Kaspersky Security Awareness

Tüm kuruluş düzeyleri için bilgisayar tabanlı eğitim programları

www.kaspersky.com.tr/awareness
#truecybersecurity

Kuruluşunuzda siber güvenliği sağlamanın etkili yolu

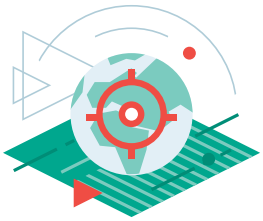
Siber olayların %80'i insan hatalarından kaynaklanır. Şirketler, personelleriyle ilgili güvenlik olaylarını düzeltmek için milyonlarını kaybeder. Ancak bu sorunları önlemeyi amaçlayan geleneksel eğitim programlarının etkisi sınırlıdır ve genellikle istenen davranışı oluşturma ve teşvik etme konusunda başarısız olur.

Müşteriler neden mevcut farkındalık eğitimi programlarından memnun değil?

- Hedef belirleme ve eğitim planlama konusunda kararsızlar
- Eğitimin yönetilmesi çok zaman alıyor
- Raporlama, hedef izleme konusunda yardımcı olmuyor
- Çalışanlar programa "inanmıyor" → bu nedenle gerekli becerileri geliştirmiyor.

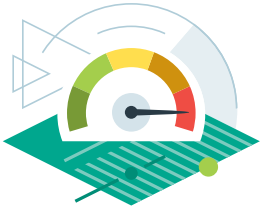
Kaspersky Security Awareness – öğrenmeye yeni bir yaklaşım

Programın temel farklılıkları



Hedeflerin belirlenmesi ve program seçimi

- Global verilere dayanarak hedef belirleme
- Dünya/endüstri ortalamalarına göre karşılaştırma

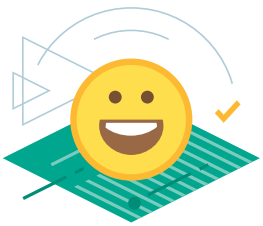


Öğrenme yönetimi

- Otomatik öğrenme
- Kendi kendine ayarlanan öğrenme yolları
- Harcanan zamanın hesaplanması

Raporlama ve analiz

- İstediğiniz zaman eyleme geçirilebilir raporlar
- Gelişim potansiyelinin anında analizi



Program verimliliği ve değerlendirme

- Gerçek oyunlaştırma
- Rekabet ve meydan okuma
- Aşırı yüklemenin önlenmesi

Etkili Güvenlik Farkındalığı

Her düzeyden personelin eğitimi, kurum genelinde güvenlik farkındalığını artırmak ve siber güvenlik, çalışanların iş sorumluluklarının bir parçası olarak algılanmasa bile tüm çalışanları siber tehditlere ve karşı önlemlere dikkat etme konusunda motive etmek için önemlidir.

Çalışan hataları günümüzde kuruluşlardaki siber güvenlik olaylarının büyük bir kısmından sorumludur.

Geleneksel farkındalık programları kullanılırken bile insan hatası, büyük bir kurumsal siber risk oluşturabilir:

Kuruluş başına 1.155.000 USD – dikkatsiz/bilgilendirilmemiş çalışanların neden olduğu saldırıların ortalama finansal etkisi*

Her KOBİ için 101.000 USD – kimlik avı/sosyal mühendislik kaynaklı saldırıların finansal etkisi **(kuruluş başına 1,3 milyon USD)***

Yıllık çalışan başına 400 dolara kadar – kimlik avı saldırılarının ortalama maliyeti**

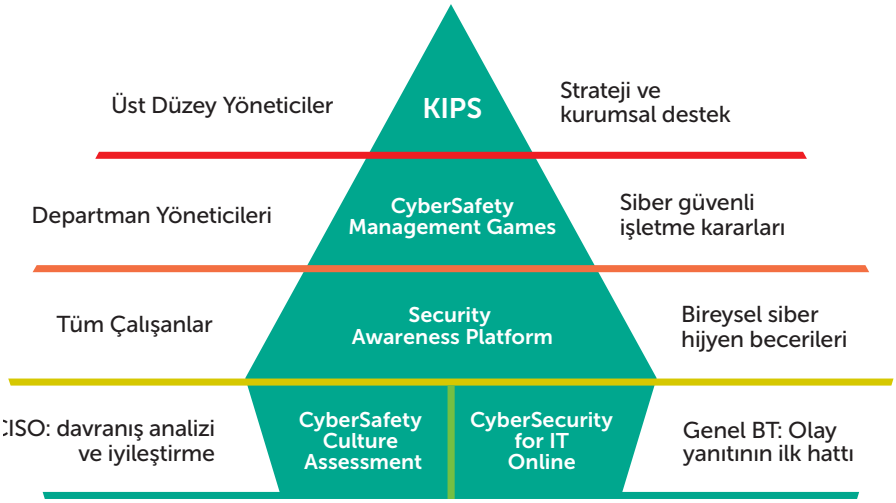
* Rapor "BT güvenliğinde insan faktörü: Çalışanlar Kuruluş İçinde İşletmeleri Nasıl Savunmasız Hale Getirir", International, Haziran 2017.

