Tüm kuruluş düzeylerine yönelik bilgisayar tabanlı eğitim programları

Kaspersky Güvenlik Farkındalığı

kaspersky GELECEĞİ YAKALAYIN

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

Kaspersky Güvenlik Farkındalığı

Kuruluşunuz genelinde siber güvenlik oluşturmanın etkili yolu

Tüm siber olayların %80'inden fazlası insan hatasından kaynaklanır. Kuruluşunuz genelinde temel siber güvenlik becerileri ve farkındalığı ile birlikte siber açıdan güvenli bir davranış kültürü, saldırı yüzeyini ve başa çıkmanız gereken olay sayısını azaltmada büyük önem taşır. Kuruluşlar, genellikle davranışı daha iyiye doğru değiştiren etkili çalışan eğitimi için doğru araçları ve yöntemleri bulmakta zorlanır. Bunu başarmanın sırrı, yetişkin eğitiminde en son teknikleri ve teknolojileri kullanan, en alakalı ve güncel içeriği sunan eğitimi sağlamaktır.

İnsan faktörü – siber güvenliğin en savunmasız unsuru

Siber güvenlik çözümleri hızla gelişerek ve karmaşık tehditlere uyum sağlayarak siber güvenliğin en savunmasız unsuru olan insan faktörüne yönelen siber suçluların hayatını daha da zorlaştırıyor.

%52 oranında C seviyesi yönetici operasyonel güvenlikte en büyük tehdidin çalışanlar olduğunu söyledi*

%43 oranında küçük işletme çalışanların BT güvenlik ilkelerini ihlal etmeleri nedeniyle bir güvenlik olayı yaşadı**

%60 oranında çalışan kurumsal cihazlarında gizli veriler (finansal veriler, e-posta veri tabanı vb.) bulunduruyor***

%30 oranında çalışan iş bilgisayarlarının oturum açma ve parola bilgilerini çalışma arkadaşlarıyla paylaştıklarını kabul etti***

%23 oranında kuruluş kurumsal veri depolaması için herhangi bir siber güvenlik kuralına veya ilkesine sahip değil***

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

Kaspersky Güvenlik Farkındalığı, kuruluşunuzun genel siber güvenliğinde kendilerine ait rolleri oynayabilmeleri için personelinizin siber güvenlik farkındalığını artıran bir dizi oldukça ilgi çekici ve etkili eğitim çözümü sunar. Davranışlardaki sürdürülebilir değişiklikler zaman aldığından yaklaşımımız, birden fazla bileşene sahip sürekli bir öğrenme döngüsü oluşturmayı içerir.

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?

Temel program farklılıkları

Önemli siber güvenlik uzmanlığı

Ürünlerimizin merkezinde yer alan bir siber güvenlik becerisine dönüşen 20 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.

* "Weathering the Perfect Storm: Securing the Cyber-Physical Systems of Critical Infrastructure" raporu. 2020

** "IT Security Economics 2021" Raporu, Kaspersky.

*** "Sorting out a Digital Clutter". Kaspersky Lab, 2019.

Çalışanlar hata yapar. Kuruluşlar para kaybeder...

$1.315.000
(kurumsal işletme başına)
Çalışanların uygunsuz BT kaynağı kullanımından kaynaklanan bir veri ihlalinin ortalama finansal etkisi*

%50
oranında işletme
doğrudan personelin uygunsuz davranışlarından kaynaklanan tehditlerle karşı karşıya kaldıklarını bildirdi (bu oran, bunu BT güvenliğine yönelik en yaygın tehdit yapıyor)*

