler, aileler ve bireyler gibi çoklu sistemleri ilgilendiren, tam anlamıyla bir karmaşık olay olduğunu belirtmeden geçmemek lazım. Virüs, hastalanan insanların vücutlarında karmaşık bir olay olarak hareket ediyor; etkileri solunum sistemini aşarak kardiyovasküler, renal, dermatolojik, nörolojik, immün ve hatta psikiyatrik sistemlere kadar uzanıyor.

## Karmaşık siber uzay, karmaşık tehdit ortamı, karmaşık siber olaylar... Doğal bir ilerleme mi?

Siber olayların karmaşıklığının artması, BT sistemlerinin ve bizzat siber uzayın karmaşıklığının artmasıyla doğrudan bağlantılı. Hatta ENISA'nın (Avrupa Birliği Siber Güvenlik Ajansı) *Ortaya Çıkan Trendler Ocak 2019'dan Nisan 2020'ye Tehdit Ortamı Raporu'na göre,* "Çeşitli sistemlerin ve ağların birbirine bağlı olması, siber olayların daha hızlı ve daha geniş alanlara yayılmasına olanak sağlayarak siber riskleri değerlendirmeyi ve hafifletmeyi zorlaştırıyor." Diğer bir deyişle, BT altyapısı karmaşıklaştıkça, karmaşık saldırı riskine daha açık hale geliyor; bu da büyük ve doğal olarak karmaşık kuruluş düzeyinde işletmeler için karmaşık olay sorununun daha da şiddetli olmasına yol açıyor.

Bununla birlikte karmaşık ortamlar ve karmaşık olaylar arasındaki korelasyon, spesifik kurumsal sistemlerin de ötesine uzanıyor. Siber uzay, ISO/IEC 27032:2012'de "insanların, yazılımların ve hizmetlerin internete bağlı teknolojik araçlar ve ağlar aracılığıyla kurduğu etkileşim sonucu ortaya çıkan, fiziksel formda bulunmayan karmaşık ortam" anlamına geliyor. Diğer bir deyişle, karşımızda üç karmaşıklık katmanı var: Siber uzay, kuruluşun BT ortamı ve siber olaylar.

Bu üç katmanın birbirine bağlı ve bağımlı olması, bu ortamı daha da karışık hale getiriyor. Üstelik her biri kendi hedeflerine ulaşmak için giderek karmaşıklaşıyor.

**Siber uzay**: Günlük iş ve eğlence yaşamını destekleyebilmek için birbirine bağlı araçlara, sistemlere ve süreçlere gitgide daha fazla ihtiyaç duyması, ortamın giderek daha karmaşıklaşmasına yol açıyor.

**Kurumsal BT ortamı**: Saldırı yüzeyinin, birbirine bağlı cihaz, sistem ve süreçlerin (tedarik zinciri de dahil) sayısındaki artış sonucu genişlemesine ek olarak, hem siber olayların hem de bu olaylardan korunmak için gereken siber güvenlik konfigürasyonlarının karmaşıklığının ciddi ölçüde artması ile karşı karşıya.

**Tehdit ortamı ve bu ortamdaki aktörler**: Bir yandan hem siber uzay hem de kurumsal ortamdaki karmaşıklığın artmasına yanıt veriyorlar, diğer yandan oldukça sofistike ve gelişmiş saldırılar düzenlemek için bu karmaşıklıktan özel olarak faydalanıyorlar (hedeflenen sistemlerin daha basit olduğu zamanlarda mümkün olmayan yanal hareketler gibi).

Acı gerçek şu ki, bu üçünün arasında karmaşıklık engelini aşmanın yollarını en hızlı bulanlar tehdit aktörleri. Bunu, diğer yöntemlerin yanında Hizmet Olarak Kötü Amaçlı Yazılım yöntemine başvurarak gerçekleştiriyorlar:

"Günümüzde siber suç işleyeceklerin önündeki engeller hızla ortadan kalkıyor, çünkü çeşitli araçlarla ve (Dark Web ve Deep Web gibi) kaynaklarla kötü amaçlı yazılımlara ve hizmet olarak kötü amaçlı yazılıma ulaşmak daha da kolaylaştığı için saldırganların elinde bir dizi (teknik) yetkinlik ve önemli kaynak var. Bunun sonucunda çok çeşitli gelişmiş teknik ve araç (ör. sosyal mühendislik teknikleri ve sıfır gün güvenlik açıkları) gelişmiş hedefli saldırılar gerçekleştirmek için siber suçlular tarafından kullanılabiliyor.