** Ponemon Institute'un, Ağustos 2015 tarihli "Kimlik Hırsızlığının Maliyeti ve Çalışan Eğitiminin Değeri" çalışmasına dayanan hesaplama.

Kaspersky Security Awareness eğitimi

Kaspersky Lab, modern eğitim teknikleri kullanan ve kurum yapısındaki her düzeye hitap eden bilgisayar tabanlı oyunlaştırılmış eğitim ürünleri ailesini piyasaya sürdü. Bu yaklaşım, ortak çalışmaya dayalı bir siber güvenlik kültürü oluşturarak kuruluşun tamamında kendi kendini yöneten bir siber güvenlik durumu yaratır.

Kuruluştaki farklı düzeyler için farklı eğitim formatları



Başarısını kanıtlamış sonuçlar sağlayan bir yaklaşım

Maksimum

%90

Olayların toplam sayısında %90'a varan azalma

En az

%50

Olayların finansal etkisinde minimum %50 azalma

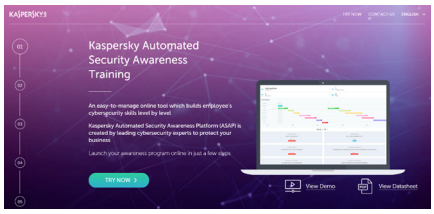
Muhteşem

%86

Katılımcıların %86'sı programı kesinlikle başkalarına tavsiye eder

Çalışanlar siber saldırganlar için önemli bir odak noktasıdır

İşletmeler siber saldırıların tehditleri karşısında daha bilinçli hale geldikçe teknik savunmalar da daha güçlü hale geliyor. Kurumsal ağları ele geçirmek, eskisinden çok daha zor. Bu nedenle, saldırganlar güvenli verilere erişmek için yeni yöntemler buluyor. Bu çabalar, onları şirket siber güvenliğinin en zayıf noktası olan çalışanlara yönlendiriyor.



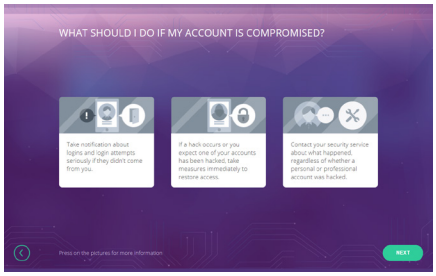
ASAP, ayarlanması kolay eğitim hedefleri, iyi dengelenmiş ve önceden tanımlanmış bir öğrenme yolu, gerçek yaşamla ilişki ve uygulanabilir raporlama sunarak çalışanlar ve yönetim için programın takdir edilmesini ve değer görmesini sağlar.

Her konu, belirli güvenlik becerilerini geliştiren farklı düzeyler içerir. Düzeyler, ortadan kaldırmaya yardımcı oldukları risk derecesine göre tanımlanır. 1. Düzey, basit ve toplu saldırılara karşı davranışı ele alır. Daha yüksek düzeyler, en gelişmiş ve hedefli saldırılara karşı farkındalık eğitimi sağlar.

Platform, 7 dilde mevcuttur: İngilizce, Almanca, İtalyanca, Fransızca, İspanyolca, Rusça ve Arapça*.

ASPS, MSP'ler ve xSP'ler için idealdir: Birden fazla işletmenin eğitim hizmetleri, tek bir hesap üzerinden yönetilebilir ve lisanslar aylık abonelik bazında satın alınabilir.

Kaspersky ASAP çözümünün tam işlevli sürümünü asap.kaspersky.com adresinden deneyin, kendi kurumsal güvenlik farkındalık eğitim programınızı kurmanın ve yönetmenin ne kadar kolay olduğunu görün!



Güvenlik farkındalığı eğitimi - siber güvenli iş gücü davranışlarını oluşturma

İki ayrı platform üzerinden mevcut çalışanlar için çeşitli siber güvenlik beceri düzeyleri sağlarken büyüyen işletmelerin ve büyük kuruluşların farklı ihtiyaçlarına da hitap eden çevrimiçi interaktif eğitim.

Büyüyen İşletmeler için Kaspersky Automated Security Awareness Platform (ASAP).

Yalnızca bilgiye değil, "model algısına" da dayanan çevrimiçi eğitim programlarına yeni bir bütünsel yaklaşım, çalışanların yeni tehditlere karşı bile güvenli bir şekilde yaklaşmalarını sağlar.

