# Kaspersky Interactive Protection Simulation

Üst düzey yöneticiler ve karar vericiler arasında siber güvenlik farkındalığı oluşturmak

kaspersky bring on the future

**Daha fazla bilgi edinmek için**
kaspersky.com.tr/awareness
adresini ziyaret edin

# Kaspersky Interactive Protection Simulation

### "İnsan sorunu"

Günümüzde işletmelerin karşılaştığı en büyük güvenlik zorluklarından biri, farklı üst yönetim rollerinin siber güvenliğe farklı açılardan bakması ve farklı önceliklere sahip olmasıdır. Bu durum, karar verme aşamasında bir tür "Güvenlik Bermuda Üçgeni" yaratabilir:

- İşletmeler güvenlik önlemlerinin
- iş hedeflerine (daha ucuz/hızlı/daha iyi) aykırı olduğunu düşünüyor.
- BT Güvenlik Yöneticileri, siber güvenliğin bir altyapı ve yatırım sorunu olarak görev alanlarının dışında olduğu hissedebilir.
- Maliyet kontrolü ile görevlendirilen yöneticiler, siber güvenlik harcamalarının maliyet yaratmaktan ziyade gelirler ve tasarruflarla nasıl ilişkili olduğunu göremeyebilir.

Bu üçü arasındaki karşılıklı anlayış ve ortaklık, etkili bir siber güvenlik için çok önemlidir. Ancak dersler ve kırmızı/mavi alıştırmalar gibi geleneksel farkındalık biçimleri kusurludur: uzundur, aşırı tekniktir ve meşgul yöneticiler için uygun değildir ve bir "ortak dil" oluşturmada başarısız olurlar.

## Bir şirketin siber bağışıklığı üst yönetim ile başlar

Günümüzde pek çok şirket için BT altyapılarının sürdürülebilirliğini gözetmek bir önceliktir. Bununla birlikte, siber güvenlik sorunlarıyla ilgilenmek genellikle BT departmanının ve BT güvenlik personelinin sorumluluğundadır ve bu da işletme içinde parçalı bir siber güvenlik davranışı kültürü yaratabilir. İşletme liderleri öncelikle satışlara, müşteri deneyimine, risklere ve maliyetlere odaklanır ve hedeflerine ulaşmak için çalışırken genellikle siber güvenliği göz ardı ederler. Ancak yönetim kurulunun desteği olmadan, bir örnek oluşturacak birleşik bir siber güvenlik kültürü oluşturmak mümkün olmayabilir.

**CEO'ların %76'sı** bir işi daha hızlı yapmak için güvenlik protokollerini atladıklarını, hız için güvenliği feda ettiklerini itiraf ediyor*.

**Yöneticilerin %62'si** kurumlarında BT güvenliğine ilişkin iletişimsizliğin en az bir siber güvenlik olayına yol açtığını kabul ediyor**.

**Bilgi Güvenliği çalışanlarının %51'i** BT güvenliğine ayrılan bütçenin artırılması konusunda konuşmayı en zor konu olarak görüyor... ancak uygulanabilir iletişim stratejileri söz konusu olduğunda fikir ayrılığı olmadığını olduklarını belirtiyorlar.

C seviyesi (%56) **ve BT (%48)** çalışanlarının çoğunluğu, BT güvenliği ile ilgili konularda iletişimi kolaylaştırmak için gerçek hayattan örnekler sunmanın en etkili yöntem olduğu konusunda hemfikir**.

## Kaspersky Güvenlik Farkındalığı platformu nasıl yardımcı olur?

Kaspersky Güvenlik Farkındalığı, uzun süreli uluslararası başarı geçmişine sahip, kanıtlanmış, verimli ve etkili bir çözümdür. Her büyüklükteki işletme tarafından **75'ten fazla ülkede bir milyondan fazla çalışanı eğitmek için kullanılan çözüm**, Kaspersky'nin siber güvenlik alanındaki 25 yılı aşkın deneyimini Kaspersky Academy'nin yetişkin eğitimindeki kapsamlı deneyimiyle bir araya getiriyor.