Papastergiou, S., Mouratidis, H. & Kalogeraki, EM. **Handling of advanced persistent threats and complex incidents in healthcare, transportation and energy ICT infrastructures.** Evolving Systems (2020).

İyi haber: Kuruluşların karmaşıklık engelini etkin ve kararlı bir biçimde önemli ölçüde aşabilecekleri yollar var. Bu yazıda da ayrıntılı olarak bunu inceleyeceğiz. Bunu yapmadan önce, başarılı bir karmaşık olay çözümlemenin önündeki beş önemli engeli ele alacağız.

## Başarılı olay çözümlemenin önündeki beş engel

Kurumsal çepere girdikten sonra dahi karmaşık tehditlerin ilerlemesini durdurmanın ve yol açabilecekleri hasarı sınırlandırmanın mümkün olduğunu biliyoruz. İlk olarak MITRE ATT&CK kurumsal çerçevesindeki İlk Erişim taktiklerinin çoğunun hala görece geleneksel olduğunu hatırlamakta fayda var.

Hedef odaklı kimlik avının APT'ler için bile hala başlıca İlk Erişim taktiklerinden biri olması, global pandemi kaosu bağlamında bizi düşündürmeli. Öncelikle ilk erişimi engelleyen rutin siber güvenlik görevlerini otomatize ederek kaç saldırının önlenebileceğini göz önünde bulundurmalıyız. Bununla birlikte bu durum, bir olayı *karmaşık* yapan şeyin, erişim girişi olmadığının da altını çiziyor (sıfır gün güvenlik açıkları gibi istisnalar hariç).

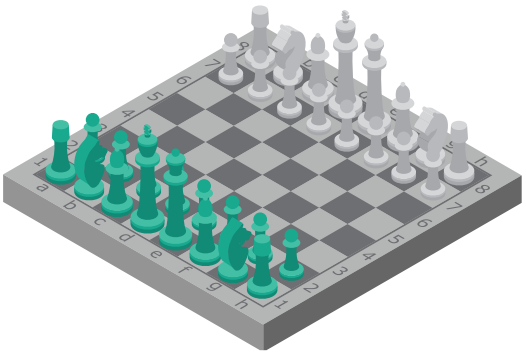
Karmaşıklık; yanal hareket, arka kapıların kurulması ve çeşitli yük teslimi ve gizlilik modları gibi taktiklerle başlıyor. Peki BT güvenliği ekiplerinin bir olayın karmaşık bir olay haline gelmesini önlemek üzere güçlerini ve uzmanlıklarını kullanmasını engelleyen ne? Karmaşık hale geldikten sonra olayı dindirmek ve başarıyla çözümlemek neden bu kadar zor?

# 1. Engel: Siber güvenlik sistemlerinin kendilerinin karmaşık olması

Dışarıdan bakan biri için ortalama bir kurumsal siber güvenlik konfigürasyonu, hayalet savaş uçaklarının kokpiti kadar kafa karıştırıcı olabilir. Öte yandan elbette ortalama bir kuruluş veya ortalama bir siber güvenlik konfigürasyonu diye bir şeyden de bahsedemeyiz. Çoklu araçlar, yüksek uzmanlık gerektiren spesifik güvenlik görevleri, bir dizi kontrol konsolu ve ardı arkası kesilmeyen alarmlar... Bu karmaşıklığın nasıl ortaya çıktığından bahsetmiştik: Bir yandan kurumsal BT güvenliği altyapısının, diğer yandan tehdit ortamının artan karmaşıklığına karşılık gelişti.