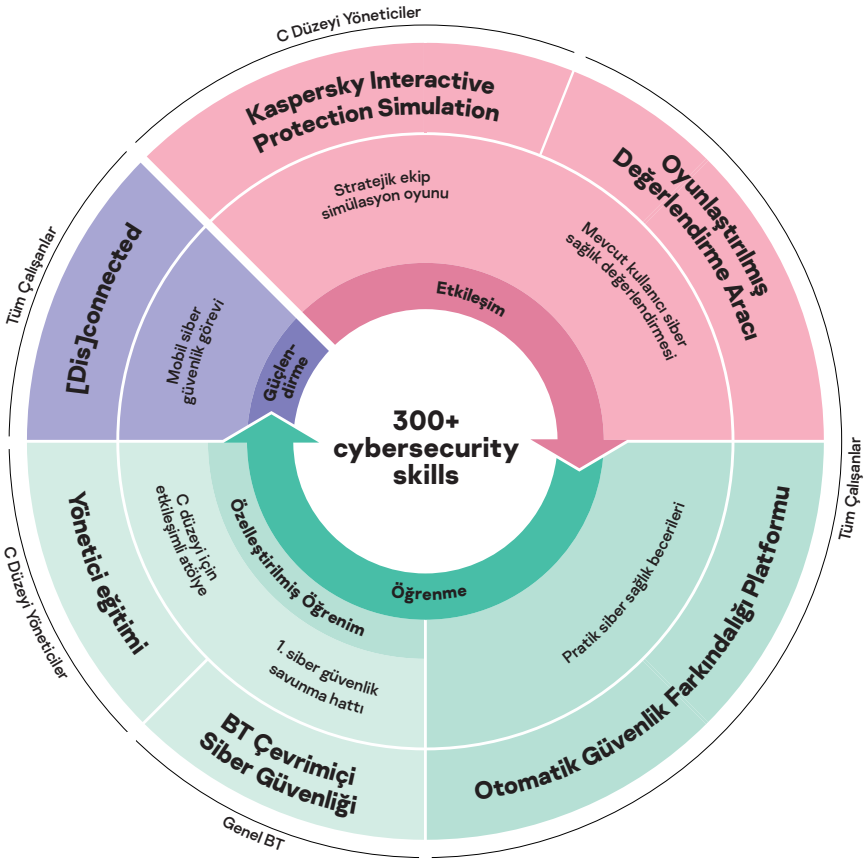
%86
oranında şirket
en az bir kişinin bir kimlik avı bağlantısına tıkladığını iddia etti**

$5,01 milyon
BEC saldırılarından ihlal başına ortalama maliyet
(BEC, saldırganların geçerli kurumsal e-posta hesaplarını ele geçirdiği veya yanılttığı bir kimlik avı türüdür)

Etkili güvenlik farkındalığı için motivasyonu artırma

Çalışanların davranışlarını değiştirmek, yaşayabileceğiniz en büyük siber güvenlik zorluğudur. İnsanlar genellikle beceri kazanmaya ve alışkanlıklarını değiştirmeye motive olmazlar, bu yüzden pek çok eğitim çabası neredeyse boş bir formaliteye dönüşür. Etkili eğitim, insan doğasının özelliklerini ve kazanılan becerileri özümseme yeteneğini dikkate alan farklı bileşenlerden oluşur. Siber güvenlik uzmanları olarak Kaspersky, siber açıdan güvenli kullanıcı davranışının neye benzediğini bilir. İçgörülerimizi ve uzmanlığımızı kullanarak, müşterilerimizin çalışanlarını saldırılara karşı bağışık hâle getirirken onlara kısıtlamalar olmadan hareket etme özgürlüğü vermek için öğrenme teknikleri ve yöntemleri ekledik.

Farklı kuruluş seviyeleri için farklı eğitim formatları



* "IT Security Economics 2021" Raporu, Kaspersky

** Cybersecurity threats trends 2021, CISCO

*** Cost of a Data Breach, 2021. IBM

Kaspersky Güvenlik Farkındalığı çözümleri

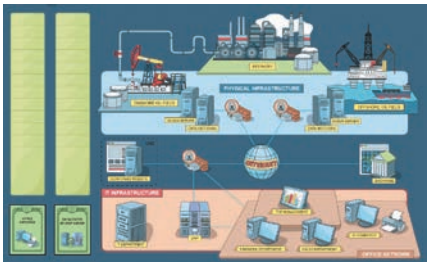
Motivasyon

Çalışanlar her zaman zorunlu eğitim konusunda istekli değildir ve konu siber güvenlik olduğunda çoğu kişi bunun çok karmaşık veya sıkıcı olduğunu düşünür veya bunlarla hiçbir ilgisi olmadığına inanır. Öğrenme motivasyonu olmadan öğrenme sonucunun çok olumlu olması olası değildir. Eğitimden sorumlu kişiler için bir başka zorluk da, hataları şirkete herkesinki kadar pahalıya mal olsa da şirket yöneticilerini eğitime dâhil etmektir. Oyunlaştırma burada devreye girer çünkü çok ilgi çekicidir, personelinizi eğitime karşı ilk dirençlerinin üstesinden gelmeye teşvik etmenin en etkili yoludur.