Portföy, her seviyedeki çalışanlarınızın **siber güvenlik farkındalığını artıran** ve onları kuruluşunuzun genel siber güvenliğinde rol oynamaları adına güçlendiren ilgi çekici eğitim ürünlerinden oluşmaktadır.

Portföyde yer alan her ürün, genel öğrenme döngüsünde belirli bir rol oynar ve ayrıca bağımsız olarak da sunulur.

## Yöneticiler için bir stratejik siber güvenlik iş oyunu

**Kaspersky İnteraktif Koruma Simülasyonu (KIPS)**, iş verimliliği ve siber güvenlik arasındaki bağlantıyı gösteren bir takım oyunu olan stratejik bir iş simülasyonudur.

Katılımcılar, BT güvenlik ekibinin üyeleri olarak simüle edilmiş bir iş ortamına yerleştirilir ve burada şirketin sorunsuz çalışmasını ve gelir elde etmesini sağlama görevini yürütürken bir dizi beklenmedik siber tehditle karşı karşıya kalırlar.

Var olan en iyi proaktif ve reaktif kontroller arasından seçim yaparak bir siber savunma stratejisi oluşturmaları gerekir. Yaptıkları her seçim, senaryonun oynanma şeklini değiştirir ve sonuçta şirketin ne kadar gelir elde ettiğini veya etmediğini etkiler.

Mühendislik, iş ve güvenlik önceliklerini gerçekçi bir siber saldırının maliyetine karşı dengeleyen ekipler, verileri analiz eder ve belirsiz bilgilere ve sınırlı kaynaklara dayalı olarak stratejik kararlar alır. Kulağa gerçekçi geliyorsa, bunun nedeni tüm senaryoların gerçek hayattaki olaylara dayanmasıdır.

---

* https://www.forbes.com/sites/louiscolumbus/2020/05/29/cybersecuritys-greatest-insider-threat-is-in-the-c-suite/?sh=466624f87626

** https://www.kaspersky.com/blog/speak-fluent-infosec-2023/

KIPS, "yaparak öğrenme" yaklaşımına sahip dinamik bir farkındalık oyunudur:

- Eğlenceli, ilgi çekici ve hızlı (2 saat).
- Takım çalışması, iş birliğini geliştirir
- Rekabet, inisiyatif ve analiz becerilerini güçlendirir.
- Oyun oynama, siber güvenlik önlemlerine ilişkin bir anlayış geliştirir
- Tüm senaryolar ve saldırılar gerçek vakalara dayanmaktadır

# KIPS neden işe yarar?

KIPS eğitimi, işletme sistemi uzmanlarını, BT çalışanlarını ve bölüm yöneticilerini hedefler ve modern bilgisayarlı sistemleri çalıştırma ile ilgili riskleri ve güvenlik sorunları konusundaki farkındalıklarını artırır.

4-6 kişiden oluşan her takım, üretim tesislerini ve bunları kontrol eden bilgisayarları içeren bir işi yürütmekle görevlidir. Oyun sırasında üretim tesisleri gelir, kamuoyu farkındalığı ve iş sonuçları üretir. Takımlar aynı zamanda, işletmenin performansını etkilemekle tehdit eden siber saldırılarla da başa çıkmak zorundadır.

Oyunun sonunda oyuncular, işlerinde uygulayabilecekleri önemli ve eyleme geçirilebilir içgörüler kazanmış olacaklar.

- Siber saldırılar gelir kaybına neden olur ve üst yönetim tarafından dikkate alınmalıdır
- Her işletmede BT ve BT dışı karar vericiler arasında etkili siber güvenlik için işbirliği şarttır
- Uygun bir güvenlik bütçesi bankayı zarara uğratmaz, ancak başarılı bir siber saldırı bunu yapabilir...
- İnsanlar güvenlik kontrolleri ve bunların önemi (denetim eğitimi, anti-virüs, vb.) konusunda hızla rahatlar.