Otomatik öğrenme yönetimi

- Platformun başlatılması yalnızca 10 dakika sürer. Kullanıcı listenizi yüklemek, kullanıcıları gruplara ayırmak ve her grup için risk seviyelerine göre hedef düzey ayarlamak hızlı ve kolaydır.
- Platformun kendisi daha sonra her grup için bir eğitim programı oluşturur. Bu eğitim programı, sürekli pekiştirme ile aralıklı öğrenme sağlar ve öğrenim modülleri, e-posta ile pekiştirme, testler ve kimlik avı simülasyonu saldırıları dahil olmak üzere farklı eğitim formatlarının bir harmanıyla otomatik olarak sunulur.

Her zaman kullanılabilen uygulanabilir raporlama

- Canlı veri izleme, eğilimler ve tahminler sağlayan kullanıcı dostu kontrol paneli ile öğrencilerinizin ilerlemesini takip edin
- Sonuçları nasıl iyileştirebileceğiniz hakkında öneriler alın

Evrensel eğitim müfredatı

- Geniş bir yelpazedeki önemli siber güvenlik konuları, başlangıç seviyesinden gelişmiş seviyelere kadar farklı düzeylerde sunulmaktadır.

Önemli avantajlar:

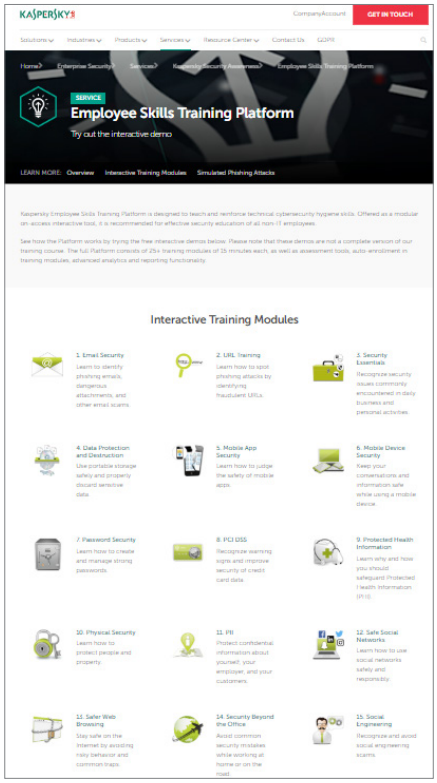
Tam otomasyon yoluyla basitlik: Programın başlatılması, yapılandırılması ve izlenmesi çok kolaydır ve sürekli yönetim tamamen otomatiktir ve yönetim müdahalesi gerektirmez.

Etkililik: Programın içeriği, bilginin akılda kalması ve daha sonra becerilerin uygulanması için eğitim oturumlarını amaca odaklanmış ve kısa tutarak mikro-öğrenmeyi destekleyecek şekilde yapılandırılmıştır.
Esnek lisanslama: Kullanıcı başına lisans modeli, en az 5 lisanstan başlayabilir.

*Arapça 2019 yılının ilk yarısında eklenecektir.

Platformu platformla birlikte verilen belgelerdeki talimatlara göre kullanarak çalışanlarınızı görevleri, sorumlulukları ve tehdit altında oldukları ortam doğrultusunda basit kavramlardan karmaşık güvenlik kavramlarına geçmeye teşvik edebilir ve bu sayede güçlü, sürekli ve ölçülebilir bir siber güvenlik eğitim planı oluşturabilir ve uygulayabilirsiniz.

Employee Skills Training Platform tüm önemli güvenlik alanlarını kapsar ve kapsamlı raporlama olanakları ve kimlik avı simülasyonları için gelişmiş değerlendirme araçları ve fonksiyonları sunar.
Platform 34 dilde mevcuttur.
İnteraktif demomuz için bkz.
www.kaspersky.com.tr/demo-sa



Kurumsal İşletmeler için EMPLOYEE SKILLS TRAINING PLATFORM

Tipik senaryolar ve durumlar, siber saldırı simülasyonları, bireysel görevler ve rehberlik sayesinde platform, potansiyel tehditlerin anlaşılmasını sağlar ve onlarla başa çıkmak için gereken becerileri geliştirir. Çevrimiçi oyunlaştırılmış öğrenme, çalışanların alıştırma yapmasını ve etkileşimli bir çalışma portalı üzerinden öğrenmesini sağlar.