%70
oranında öğrenilen bilgi
geleneksel eğitim biçimlerinde bir gün içinde unutuluyor

%42 oranında katılımcı (1000'den fazla çalışana sahip şirketlerde çalışan)
katıldıkları eğitim programlarının çoğunun yararsız olduğunu ve ilgilerini çekmediğini söyledi**

KIPS eğitimi üst düzey yöneticilerin, iş sistemleri uzmanlarının ve BT uzmanlarının her türlü BT sistemi ve sürecini kullanmaya ilişkin riskler ve zorluklarla ilgili farkındalıklarını artırmayı hedefler.



Kaspersky Interactive Protection Simulation (KIPS): Bir işletmenin gözünden siber güvenlik

KIPS, karar makamları (kıdemli iş, BT ve siber güvenlik görevlileri) arasında bir anlayış oluşturan ve siber güvenlik algılarını değiştiren 2 saatlik etkileşimli bir takım oyunudur. Kötü amaçlı yazılımların ve diğer saldırıların işletme performansı ve geliri üzerindeki gerçek etkisine ilişkin bir yazılım simülasyonu sunar. Oyuncuları stratejik düşünmeye, bir saldırının sonuçlarını tahmin etmeye, zaman ve para kısıtlamaları dâhilinde buna göre yanıt vermeye zorlar. Her karar, tüm iş süreçlerini etkiler; temel amaç, işlerin sorunsuz şekilde yürümesini sağlamaktır. Oyunu en fazla gelirle bitiren, siber güvenlik sistemindeki tüm tuzakları bulup analiz eden ve uygun şekilde müdahale eden takım kazanır.

13 endüstriyel senaryo
(sürekli ekleme yapılıyor)

Her senaryo, siber güvenliğin iş sürekliliği ve kârlılık açısından rolünü ortaya koymakta, ortaya çıkan zorlukları, tehditleri ve kuruluşların siber güvenliklerini oluştururken yaptıkları tipik hataları vurgulamaktadır. Ayrıca siber tehditlere karşı istikrarlı operasyonların ve sürdürülebilirliğin korunmasına yardımcı olan satış ve güvenlik ekipleri arasındaki iş birliğini de teşvik eder.

Senaryoların özelleştirilmesi

2022 yılının 3. çeyreğinden itibaren seçilen endüstriyel senaryolar için şirketler, farklı saldırılarla kendi oyun senaryolarını oluşturabilecekler. KIPS kurumsal lisansına sahip şirketler, farklı saldırı kombinasyonları kullanarak aynı endüstriyel senaryoyu birden çok kez oynayabilir.

KIPS Sanal Gerçeklik

KIPS Enerji Santrali Sanal Gerçekliği, bir enerji tesisinin gerçek operasyonlarına mümkün olduğunca yakın gerçekçi bir ortamda yeni ve sürükleyici bir deneyimdir. Bu teknoloji, yöneticilerin bilgi güvenliği uzmanları olarak "çalışmasına", siber güvenliğin rolünü ve iş üzerindeki etkisini görsel olarak göstermesine olanak tanır; böylece BT kararlarının sonuçlarını yalnızca soyut bir fikirden ziyade son derece gerçekçi 3B grafiklerle görebilirler.

Başlangıç noktası

İnsanlar genellikle yetersizlik düzeylerinin farkında değiller ve bu da onları özellikle savunmasız hâle getiriyor. Diğer eğitimlerin etkili olabilmesi için teste tabi tutulmaları ve siber güvenlik yeterlilik düzeyleri hakkında ayrıntılı ve net geri bildirim almaları gerekir. Bu, aşina olunan materyallerde zaman kaybedilmemesini de sağlar.