## KIPS iki şekilde sunulur:

Oldukça popüler olan **KIPS Canlı** seçeneği bir heyecan ve coşku atmosferi yaratır ve bir kurum içinde siber güvenlik kültürünün oluşturulması için harika bir araçtır.

**KIPS Çevrimiçi** versiyonunda, kullanıcılar kendileri için uygun olan konumlardan çok sayıda katılımcıyla etkileşime geçebilirler.

Küresel kuruluşlar veya halka açık etkinlikler için mükemmel olan KIPS Çevrimiçi, uzaktaki ekipleri sahadaki etkinliğe eklemek için KIPS Canlı ile birleştirilebilir.

- Herhangi bir konumdan aynı anda yaklaşık 300 takım (= 1000 katılımcı).
- Farklı takımlar, farklı dillerde oyun arayüzü seçebilirler.
- Müşteriler, kütüphaneden oyundaki saldırıların sayısını ve türlerini belirleyerek önceden yüklenmiş senaryoları kişiselleştirebilir.
- Lisans süresi boyunca istedikleri sıklıkta KIPS oynamalarına izin veren bir lisansa sahip olan müşteriler, önceden tanımlanmış ayarlarla oynayabilir veya kütüphaneden farklı saldırılar seçip birleştirerek oyun senaryosunu her oynadıklarında kişiselleştirebilirler. Bu işlevsellik oyunu her seferinde değiştirerek daha da ilginç hale getiriyor.
- Çevrimiçi versiyonun bir diğer avantajı da oyuncuların tercihlerine ilişkin istatistikler, takımların belirli durumlardaki eylemlerine ilişkin veriler ve bir önceki oyuna göre oyuncu eylemlerinin bir karşılaştırmasını alabilmektir.

KIPS şunları gösterir:

- Siber güvenliğin iş sürekliliği ve karlılıkta oynadığı rol.
- İşletmelerin karşılaştığı yeni zorluklar ve tehditler.
- Şirketlerin siber güvenlik politikalarını oluştururken yaptıkları tipik hatalar.
- İşletme ve güvenlik ekipleri arasındaki işbirliği, istikrarlı operasyonların sürdürülmesine ve siber tehditlere karşı sürekli koruma sağlanmasına nasıl yardımcı olur?

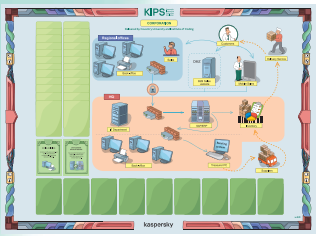
Senaryoya bağlı olarak takımlar, o sektördeki şirketin BT güvenliğinden sorumlu olur. Görevleri, şirketin normal ve kesintisiz işleyişini sağlamak, müşteriler ve tedarikçilerle ilişkileri sürdürmek ve siber tehditleri bulup etkisiz hale getirmektir.

İşletme siber saldırıya uğradıkça, oyuncular üretim ve gelirler üzerindeki etkiyi deneyimler ve gelir kaybetmeden saldırının etkisini en aza indirmek için farklı iş ve BT stratejileri ve çözümleri benimsemeyi öğrenirler.

Oyunu en fazla gelirle bitiren, siber güvenlik sistemindeki tüm tuzakları bulup analiz eden ve uygun şekilde müdahale eden takım **KAZANIR.**

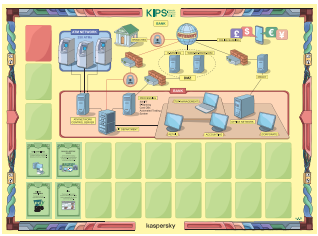
# Tüm dikey pazarlar için kurumsal KIPS senaryoları

### Şirket



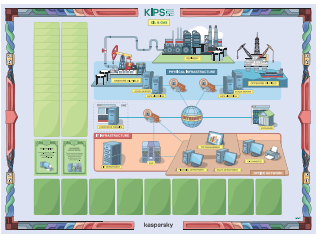
Kuruluşu **fidye yazılımlarından, APT'lerden, otomasyon güvenlik kusurlarından koruyun.**