Etkileşimli Eğitim Modülleri

- Eğlenceli ve kısa
- Zincirleme etkisi içeren alıştırmalara dayalı
- Otomatik kayıt belirli becerileri güçlendirir
- 33 modül tüm güvenlik alanlarını kapsar

Bilgi Değerlendirmesi

- Önceden tanımlanmış veya rastgele değerlendirmeleri, müşteri tarafından tanımlanan soruları ve özelleştirilebilir uzunluk seçeneklerini içerir
- Geniş bir güvenlik senaryosu yelpazesini kapsar
- Karışık sorulardan oluşan geniş soru kitaplığı, hile yapılmasını önler

Kimlik Avı Saldırıları Simülasyonu

- Çeşitli şablonlar ve zorluk düzeyleri ile 3 tür kimlik avı saldırısı
- Çalışanlar, kimlik avı e-postalarını her açtığında ortaya çıkan "öğrenme fırsatları"
- Özelleştirilebilir şablonlar
- Saldırı simülasyonu perfomansıyla tespit edilen bilgi eksikliklerini kapatmak için eğitim modüllerinin otomatik olarak atanması

Raporlama ve Analiz

- Sonuçlar bölüm, konum ve iş birimi olarak ayrılır ve bireysel düzeyde de sunulur
- Çalışan beceri düzeylerini ve dinamiklerini izler
- LMS'nize çeşitli formatlarda veri aktarımını destekler

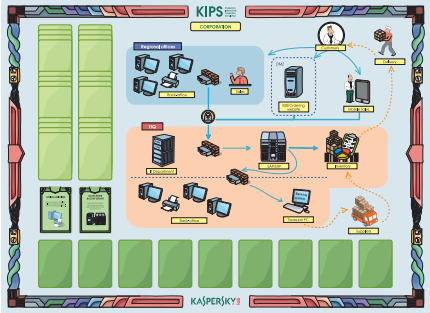
Önemli avantajlar:

- **Zaman tasarrufu.** Sadece çalışanın bireysel göreviyle doğrudan ilgili olan eğitim üstlenilir: Çalışanın görevine ve uzmanlık düzeyine bağlı olarak belirli eğitim modülleri atanabilir.
- **Oyunlaştırma ve etkileşimli olma:** Sıkıcı açıklamalar yoktur; yalnızca yaparak öğrenilen interaktif yöntemler kullanılır
- **Sadece bilgi değil, sağlam beceriler sunar:** Eğitim materyallerini ve testleri, gerçek yaşam durumları simülasyonlarıyla birleştirir.
- **Karşılaştırmalı değerlendirme için veri sağlar:** Kurumsal performansınızı sektördeki genel performans ile karşılaştırır.
- **Ek kaynak gerekmez:** Eğitim müşterinin iş yerinde gerçekleştirilebilir; ek beceri/eğitim/kaynak gerekmez.

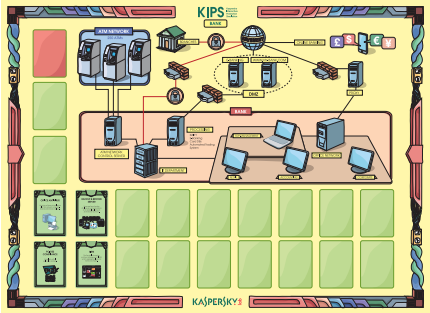
KIPS eğitimi, üst düzey yöneticiler, iş sistemi uzmanları ve BT uzmanlarını hedef alır ve kullanılan modern bilgisayarlı sistemlerin riskleri ve güvenlik sorunları hakkında farkındalıklarını arttırmayı amaçlar.

Bazı KIPS senaryoları:

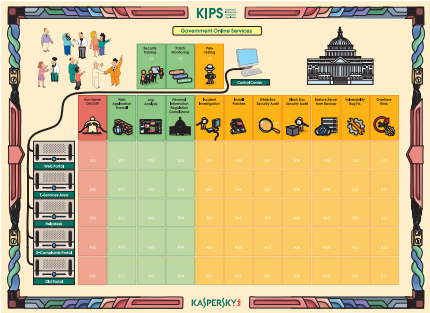
Şirket



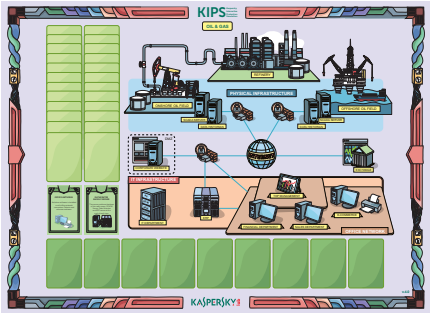
Banka



e-Devlet



Petrol ve Doğal Gaz



KIPS online:

- Global kuruluşlar için ideal
- Eşzamanlı olarak 300 ekibi destekler
- Farklı takımlar, farklı dillerdeki oyun arayüzlerini seçebilir
- Bir eğitmen, her oturuma WebEx aracılığıyla liderlik eder

Kaspersky Interactive Protection Simulation (KIPS) eğitimi stratejik anlayışı ve desteği teşvik eder.

KIPS nedir?

KIPS, katılımcıların kârı en üst düzeye çıkarmaya ve pazardaki güveni korumaya çalışırken bir dizi beklenmedik siber tehdidi yönetmekle görevlendirildiği bir iş ortamını taklit eden bir rol yapma oyunudur ve takım olarak oynanır.