Öğrenme

Çevrimiçi öğrenme platformumuz, farkındalık programının temelini oluşturur. **300'den fazla siber güvenlik becerisi** ile tüm önemli BT güvenliği konularını kapsar.
Her ders vakalar ve gerçek hayattan örnekler içerir, böylece çalışanlar günlük işlerinde başa çıkmak zorunda oldukları şeylerle bağlantı kurabilirler. Ayrıca bu becerileri ilk dersten hemen sonra kullanabilirler.

Kaspersky ASAP: çalışanların siber güvenlik becerilerini seviye seviye geliştiren, yönetimi kolay çevrimiçi araç

ASAP'de ele alınan konular:

- Parolalar ve Hesaplar
- E-posta
- Web Siteleri ve İnternet
- Sosyal Medya ve Mesajlaşma Uygulamaları
- Bilgisayar Güvenliği
- Mobil Cihazlar
- Gizli verileri koruma
- GDPR
- Endüstriyel Siber Güvenlik

ASAP Hızlı kurs

Eğitimin ses-görüntü formatında kısa bir sürümü.

- Etkileşimli teori
- Videolar
- Testler

Kaspersky ASAP, çok dilli bir çözümdür.

Oyunlaştırılmış Değerlendirme Aracı: çalışanların siber güvenlik becerilerini değerlendirmenin hızlı ve heyecan verici yolu

Kaspersky Oyunlaştırılmış Değerlendirme Aracı (GAT), çalışanlarınızın siber güvenlik bilgi düzeylerini hızlı bir şekilde tahmin etmenize olanak tanır. İlgi çekici interaktif yaklaşım, klasik değerlendirme araçlarında sıklıkla görülen sıkılma hâlini ortadan kaldırır. Çalışanların 15 dakika içinde siber güvenlikle ilgili 12 günlük durumu gözden geçirmeleri, karakterin eylemlerinin riskli olup olmadığını değerlendirmeleri ve müdahalelerindeki güven düzeyini ifade etmeleri gerekir.

Tamamlandıktan sonra kullanıcılar, siber güvenlik farkındalığı düzeylerini yansıtan bir puana sahip bir sertifika alırlar. Ayrıca açıklamalar ve faydalı ipuçları ile her alan hakkında geri bildirim alırlar.

GAT'nin oyunlaştırılmış yaklaşımı, çalışanları motive ederken aynı zamanda belirli siber güvenlik durumlarını çözmelerini sağlayarak bilgilerinde boşluklar olabileceğini de gösterir. Bu aynı zamanda BT/İK departmanlarının kuruluşlarındaki siber güvenlik farkındalığı düzeylerini daha iyi anlamaları için faydalıdır ve daha geniş bir eğitim kampanyasına giriş aşaması olarak işlev görebilir.

Kaspersky Otomatik Güvenlik Farkındalığı Platformu: her ölçekten kuruluş için verimlilik ve eğitim yönetimi kolaylığı

Kaspersky ASAP, çalışanların siber güvenlik becerilerini şekillendiren ve onları doğru şekilde davranmaya motive eden etkili ve kullanımı kolay bir çevrimiçi araçtır.

Eğitim tüm şirketlerin güvenlik farkındalığı gereksinimlerini karşılasa da, otomatikleştirilmiş yönetim öncelikle özel eğitim yönetimi kaynaklarına sahip olmayanlara hitap edecektir.

Temel avantajlar:

- **Tam otomasyon sayesinde basitlik:** Programın başlatılması, yapılandırılması ve izlenmesi çok kolaydır, sürekli yönetim tamamen otomatikleştirilmiştir ve yönetici müdahalesi gerektirmez. Platform, her çalışan grubu için bir eğitim programı oluşturarak öğrenim modülleri, e-posta güçlendirme, testler ve kimlik avı saldırısı simülasyonları dâhil bir dizi eğitim formatı aracılığıyla otomatik olarak sunulan aralıklı öğrenme sağlar.
- **Yeterlik:** Program içeriği, sürekli pekiştirme ile artan aralıklı öğrenmeyi destekleyecek şekilde yapılandırılmıştır. Metodoloji, bilginin akılda tutulmasını ve sonraki becerilerin uygulanmasını sağlamak için insan hafızasının inceliklerine dayanmaktadır.
- **Esnek öğrenme:** Size uygun çalışan eğitimi seçeneğini belirleyin: Çalışanlara siber güvenlik eğitimine yönelik yasal gereklilikleri hızla karşılamanıza veya bilgilerini güncellemenize yardımcı olacak basit bir Hızlı kurs atayın veya daha ayrıntılı ve kapsamlı siber güvenlik becerileri gelişimi için karmaşıklık düzeylerine ayrılmış bir Temel kurs seçin.
- **Esnek lisanslama** (Yönetilen Hizmet Sağlayıcıları için): Kullanıcı başına lisanslama modeli en az 5 lisanstan başlayabilir.

ASAP, MSP'ler ve xSP'ler için idealdir; birden fazla işletme için eğitim hizmetleri tek bir hesap üzerinden yönetilebilir ve aylık lisans abonelikleri mevcuttur.

Kaspersky ASAP'nin tam işlevsel sürümünü asap.kaspersky.com adresinden deneyin; kendi kurumsal güvenlik farkındalığı eğitim programınızı oluşturmanın ve yönetmenin ne kadar kolay olduğunu kendiniz görün!

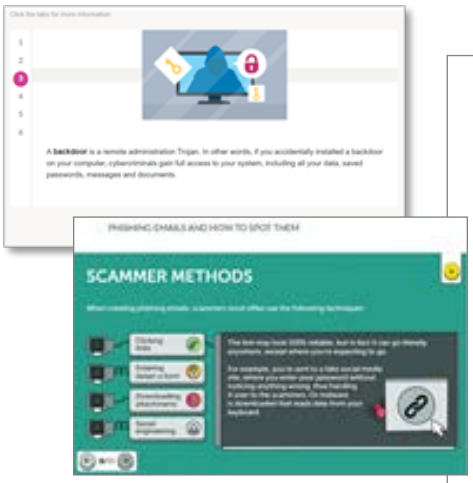
Temel kurs

Hızlı kurs

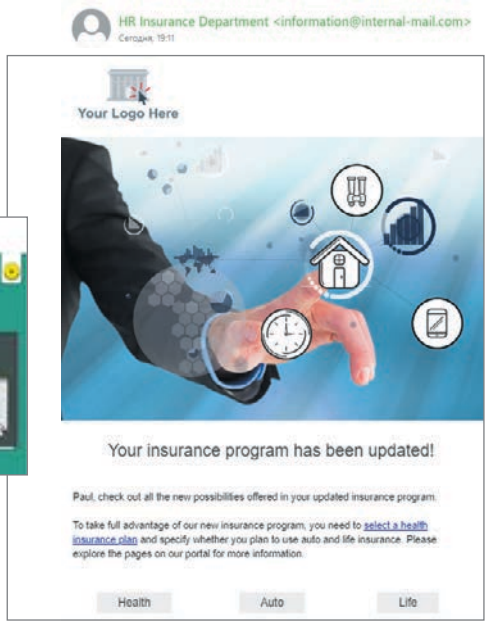
Temsili kimlik avı kampanyaları

Kimlik avı saldırısı simülasyonları, çalışanların siber saldırılara direnme becerilerini test edip onlara yardım etmek ve şirket yönetiminin eğitimin faydalarını görmesini sağlamak için eğitim öncesinde, sırasında ve sonrasında kullanılabilir.

Etkileşimli dersler



Kimlik avı saldırısı simülasyonları



Sonuçları takip edin

Panodan çalışanların ilerlemesini takip edebilir, tüm şirketin ve tüm grupların ilerlemesini tek bakışta değerlendirebilirsiniz. Bireysel seviyede de daha fazla ayrıntı edinebilirsiniz.

Güçlendirme

Güçlendirme, öğrenme programının önemli bir parçasıdır ve öğrenme sırasında kazanılan bilgi ve becerileri pekiştirmek için gereklidir.