### Banka



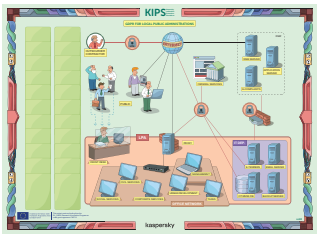
Finans kurumlarını Tyukpin, Carbanak gibi **üst düzey gelişen APT'lerden koruyun.**

### Petrol ve gaz



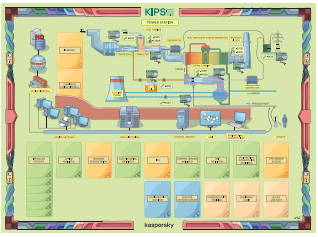
Web sitesi tahrifatından **gerçek bir fidye yazılımına ve sofistike bir APT'ye kadar çeşitli tehditlerin etkisini keşfedin.**

### Yerel kamu yönetimleri



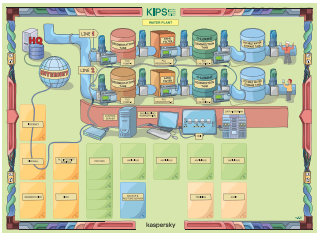
Genel web sunucularını saldırılara karşı koruma ve güvenlik açıklarının suistimal edilmesini önleyin.

### Enerji santrali



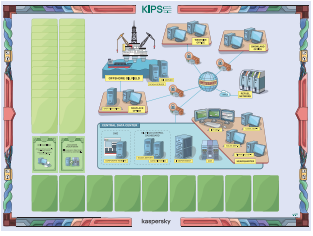
Endüstriyel kontrol sistemlerini ve kritik altyapıyı Stuxnet tarzı siber saldırılardan koruyun.

### Su arıtma tesisi



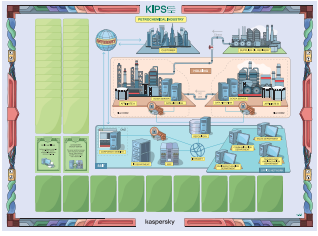
Bir su arıtma tesisinin BT altyapısını koruyarak iki üretim hattının istikrarını sağlayın.

### Petrol holdingi



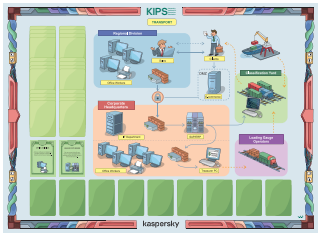
Dünyanın dört bir yanında ofisleri bulunan küresel bir Petrol ve Enerji şirketinin gelirlerini korumak için siber güvenliği sağlayın.

### Petrokimya sanayii



Etilen üretimine odaklanarak büyük bir petrokimya holdinginin yeni şubesinin normal işleyişini sağlayın.

### Ulaşım

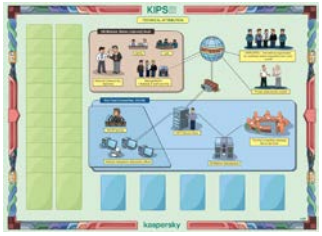


Lojistik şirketlerini Heartbleed, APT, B2B Ransomware, Insider saldırılarına **karşı koruyun.**

### Havalimanı

Havalimanında yolcuların güvenliğini ve malların zamanında teslim edilmesini sağlayın, varlıklarını çok sayıda siber saldırı ve tehditten koruyun.

### Teknik niteleme



BM sunucularına yönelik karmaşık bir APT saldırısını araştırın ve teknik olarak ilişkilendirin.

### Küçük-Orta Ölçekli İşletme

KOBİ'lerin işletmelerini DDoS, Fidye Yazılımı, Mobil Uygulama saldırısı ve Kimlik hırsızlığı ile ilgili siber güvenlik tehditlerinden korumalarına yardımcı olun.