Bu yüzden siber güvenlik konfigürasyonlarındaki karmaşanın, üstesinden gelmesi gereken karmaşık olayları başarıyla çözümlemenin önünde bizzat engel oluşturması aslında ironik bir trajedi. Bu karmaşa şu sebeplerle başarılı sorun giderme ve olay çözümlemeye ket vuruyor:

- Araçlar içinde boğulan ekipler, çok değerli zamanlarını ayrı çözümler arasında 'çevirmenlik' yaparak harcıyor. Siber güvenlik teknolojisi yığınları (ve genel olarak tüm teknoloji yığınları) çoğunlukla sanal Babil Kulelerine dönüşüyor ve farklı araçların farklı 'diller' konuşması, kesintisiz ve sorunsuz bir operasyona engel oluyor.
- Siber olay verileri, potansiyel giriş noktalarında yer alan entegre olmayan çeşitli veri sensörlerinden küçük örneklemler halinde toplandığında ekipler çoğunlukla büyük resmi gözden kaçırıyor ve bu yüzden belirgin bir giriş işareti ortaya çıkmadan önce karmaşık bir olayın gelişmekte olduğunu fark edemiyorlar. Diğer bir deyişle, olay tam olarak anlaşılamıyor; bu da nihayetinde zarara yol açıyor.
- Sistematik ve tutarlı olmayan olay müdahalesi sürecinde alarmlarla uğraşmaktan kaynaklanan sürekli manuel işlem ihtiyacı, değerli enerjiyi tüketiyor; hayati önem taşıyan alarmların atlanmasına ve yanlış pozitiflere çok fazla dikkat verilmesine neden oluyor.



# 2. Engel: Zayıf ya da geçersiz tehdit istihbaratı

Tehdit İstihbaratı, işletmenizi hedef alan siber tehditlere yönelik derinlemesine görünürlük vaadini yerine getirebilmek için üç aşamalı bir testi geçebilmeli:

Kapsamlı mı?

Doğru mu?

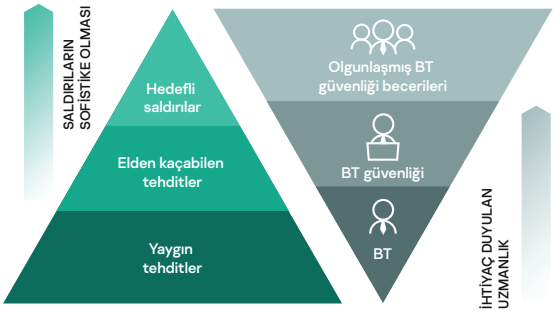
Güncel mi?

Bununla birlikte, bu testi geçmek yalnızca ilk adım. Günümüzde çok sayıda kuruluş düzeyinde işletmenin karşılaştığı engel, kapsamlı, doğru ve güncel tehdit istihbaratına sahip olsalar bile çok önemli bir noktanın eksik kalması: Geçerlilik. Günümüzün tehdit istihbaratı akışlarına aşina olan her BT güvenliği uzmanı bunun zaten farkındadır.

Geçerlilik, niteliğin nicelikten daha önemli olduğunu ifade etmenin bir yolu olabilir, ancak bu yalnızca kısmen doğru. Tehdit istihbaratı her ikisini de sunan ve özel olarak o işletme için, o anda, o ortamda geçerli olan istihbaratla bütüncül bir siber güvenlik sistemince kanalize edilmeli veya işlenmelidir. Geçerlilik tek seferlik bir uğraş değildir; siber güvenlik konfigürasyonunda yer alan entegre unsurlar arasındaki geri bildirim döngüsünü ilgilendiren devamlı bir süreçtir.

Diğer tespit ve tehdit avı mekanizmalarına entegre olan bağlamsal açıdan geçerli tehdit istihbaratı, anlamı ve bağlamı otomatik olarak bulur ve en baştan netlik sağlayarak değerli zamanı boşa harcamaz.