Öğrenilen becerileri alışkanlıklara dönüştürmenin en iyi yolu uygulamaya koymaktır. Aynı zamanda insanlar bazen hata yapar ve kişisel deneyimlerinden ders alırlar. Ancak konu siber güvenlik olduğunda, kendi hatalarınızdan ders çıkarmak çok pahalıya mal olabilir.

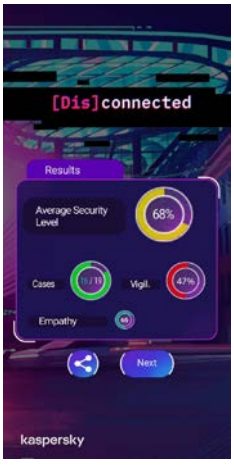
Oyunlaştırılmış eğitim yoluyla kendinize veya şirketinize herhangi bir zarar vermeden bir durumu "yaşayabilir" ve sonuçlarını deneyimleyebilirsiniz.

[Dis]connected: mobil siber güvenlik görevi

[Dis]connected, kullanıcıları sağlıklı bir iş-yaşam dengesi kurma ve hem kişisel hem de profesyonel hayatlarında başarılı olma arayışına davet eden son derece sürükleyici ve hikâye bakımından zengin görsel roman niteliğinde bir mobil siber güvenlik oyunudur.

Siber güvenlik unsurları oyunun hikâyesine yedirilmiştir ve oyun, siber güvenlikle ilgili kararlarımızın hedeflere ulaşmaya veya bu hedefleri bozmaya nasıl yardımcı olabileceğini ortaya koymaktadır. Parolalar ve hesaplar, e-posta, web'de gezinme, sosyal ağlar ve mesajlaşma uygulamaları, bilgisayar güvenliği ve mobil cihazlar dâhil olmak üzere çözülmesi gereken 24 vaka vardır. Mesajlaşma ve bankacılık uygulamaları gibi yerleşik benzetimli uygulamalar, kapsamlı bir sürükleyici deneyim sunar.

Oyunun sonunda oyuncular, projeyle ne kadar başarılı bir şekilde başa çıktıklarına dair özet niteliğinde bilgi edinirler ve güvenlik becerilerinin bugün ve yarın için yeterli olup olmadığını öğrenirler.



Oyun, cep telefonlarında çalışır. Google Play ve App Store'da **ücretsiz bir deneme sürümü** mevcuttur: https://kas.pr/mobilestores

Gelişmiş öğrenim

Genel BT uzmanları: Yardım masaları ve diğer teknik açıdan bilgili personel, standart farkındalık programları onlar için yeterli olmadığından genellikle eğitimin dışında bırakılır ancak şirketlerin onları siber güvenlik uzmanlarına dönüştürmesine de gerek yoktur: Çok pahalı, zaman alıcı ve gereksizdir.

Bu boşluğu dolduran eğitimi duyurmaktan mutluluk duyuyoruz; uzman eğitimi kadar kapsamlı değildir, sıradan çalışanlara yönelik eğitimden daha ileri düzeydir.

CITO eğitimi modülleri:

- Kötü amaçlı yazılım
- Potansiyel olarak istenmeyen programlar ve dosyalar
- Araştırma temelleri
- Kimlik avı olay müdahalesi
- Sunucu güvenliği
- Active Directory Güvenliği

CITO gönderim yöntemi:
Bulut veya SCORM formatı

CITO modüllerinden birini ücretsiz olarak deneyin: cito-training.com

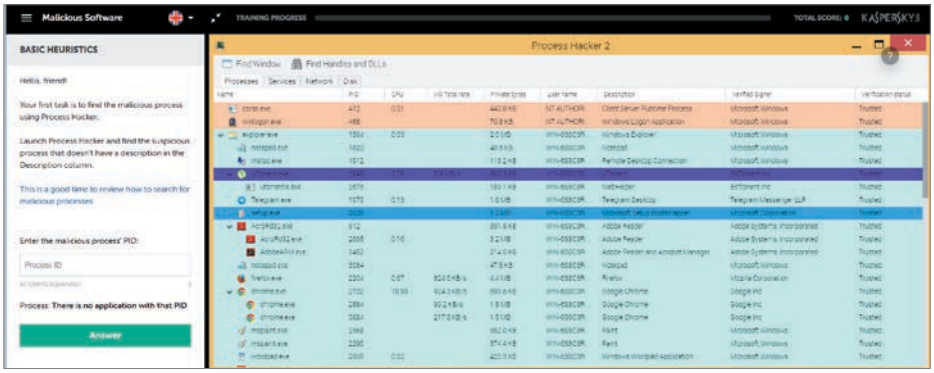
Cybersecurity for IT Online: Olay savunmasının ilk hattı