### Telekom

Bir telekomünikasyon sağlayıcısı, bir bulut hizmeti sağlayıcısı, bir oyun geliştiricisi ve genel merkezden oluşan büyük bir telekomünikasyon holdinginin varlıklarını koruyun.

## KIPS'ten daha da fazla yararlanmak ister misiniz?

Neden KIPS deneyiminizi Kaspersky'nin Güvenlik Farkındalığı portföyünün bir parçası olan **Yönetici Eğitimi** ile tamamlamıyorsunuz? Yöneticilere yönelik bu eğitim, Güvenlik Farkındalığı yaklaşımınıza bağlı olarak KIPS oyununuzdan önce veya sonra alınabilir. Mevcut tehdit ortamının işletmeniz için ne anlama geldiğini, bir siber saldırı durumunda ne gibi önlemler almanız gerektiğini ve diğer birçok ilginç, ilgili ve faydalı bilgiyi keşfederek KIPS deneyiminizi artırın. (Yönetici Eğitimi iki formatta sunulmaktadır: etkileşimli çevrimdışı atölye çalışması veya çevrimiçi kurs olarak)

### KIPS kullanıcıları ve müşterileri oyun hakkında ne diyor?

Kaspersky Endüstriyel Koruma Simülasyonu gerçekten ufuk açıcıydı ve tüm güvenlik uzmanları için zorunlu hâle getirilmelidir.

**Warwick Ashford,**
Computer Weekly

CERN'de binlerce insanın üzerinde çalıştığı çok sayıda BT ve mühendislik sistemimiz var. Bu nedenle, siber güvenlik açısından bakıldığında, farkındalığı artırmak ve insanları siber güvenliğe önem vermeye teşvik etmek, teknik kontroller kadar önemlidir. Kaspersky eğitiminin ilgi çekici, aydınlatıcı ve verimli olduğu kanıtlandı.

**Stefan Luders,**
CERN CISO

Gerçekten aydınlatıcıydı ve bazı katılımcılar bu oyunu şirketlerinde kullanmak istedi.

**Joe Weiss PE,**
CISM, CRISC, ISA Fellow

Üyelik ve iş birliğine dayalı bir insan ağı oluşturmalıyız ve KIPS, bunu başlatmak için mükemmel bir yoldur.

**Daniel P. Bagge,**
Národní centrum kybernetické bezpeč nosti, Çek Cumhuriyeti

### Bir KIPS oturumuna nasıl hazırlanılır

**Program:** KIPS'yi ayrı bir etkinlik veya mevcut etkinlik/konferans/seminer içindeki oturum olarak planlayın (bu durumda KIPS için en uygun zaman ilk günün akşamıdır).

**Grup:** 3-4 kişilik takımlara bölünmüş 20-100 kişi; ideal olarak her ekip Yönetim, Mühendislik, CISO/BT Güvenliği bölümlerindeki kişilerden oluşmalıdır:

- Her rolden/işlevden en az 1 üye olması en iyisidir,
- Ekipler farklı veya aynı şirketteki/departmandaki kişilerden oluşabilir,
- Katılımcıların birbirlerini tanıyıp tanımamaları önemli değildir.

**Düzen:** Oyun 1,5-2 saat sürer ancak oda, hazırlık ve düzenleme için oyundan 2 saat önce Kaspersky'nin kolaylaştırıcı ekibi için kullanılabilir hâlde olmalıdır.

**Oda:** Plan kişi başına yaklaşık 3 metrekare, sütunsuz, standart AV Ekipmanı: Projektör (6-8 lümen), Perde, Ses sistemi (hoparlörler, uzaktan kumanda, mikrofonlar).

**İnternet erişimli Wi-Fi** (KIPS oyun sunucusuna erişim için), Wi-Fi destekli her takım (4 kişi) başına 4Mbps iPad veya başka bir tablet.