# 3. Engel: Basit yaygın tehditlere gereğinden fazla odaklanma alışkanlığı

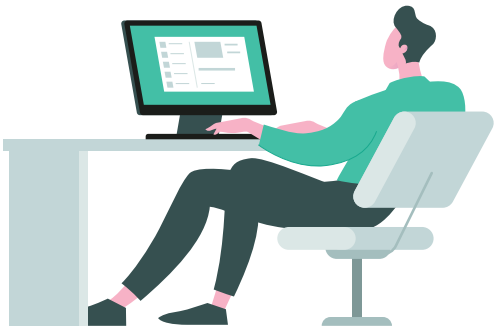



Basit yaygın tehditler hala işletmelerin karşılaştığı tehditlerin büyük bir yüzdesini oluşturuyor. Bu anlamda, BT güvenliği açısından olgunlaşmış büyük işletmelerde bile bu tür tehditlere gereğinden fazla odaklanma eğilimi görülmesi çok şaşırtıcı değil.

Ancak, bu tehditlerle ilgili olayların maliyetleri, hedefli saldırılar ve APT saldırıları gibi yıkıcı karmaşık saldırıları içeren geri kalan yüzdelik kesimin yol açabileceği zararla kıyaslandığında gözardı edilebilir.

Bazı BT güvenliği ekiplerinin hala basit tehditlere gereğinden fazla (karmaşık olaylar pahasına) odaklanmasının diğer sebebi ise daha açık. Çözülmesi kolay, karmaşık olmayan bir soruna odaklanma isteği, insanlar için çok doğal. Dahası, basit tehditlerin bu kadar karmaşıklıktan uzak olma sebebi, en basit, en zayıf yapılandırılmış siber güvenik konfigürasyonlarının bile bunları otomatik olarak gayet iyi tespit edebilmelerine karşın iş çözümlemeye geldiğinde yeterince otomasyon sunamaması. Bu yüzden basit tehditler çok fazla alan kaplayarak çok daha ölümcül sonuçlar doğurabilecek karmaşık olaylara odaklanamamak pahasına gerekmeyen ölçüde dikkat isteyebilir.

# 4. Engel: Siber güvenlik uzmanlığı krizi



ABD Ulusal Siber Güvenlik Eğitimi Girişimi (NICE) tarafından başlatılan bir girişim olan Cyberseek Heat Map haritasına hızlıca göz gezdirdiğimizde siber güvenlik uzmanlığı krizinin boyutları ortaya çıkıyor. Cyberseek yalnızca Amerika'yla ilgilense de global yetersizlik hakkında da oldukça işe yarar (ve çarpıcı) bir bakış sunuyor.

30 Ocak 2021 itibariyle ABD'de siber güvenlik iş gücünde yer alan 941.904 kişiye karşılık 521.617 siber güvenlik uzmanı aranıyor. Arz-talep oranı ortalaması ulusal olarak 1,8.

Bu, iş güvenliği açısından siber güvenlik uzmanları için iyi bir haber (ve lise çağındaki çocuklarınızı bu tür bir kariyere teşvik etmek için iyi bir zaman) olsa da, iş yaşamının niteliği ve verimlilik açısından hiç de iyi bir haber değil.

Analistlerin çoğu, siber güvenlik uzmanlığı krizinin eğitimdeki yanlışlardan kaynaklandığı sonucuna varıyor, ancak bu içgörünün krizin ortasındaki işletmelere bir yardımı dokunmuyor. Bu yanlışlar (kısmen Cyberseek gibi girişimler tarafından) ele alınıp düzeltilene kadar işletmelerin mevcut BT ekiplerinin gücünü maksimize ederek ve karmaşık olayları başarıyla çözümlemek için ihtiyaç duydukları araçları, desteği, rehberliği ve yardımı onlara sağlayarak bu engelle başa çıkmaları gerekiyor.

# 5. Engel: Hız sorunu

Karmaşık olayları başarıyla çözümlemenin önündeki son engel, ilk dört engeli birbirine bağlıyor. Sıfır gün güvenlik ihlalleri, kötü amaçlı yazılım içermeyen saldırılar, dosyasız saldırılar ve "living-off-the-land" saldırıları gibi karmaşık zorluklar karşısında hız her şey demek.

Hedef odaklı kimlik avının bir ilk erişim kazanma taktiği olarak yaygınlığı meselesinde gördüğümüz gibi, karmaşık bir olay illa karmaşık bir şekilde başlamıyor. Ekip yeterince hızlı davranabilse yıkıcı (ve pahalı) sonuçları önlenebilecek olan çok sayıda karmaşık olay var.