Temel düşünce, mevcut en iyi proaktif ve reaktif kontrollerin arasından seçim yaparak bir siber savunma stratejisi geliştirmektir.

KIPS, şu nedenlerden dolayı son derece etkilidir:

- Siber güvenliğe, uygulanabilir yeni bir yaklaşım getirir
- Eğlenceli, ilgi çekici ve hızlıdır (2 saat)
- Ekip çalışması ile iş birliğini tesis eder
- Girişim ve analiz becerilerini rekabet yoluyla geliştirir
- Siber güvenlik ve siber güvenlik davranışlarının oluşturulmasında, keşiflerin ve hataların oyun yoluyla güvenli bir şekilde yapılmasını ve analiz edilmesini sağlar

KIPS deneyimi:

- Yeni ortaya çıkan tehditler için hazırlıklı olun; suçluların teknik olarak (tehdit istihbaratı) nasıl çalıştığını öğrenin ve hedeflerini anlayın
- Olay müdahalesini, olay önleme ile nasıl birleştireceğinizi görün
- Güvenlik denetimlerini doğru şekilde yapılandırmayı unuttuğunuzda neler olacağını görün
- Güvenlik, BT ve iş açısından eş zamanlı uyarılara dikkat edin

Sektörle ilgili senaryolar mevcuttur

(tümü KIPS Live ve KIPS Online sürümlerinde mevcuttur. Oyun, 10 dilde desteklenmektedir)

- **Şirket:** Kuruluşu Fidye yazılımı, APT'ler, otomasyon güvenlik kusurlarından vb. koruma.
- **Banka:** Finansal kurumları ATM'lere, yönetim sunucularına ve iş sistemlerine saldıran üst düzey APT'lerden koruma.
- **e-Devlet:** Saldırılara ve güvenlik açıklarından yararlanan yazılımlara karşı kamu web sunucularını koruma.
- **Elektrik Santrali/Su Tesisi:** Endüstriyel kontrol sistemlerini ve kritik altyapıyı koruma.
- **Taşımacılık:** Yolcu ve yük taşıyıcılarını Heartbleed, fidye yazılımı ve APT'lere karşı koruma.
- **Petrol ve Doğal Gaz:** Web sitesinin değiştirilmesinden mevcut fidye yazılımlarına ve gelişmiş APT'lere kadar çeşitli tehditlerin etkisini keşfetme.

Her senaryo, katılımcılara iş sürekliliği ve kârlılık açısından siber güvenliğin gerçek rolünü gösterir. Yeni ortaya çıkan zorlukların ve tehditlerin yanı sıra kuruluşların siber güvenliklerini sağlamaya çalışırken yaptıkları hataları vurgular, aynı zamanda ticaret ve güvenlik ekipleri arasında siber tehditlere karşı istikrarlı operasyonları ve sürdürülebilirliğin sağlanmasına yardımcı olan bir iş birliğini teşvik eder.

CyberSafety Management Games birim yöneticilerini eğitir ve motive eder

- Oyunlaştırmayı güvenlik konularının kapsamlı bir şekilde ele alınması, örnekler, açıklamalar ve alıştırmalar ile birleştirir,
- Kolay yönetilen eğitim sunma sürecini destekleyen özel amaçlı CyberSafety Management Games yazılımı ile desteklenir,
- Toplam 4 saat süren kısa modüllere bölünmüştür.

CyberSafety Management Games – siber güvenli iş kararlarının alınmasını sağlama

Bu son derece interaktif atölye çalışması (bilgisayar tabanlı ve öğretmenli öğrenmenin birleşimi), bölüm yöneticilerinin kendi işlerinde siber güvenliğin önemi konusuna odaklanmasını sağlar ve yöneticilere kendi bölümlerinde güvenli çalışma ortamını oluşturmak için gereken yeterlilik, bilgi ve bakış açısını kazandırır.

Güvenlik Ekibi için en büyük zorluk genellikle, çalışanlarla her gün etkileşimde bulunan ve iş kararlarını veren kişilerden oluşan yönetimin dikkatini çekmektir.

Bu nedenle Kaspersky Lab, **özellikle bölüm yönetimini/orta düzey yönetimi siber güvenlik destekçisi ve savunucusu haline getirmeyi amaçlayan bir eğitim programı geliştirmiştir.**

Kaspersky CyberSafety Management Games yöneticilere şunları sağlar:

- **Anlama:** Siber güvenlik önlemlerinin, önemli ancak karmaşık olmayan eylemler olarak içselleştirilmesi
- **İzleme:** Günlük çalışma süreçlerine siber güvenlik açısından bakma
- **Siber Güvenli Karar Verme:** İş süreçlerinin ayrılmaz bir parçası olarak siber güvenliğe önem verme
- **Güçlendirme ve İlham:** Departman ekiplerine etkili liderlik ve rehberlik sağlama.