**Mobilya:** 4 kişilik katılımcı masaları (en az 75x180 cm boyutlarında dikdörtgen masa veya en fazla 1,5 m çapında yuvarlak masa), Katılımcılar masalarda 4 kişilik gruplar hâlinde oturmalıdır. Ortak ev sahibi için masalar, tüm katılımcılar için sandalyeler.

# Referanslar ve vaka çalışmaları

KIPS Oyunu, 50'den fazla ülkede endüstriyel güvenlik uzmanları tarafından oynandı.

- KIPS; İngilizce, Rusça, Almanca, Fransızca, Japonca, İspanyolca (AB), İspanyolca (LA), Portekizce, Türkçe, İtalyanca, Çince, Hollandaca ve Arapça dillerine çevrilmiştir.
- KIPS, aralarında CyberSecurity Malaysia, Çek Cumhuriyeti NSA ve Hollanda'daki Cyber Security Centrum'un da bulunduğu çok sayıda devlet kurumu tarafından kullanılmakta ve ulusal kritik altyapı kuruluşlarındaki yüzlerce uzman için kritik altyapı farkındalığını artırmaktadır
- KIPS, SANS Enstitüsü gibi önde gelen eğitim otoriteleri tarafından lisanslanmıştır ve dünya genelinde SANS öğrencilerinin eğitiminde kullanılmaktadır
- KIPS, Mitsubishi-Hitachi Power Systems dahil olmak üzere güvenlik hizmeti sağlayıcıları ve satıcıları tarafından lisanslanmıştır ve kritik altyapı müşterileri için eğitimde kullanılmaktadır
- KIPS, Avrupa Komisyonu'nun küçük ve mikro işletmeleri siber tehditlere karşı eğitmek ve korumak ve gizlilik yönetimlerini geliştirmek için yürüttüğü Geiger projesinin bir parçasıdır

# Eğitmen eğitimi mevcuttur

Bir müşteri KIPS'yi daha geniş bir kitleyi eğitmek için kullanmak istiyorsa - birden fazla departman veya tesisten çok sayıda çalışan, yönetici ve uzman - KIPS eğitimi için bir lisans satın almak, dâhilî eğitmenleri eğitmek ve KIPS oturumlarını müşterinin belirlediği şekilde yürütmek faydalı olabilir.

## Bu lisans türü şunları içerir:

- KIPS eğitim programını şirket içinde kullanma hakları.
- Bir eğitim materyalleri seti ve bunları kullanma/çoğaltma hakları.
- Lisans süresi boyunca KIPS yazılım sunucusu için giriş/şifre.
- KIPS eğitiminin nasıl yürütüleceği ve gerçekleştirileceği konusunda eğitmen kılavuzu, program liderleri için eğitim ve öğretim.
- Bakım ve destek (KIPS yazılımı ve eğitim içeriği için güncellemeler ve destek).
- KIPS Senaryolarının isteğe bağlı olarak özelleştirilmesi (ek ücret uygulanır).

# Ortaklar ve eğitim merkezleri için KIPS

KIPS, iş ortaklarının Farkındalık çözümlerinden çeşitli şekillerde yararlanmaları için harika bir fırsattır. Bunu yalnızca bir ürün olarak satmakla kalmazlar, aynı zamanda eğitim merkezi müşterilerine de satabilir, hatta oturumları kendileri düzenleyebilirler. (Kaspersky'nin eğitim uzmanları, bu seçeneği tercih ederlerse iş ortaklarına eğitim için beceri kazandırabilir).

Kaspersky Security Awareness

## Temel program farklılıkları

### Önemli siber güvenlik uzmanlığı

Ürünlerimizin merkezinde yer alan bir siber güvenlik becerisine dönüşen 25 yılı aşkın siber güvenlik deneyimi

### Kuruluşunuzun her düzeyinde çalışanların davranışlarını değiştiren eğitimler

Oyunlaştırılmış eğitimimiz, eğlenceli eğitim yoluyla katılım ve motivasyon sağlarken öğrenme platformları, öğrenilen becerilerin süreç sırasında unutulmamasını sağlamak için siber güvenlik becerilerinin benimsenmesine yardımcı olur.