Cybersecurity for IT Online, BT ile ilgilenenlere yönelik etkileşimli bir eğitimdir. Güçlü siber güvenlik ve birinci seviye olay müdahalesi becerileri geliştirir.

Program, BT uzmanlarına görünüşte iyi huylu bir bilgisayar olayında olası bir saldırı senaryosunu tanımak üzere pratik beceriler kazandırır. Aynı zamanda tüm BT ekibi üyelerinin güvenlik savunmasının ilk hattı olarak rolünü güçlendirerek kötü amaçlı belirtileri bulmaya teşvik eder.

CITO ayrıca, BT uzmanlarınıza teorik, pratik ve alıştırmaya dayalı beceriler kazandırarak BT güvenliğine verilecek olay verilerini toplamalarına olanak sağlamak için BT güvenlik araçlarının ve yazılımlarının nasıl kullanılacağını ve araştırma temellerini öğretir.

Bu eğitim, başta hizmet masaları ve sistem yöneticileri olmak üzere kuruluşunuzdaki tüm BT uzmanları için önerilir. Uzman olmayan çoğu BT güvenliği ekip üyesi de bu kurstan yararlanabilir.



Üst düzey yöneticiler, siber suçlular için en çok arzu edilen hedefler arasındadır ancak genellikle eğitimciler için gerçek bir zorluk teşkil ederler. Ancak çeşitli siber güvenlik girişimlerine ve savunmalarına katılımları ve destekleri olmadan kuruluşta bir siber güvenlik kültürü oluşturmak imkânsızdır.

Siber güvenlik; proje yönetimi, finansal araçlar ve işletmenin operasyonel verimliliği ile birlikte gelir yaratmanın önemli bir unsurudur. Bu, yöneticiler için kursumuzun odak noktasıdır.

Yönetici eğitimi: dijital dönüşüm için iş esnekliğini artırma

İşletme liderleri ve üst düzey yöneticiler, siber tehditleri ve bunlara karşı nasıl korunulacağını daha iyi anlamalarını sağlayan, eğitmen liderliğindeki bir kurs aracılığıyla siber güvenlikle ilgili temel bilgileri öğrenirler.

Araştırmalar, olay müdahalesinin hızı ve verimliliği ile bir olayın neden olabileceği hasarın derecesi arasında doğrudan bir bağlantı olduğunu göstermektedir. Kurs, özellikle siber güvenliğin finansal yönlerine ve buna yatırım yapmanın fizibilitesine önem vererek C seviyesi yöneticilerinizin siber güvenlik ve iş verimliliği arasındaki bağlantıyı daha iyi anlamalarını sağlar.

Kaspersky Interactive Protection Simulation (KIPS), uygulamalı alıştırmalar yoluyla materyali daha da pekiştirmek için bu eğitime ek olarak kullanılabilir.

Kursun hedefleri

- Modern siber tehditler ve işletmeye yönelik riskleri hakkında en güncel bilgileri paylaşmak
- Eğitimi alan kişileri modern siber tehdit alanı ile ilgili bilgilendirmek
- Kurumsal ve kişisel siber güvenlik kültürünün temel kurallarını uygulama fırsatı sağlamak
- Bilgi güvenliği alanındaki temel düzenleme sorunlarının işletme üzerindeki etkisinin anlaşılmasını sağlamak
- Siber güvenliğin temel kavramlarını ve hedefli saldırılara karşı korunma yöntemlerini netleştirmek
- Şirket politikası için pratik önerilerde bulunmak
- Olaylara müdahale etme ve olayları araştırma için iletişim konusunda tavsiye vermek