Şirket eğitim merkezleri için "Eğitmeni eğit" yaklaşımı şu önemli uygulama avantajlarını sunar:

- Sunum kolaylığı: Farkındalık eğitmenleri güvenlik uzmanı olmak zorunda değildir;
- Programlama kolaylığı: Kısa modüler eğitim oturumları çalışanın çalışma planına uygundur.

Yardım masası uzmanları, genel BT güvenliğini ve yerel hizmet yöneticilerini hedefleyen Siber Güvenlik BT eğitimi.

Eğitim biçimi

Eğitim %100 çevrimiçidir: Katılımcıların yalnızca LMS ve bir Chrome tarayıcısı ile internet bağlantısına/erişimine sahip olması gerekir.

4 modülden her biri, kısa bir teorik özet, pratik ipuçları ve 4 ve 10 arasında alıştırmadan oluşur. Her bir modülde belirli bir beceri için alıştırma yapılır ve günlük çalışma hayatında BT Güvenlik araçlarının ve yazılımının nasıl kullanılacağı gösterilir.

Çalışmanın bir yıla yayılması amaçlanmıştır. Tavsiye edilen ilerleme hızı, haftalık 1 alıştırma şeklindedir. Her alıştırma 5 ila 45 dakika arasında tamamlanır.

Cybersecurity for IT Online

BT biriminin çalışmalarına dahil olan herkes için güçlü siber güvenlik ve birinci seviye olay müdahale becerileri oluşturan interaktif eğitim

Konuyla ilgili tüm çalışanlar sistematik bir eğitim almadan güçlü bir kurumsal siber güvenlik tutumu benimsemek mümkün değildir. Birçok kuruluş, siber güvenlik eğitiminin yanı sıra BT Güvenlik ekipleri için uzman eğitimi ve BT dışındaki çalışanlar için güvenlik farkındalığı eğitimi olmak üzere iki farklı düzeyde eğitim sağlamaktadır. Bu yaklaşımların hiçbiri, doğrudan güvenliğe dahil olmayan birçok BT personeli için işe yaramaz, ancak kurumsal siber güvenliğe özel ve önemli katkılar yapmak için ideal bir şekilde konumlandırılan çalışanlar için faydalıdır.

Birinci savunma hattı olay yanıtı

Kaspersky Lab, genel Kurumsal BT uzmanları için pazardaki ilk çevrimiçi beceri eğitimini sunar.

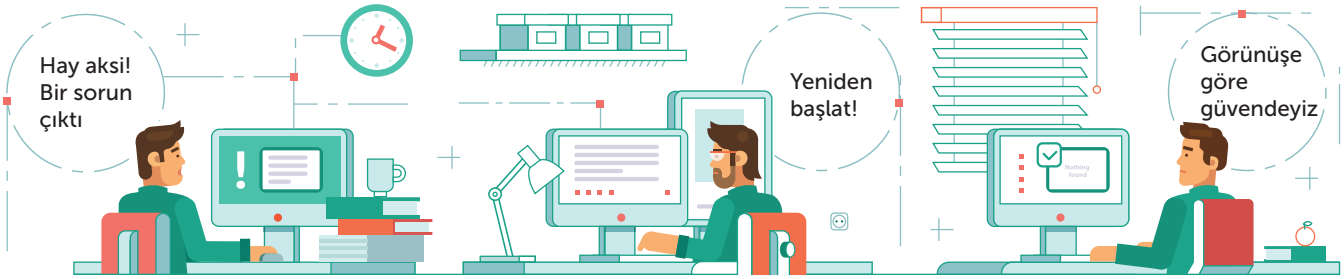
Kurs 4 modülden oluşur:

- Kötü amaçlı yazılımlar
- Olası istenmeyen programlar ve dosyalar
- İncelemenin temelleri
- Kimlik avı olayı yanıtı

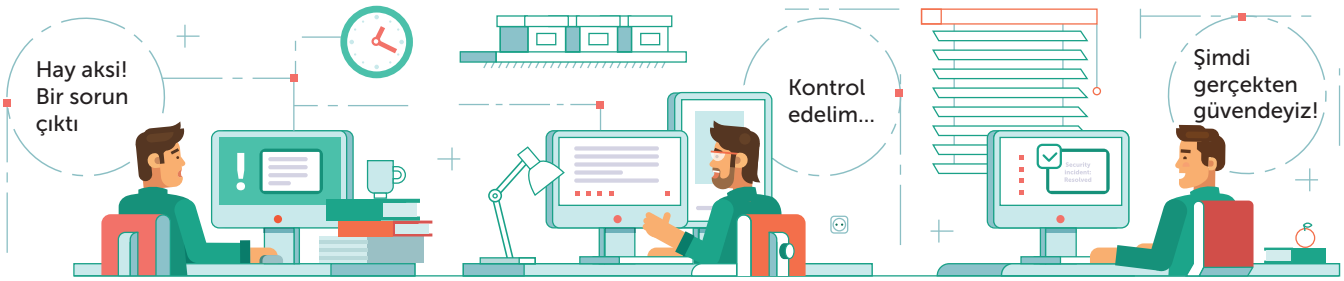
Bu kurs, BT uzmanlarına aşağıdakileri içeren pratik beceriler kazandırır:

- Zararsız gibi görünen bir PC olayındaki olası bir saldırı senaryosunu tanıma
- BT Güvenlik ekibine iletmek için olay verilerini toplama
- Tüm BT ekip üyelerinin güvenlik savunmasının birinci hattı rolünü üstlenmesini sağlayarak kötü niyetli belirtileri bulma

Mevcut Durum



Olması Gereken



Bu değerlendirme, güvenlik kültürünüze farklı açılardan bakar:

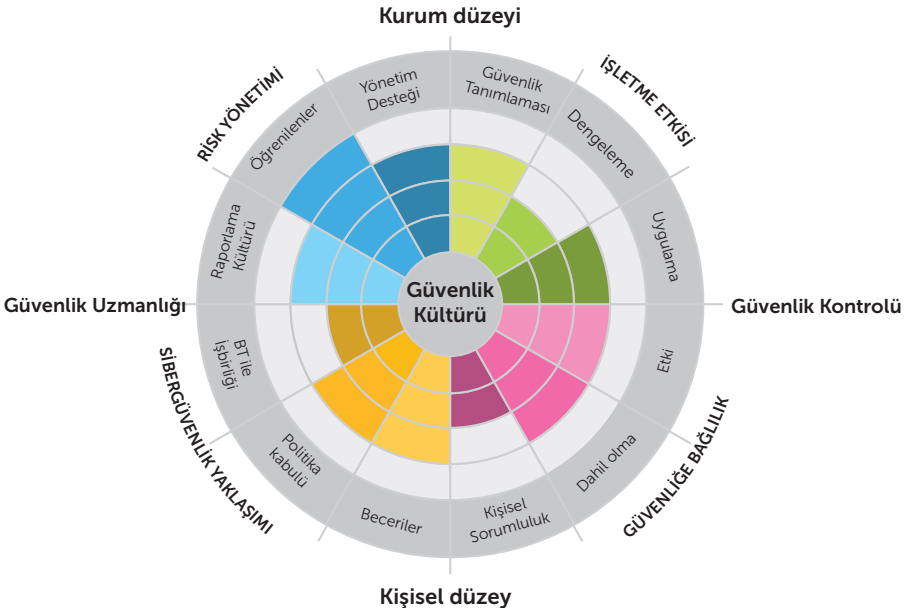
- Kuruluş (yönetim)
- Bireysel (çalışan)
- Uzmanlıktan faydalanma
- Bir süreç olarak Güvenlik Kalitesi

Değerlendirme, yaklaşık 15 dakika içinde çalışanlar tarafından tamamlanan bulut tabanlı bir anket yoluyla yapılır. Anketin tüm çalışanlar tarafından tamamlanması yaklaşık 2 hafta sürer.

Müşteri, anket bulgularının birleştirilmiş bir raporunu alır.

CyberSafety Culture Assessment

CyberSafety Culture Assessment, şirketin her düzeyinde siber güvenlik konusundaki günlük tutum ve davranışlarını analiz eder ve çalışanların siber güvenliğin farklı yönlerini nasıl algıladığını ortaya koyar.



Değerlendirme sonuçları, daha fazla odaklanma gerektiren dengesizliklerin ve alanların belirlenmesinin yanı sıra bilinçlendirme ve eğitim, şirket içi tanıtım, bilgi paylaşımı ve ticari iş birliği dahil olmak üzere Güvenlik Departmanının iç ve dış faaliyetlerinde öncelikleri doğrulama ve düzenlemede kullanılabilir.

CyberSafety Culture, kuruluş genelinde birlikte ölçülen bilgi alanlarının değerlendirilmesini kapsar. Değerlendirme sonuçları, iş verimliliğini desteklemek için siber güvenliğin rolü ve yeri hakkındaki görüşmelerin temelini oluşturur:

- Siber Güvenlik Anlayışı (güvenliğe ve ilkelere bakış açısı),
- Risk Yönetimi (rehberlik, geri bildirim, ilerlemeler)
- Bağlılık (güvenliğe karşı tutumlar ve davranışlar)
- İşe Etkisi (güvenlik ve iş verimliliği arasındaki denge)

Lütfen Cybersafety Culture raporunun şirketin teknik güvenlik olgunluk düzeyini değerlendirmediğini ve Güvenlik Departmanı'nın etkililiğini ölçmediğini unutmayın.