# Kaspersky Güvenlik Farkındalığı – BT güvenliği becerilerinde uzmanlaşmak için yeni bir yaklaşım

Davranışlardaki sürdürülebilir değişiklikler zaman aldığından, yaklaşımımız birden fazla bileşen içeren sürekli bir öğrenme döngüsü oluşturmayı içerir.
Oyun tabanlı öğrenme, üst düzey yöneticilerin ilgisini çekerek onları siber güvenlik girişimlerinin savunucuları ve siber güvenli davranış kültürü oluşturmanın destekçileri haline getirir. Oyunlaştırılmış değerlendirme, çalışanların bilgilerindeki boşlukları tanımlamaya ve onları daha fazla öğrenme için motive etmeye yardımcı olurken, çevrimiçi platformlar ve simülasyonlar onları doğru becerilerle donatır ve güçlendirir.

### Sürekli öğrenme döngüsü

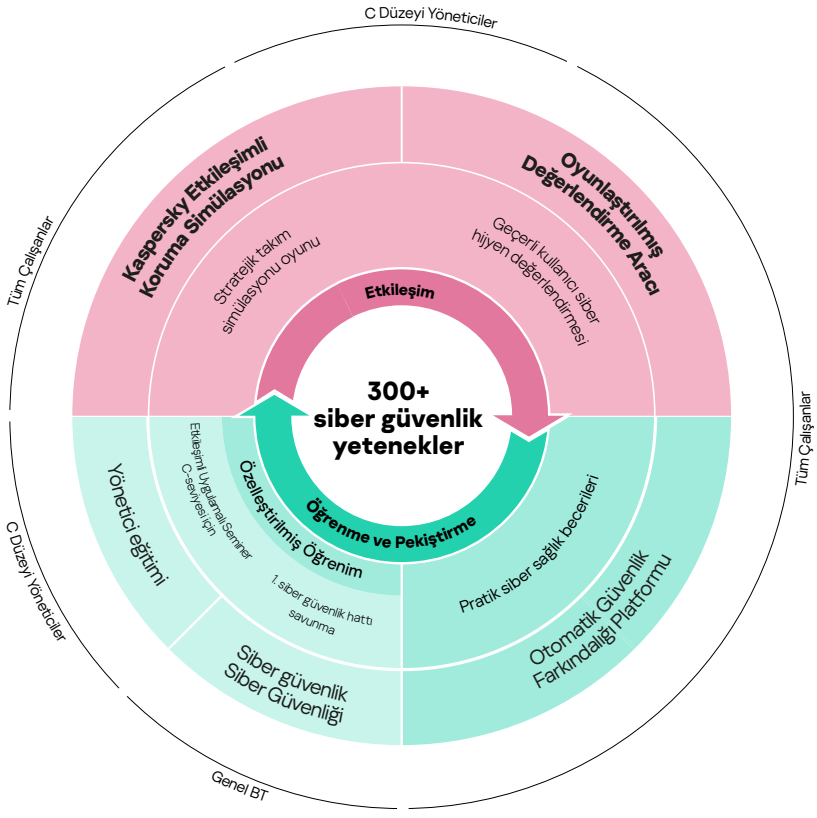
**Katılım/ motivasyon**
- Neden buna ihtiyacım var?
- Kavrama