Bu elbette karmaşık bir olayın gelişimi sırasında 'her şey için çok geç' olan bir noktaya varılacağı anlamına gelmiyor; yalnızca zaman ilerledikçe karmaşıklık düzeyi de ilerliyor. Konu karmaşık olaylar olduğunda hızın her şey olduğunu söylemek kulağa basit gelebilir. Ancak hızla neyi kastettiğimiz dikkate alındığında bu önerme kesinlikle doğru.

Hız, durmaksızın yangın söndürmek ya da en ufak şeyden tetiklenip dikkatimizi talep eden her alarma çabucak yanıt vermek demek değil. Tüm olmazsa olmaz tespit ve yanıt süreçlerini kararlı ve istikrarlı biçimde doğru olarak yürütmenin hızı demek. Buna proaktif tehdit avı, kök neden analizi ve geriye dönük analiz, düzeltme, hasar giderme ve olay müdahalesi de dahil.

## Karmaşık olaylarla karşı karşıya olan işletmeleri gelecekte neler bekliyor?

2021 yılının başı, gelecekle ilgili herhangi bir soruya yanıt aramak için en kötü zaman gibi görünüyor. Ne de olsa pandemi, araçlarımızı, sistemlerimizi ve uzmanlarımızı hazırlıksız yakalayan başlı başına karmaşık bir olay. Ancak yine de kesin olarak bildiğimiz bazı şeyler var. Örneğin, APT'lerin ve diğer karmaşık saldırıların gelişmeye devam edeceğini ve **uzaktan çalışmanın pandemiden sonra bile büyük olasılıkla yükselmeyi sürdüreceğini** biliyoruz. Dünya lideri siber güvenlik araştırmacılarından oluşan Global Araştırma ve Analiz Ekibimiz (GReAT), 2021'de APT'ler hakkında şu **öngörülerde bulunuyor:**

- Sahte bayrak saldırıları (Olympic Destroyer gibi) yeni bir seviyeye ulaşacak
- Fidye yazılımlar gitgide daha hedefli hale gelecek
- Yeni çevrimiçi bankacılık ve ödeme vektörleri ortaya çıkacak
- Daha fazla altyapı saldırısı ve bilgisayar olmayan hedeflere yönelik saldırı
- Asya ve Avrupa arasındaki ticaret yolları etrafında artan saldırılar
- Saldırı yöntemlerinin daha sofistike hale gelmesi
- Mobil saldırılara daha fazla odaklanma
- Deepfake'lerden DNA sızıntılarına kadar kişisel bilgilerin kötüye kullanımı

BT güvenliği uzmanlarını bu tür karmaşık olayların beklemesi dünyanın sonu anlamına gelmiyor.

ENISA'nın Ocak 2019-Nisan 2020 Araştırma Konuları raporuna dönersek karmaşık olayları başarıyla çözme arayışı ile ilgili bir umut ışığı olduğunu ve çalışmalarımızın odağına almamız gereken noktayı görüyoruz: İnsan boyutu.

*"Siber güvenlik hala ağları, bilgi sistemlerini ve verileri (NIS) koruma pratiği olarak algılanıyor. Bu tanımın sosyolojik, davranışsal ve ekonomik kaygıları ve işin içinde yer alan tarafların oynadığı rolleri de içerecek şekilde genişletilmesi gerekiyor. Bundan sonraki siber güvenlik araştırmalarında ve inovasyon tartışmalarında bu bir öncelik olmalı. İnsanın ihtiyaçlarına, becerilerine ve beklentilerine uygun güvenlik kararlarının alınabilmesi için işin insan boyutunu daha iyi anlamak, tüm siber güvenlik stratejisi tanımları için büyük önem taşıyor."*

Bizim meselemizle ilgili olarak, yukarıda bahsedilen 'taraflar', BT güvenliği uzmanlarına ve sorumluluk taşıdıkları işletme yöneticilerine işaret ediyor. İhtiyacımız olan tüm siber güvenlik uzmanlarını işe alamayabiliriz. O halde soru, elimizdekileri nasıl geliştirebiliriz?