CyberSafety Culture raporu, çalışanların siber güvenliği nasıl algıladığını; kültürü, alışkanlıkları, ritüelleri ve günlük siber güvenlik uygulamalarını nasıl gördüklerini ve kurumsal güvenliğin farklı yönleriyle ilgili kişisel algılarını ortaya koymaktadır. Bu algı, sadece güvenlik veya risk yönetimi departmanının faaliyetleri ile değil, çeşitli şirket uygulamaları ve birimleri ile oluşur.

Kaspersky Security Awareness eğitim programları:

Yeni yaklaşım — kanıtlanmış etkililik

Daha fazla:
30x
Güvenlik bilincinde yatırım getirisi

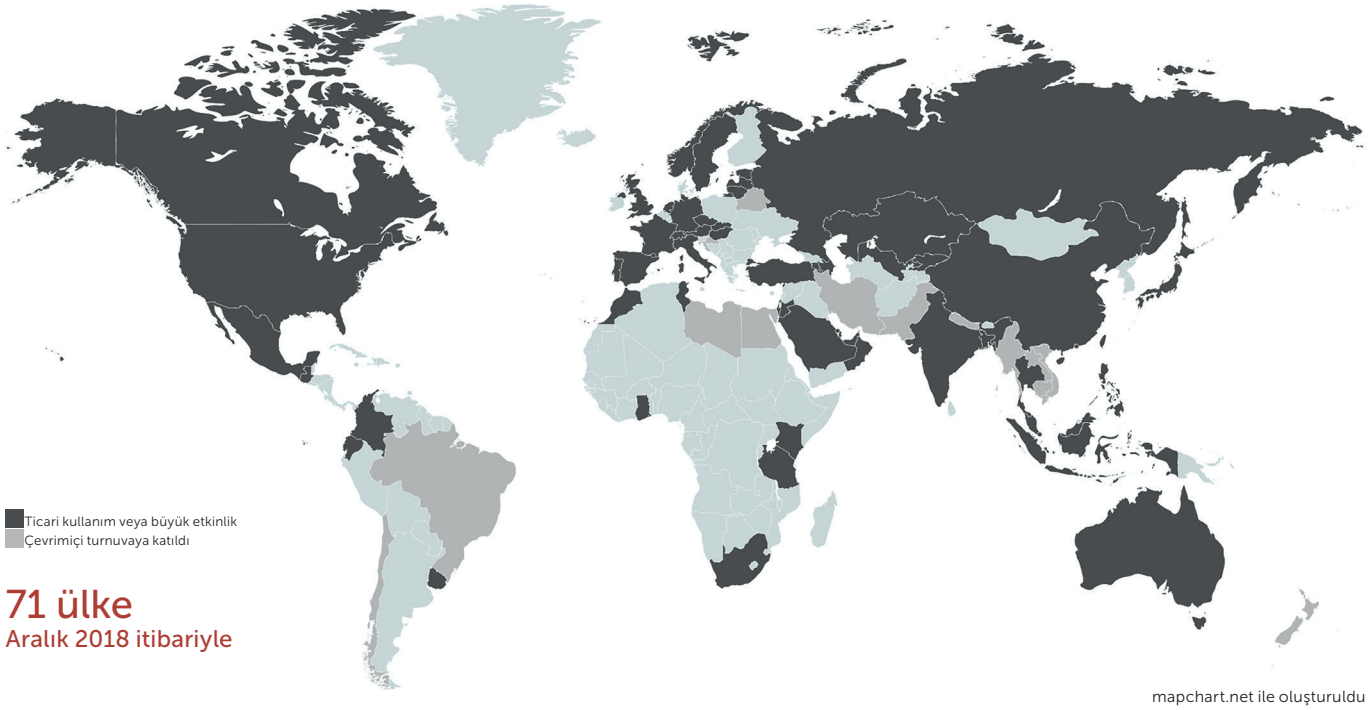
Maksimum
%90
Olayların toplam sayısında %90'a varan azalma

Minimum
%50
Olayların finansal etkisinde minimum %50 azalma

Maksimum
%93
%93'e varan oranda günlük çalışmalar için bilginin uygulanma olasılığı

Muhteşem
%86
Katılımcıların %86'sı deneyimi önermeye istekli

Dünya Genelinde Kaspersky Security Awareness



71 ülke
Aralık 2018 itibariyle

mapchart.net ile oluşturuldu

www.kaspersky.com.tr

Kaspersky Lab
Kurumsal Siber Güvenlik: **www.kaspersky.com.tr/enterprise**
Kaspersky Security Awareness: **www.kaspersky.com.tr/awareness**
Ürün tanıtımı: **www.kaspersky.com.tr/demo-sa**