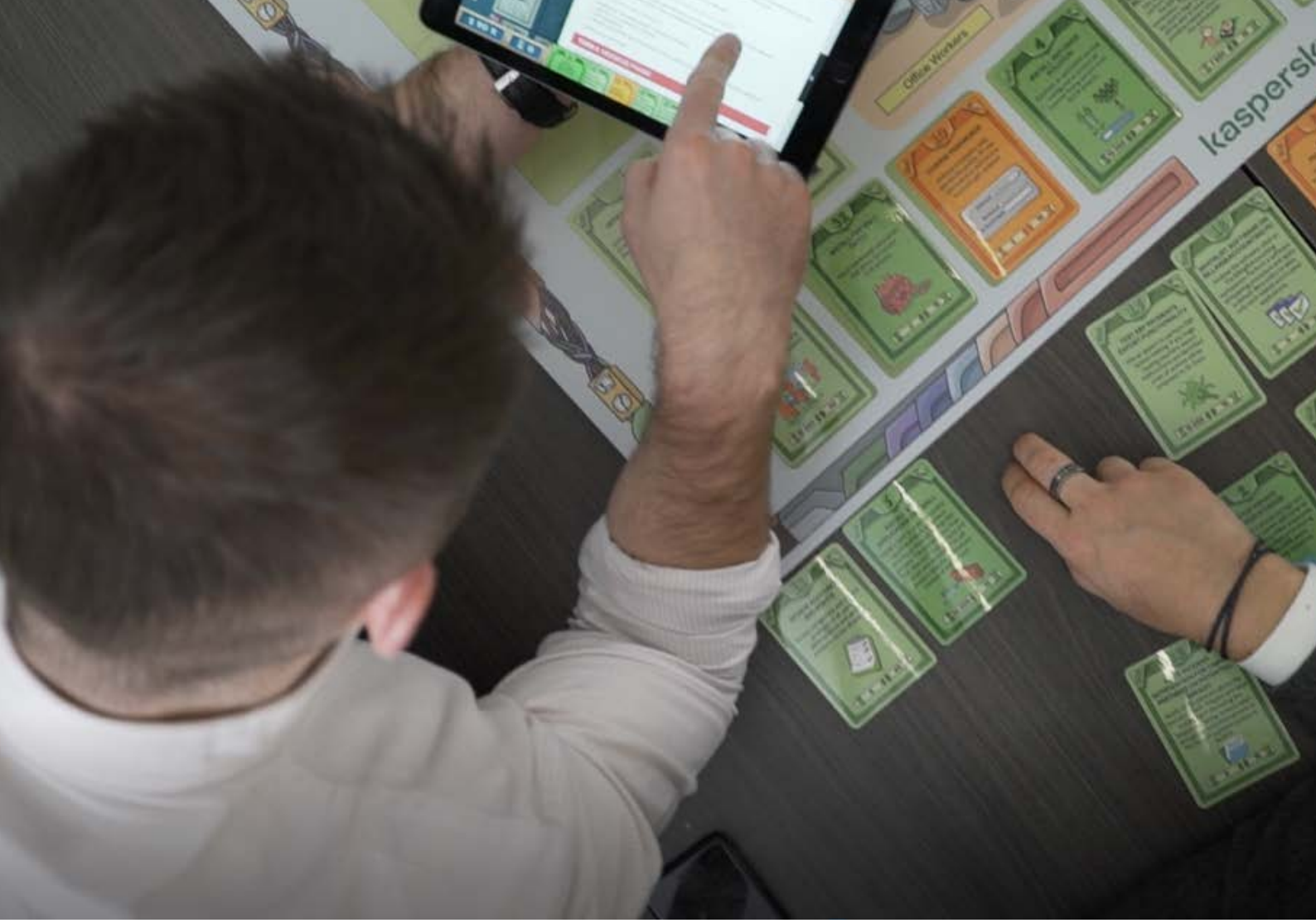
**Başlangıç noktası**
- Bilgi sahibi miyim?
- Hangilerini biliyorum ve boşluklar nerede?

**Öğrenme**
- Mikro öğrenme
- Sürekli öğrenme
- Uyum sağlama

**Güçlendirme**
- Doğru anlamış mıyım?
- Bunu hatırlıyor muyum?
- Buna göre hareket ediyor muyum?

## Farklı kuruluş seviyeleri için farklı eğitim formatları






Kurumsal Siber Güvenlik: www.kaspersky.com.tr/enterprise
Kaspersky Güvenlik Farkındalığı: www.kaspersky.com.tr/awareness

www.kaspersky.com.tr

kaspersky