Kaspersky Güvenlik Farkındalığı: esnek eğitim yöntemleri

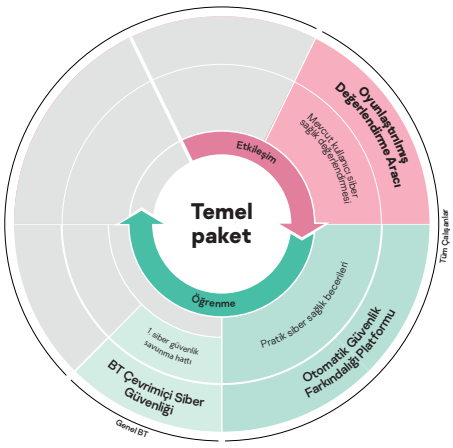
Kaspersky eğitim çözümleri, şirketinizin her düzeyini kapsar ve tek başına veya toplu olarak kullanılabilir. Ayrıca ihtiyaçlarınıza göre hazırlanmış paketleri kullanmaya başlamanızı da kolaylaştırıyoruz.

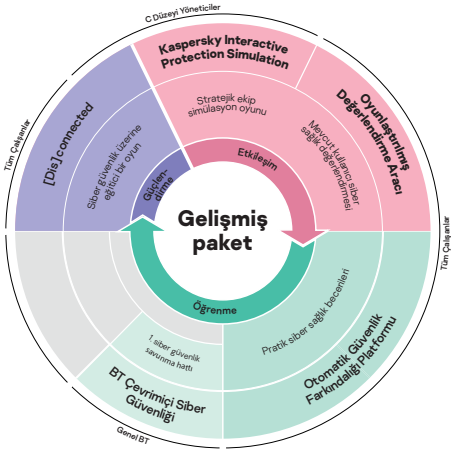
Çalışanların siber güvenlik farkındalığını artırmak için zahmetsiz bir seçenek. Kurulumu kolay, yönetimi kolay.

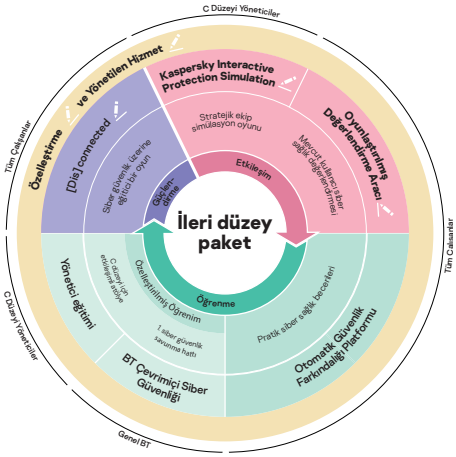
Başarılı bir şekilde çalışmanıza ve genel siber güvenlik eğitimi için düzenleyici gereksinimleri veya üçüncü taraf gereksinimlerini karşılamanıza yardımcı olacak temel düzeyde bir güvenlik eğitimi sağlar.

Basit bir "eksiksiz" eğitim çözümü kullanarak daha büyük kuruluşların iş sürekliliğini sürdürmesine yardımcı olur. Öğrenme döngüsünün her aşamasını kapsayarak her kuruluş seviyesini destekler ve davranışı değiştirir.

Yöneticilerin tehdit senaryoları hakkında yeterli bilgi sahibi olması, çalışanların otomatik siber güvenlik becerilerine sahip olması ve genel BT personelinin ilk savunma hattı olarak sizi desteklemesi için özelleştirme ve yönetilen hizmetler içeren maksimum siber güvenlik farkındalığı sağlar.







Kaspersky Güvenlik Farkındalığı eğitimi, başarıyı sağlamak için en son eğitim yöntemlerini ve gelişmiş teknikleri kullanır. Esnek yeni paket çözümler ihtiyaçlarınıza göre uyarlanabilir, dolayısıyla herkes için bir çözüm vardır. kaspersky.com/awareness adresini ziyaret ederek daha fazla bilgi alın

Kaspersky Güvenlik Farkındalığı: kaspersky.com.tr/awareness
BT Güvenliği Haberleri: business.kaspersky.com

kaspersky.com.tr

kaspersky GELECEĞİ YAKALAYIN