## Uzman teknoloji, uzman ellerde

Atılacak ilk adım, BT açısından en üst düzeyde olgunluğa erişmiş işletmelerin bile karmaşık tehditleri ve APT saldırılarını alt etmesinin beklenmediğini anlamak. Bu, bölgeler ve sektörler arasında sürekli yer değiştiren global bir problem ve bu yazıda bahsettiğimiz engeller, karmaşık olayları başarıyla çözümle gayretlerinde birçok ekibin yoluna taş koyuyor.

Bu yüzden tüm kurumsal müşterilerimizi tüm başarılı karmaşık olay stratejilerinin üç ayağı olarak gördüğümüz üç noktaya gereken özeni göstermeye teşvik ediyoruz. Güvenlik ekipleri şu özelliklere sahip olmalı:

- **Donanımlı:** Siber güvenlik, beceri sahibi bir çalışanın bile haklı olarak araçlarını suçlayabileceği bir uzmanlık alanıdır. Çok vektörlü saldırılara ve diğer karmaşık olaylara karşı korunma, eksiksiz görünürlük sağlayarak engelleyici siloları yok eden, 'alarm yorgunluğunu' önleyen ve olay müdahalesi sürecindeki diğer rutin görevleri ortadan kaldıran birleştirilmiş bir platform gerektirir.

- **Bilgi sahibi:** BT olgunluğuna erişmiş işletmeler, mevcut ileri uzmanlık düzeylerinin onları hep idare edeceği yanılgısına asla düşmemelidir. Siber suç ortamının durmaksızın değiştiği ve geliştiği unutulmamalıdır. Güvenilir bir siber güvenlik ortağından alınan sürekli eğitim ve güçlü tehdit istihbaratı hayati önem taşır.

- **Güçlendirilmiş:** Karmaşık bir olay ya da APT keşfedilmesi durumunda, en ileri düzeydeki BT güvenliği analistleri bile üçüncü taraf görüşü, yönetilen tehdit avı ve olay müdahalesi için dışarıdan desteğe erişebilmelidir. APT'lerden kaynaklanan karmaşık olaylar çoğunlukla oldukça hedefli olsa da nadiren tek bir kurbanı hedeflerler. Dışarıdan alınan uzmanlık, bir APT'nin izleyebileceği yola birçok sektörden global bir ışık tutar ve sistemden elimine etmenin en kesin yolu hakkında eyleme dökülebilir öneriler sunar.

## BT güvenliği uzmanlarınızın karmaşık olayları kontrol etme biçiminde devrim yaratın

En karmaşık ve hedefli siber saldırılara karşı yürüttükleri mücadelede ekibinizi donatan, bilgilendiren ve rehberlik eden kapsamlı bir savunma konsepti olan Kaspersky Expert Security ile BT güvenliği uzmanlarınızın karmaşık olayları kontrol etme biçiminde devrim yaratın. Siber güvenlik dehalarının desteğini arkasına alan Kaspersky Expert Security, endüstri lideri teknolojilerin, elit tehdit istihbaratının, insan uzmanlığının, eğitimin ve hizmetlerin kusursuz bir kombinasyonuna sahip olan bir Genişletilmiş Tespit ve Yanıt (XDR) platformu. Bütüncül yaklaşımımız, çok boyutlu tehdit keşfi, etkili araştırma ve proaktif tehdit avı konularında ekibinizin siber güvenlik gücünü arttırarak tüm modern tehdit çeşitlerine hızlı ve merkezi yanıt vermeyi sağlar

Daha fazla bilgi için go.kaspersky.com/expert

Siber Tehdit Haberleri: www.securelist.com
BT Güvenliği Haberleri: www.kaspersky.com/blog
Tehdit İstihbaratı Portalı: opentip.kaspersky.com
Bir bakışta teknolojiler: www.kaspersky.com/TechnoWiki
Ödüller ve takdirler: media.kaspersky.com/en/awards
İnteraktif Portföy Aracı: kaspersky.com/int_portfolio

**www.kaspersky.com.tr**

kaspersky GELECEĞİ YAKALAYIN