Genel BT uzmanları için Birinci Seviye Olay Müdahalesi (First-line Incident Response) eğitimi

BT Çevrimiçi Siber Güvenlik Eğitimleri

Ücretsiz deneme
cito.kaspersky.com

kaspersky GELECEĞİ YAKALAYIN

Kaspersky Cybersecurity for IT Online

BT Çevrimiçi Siber Güvenliği (CITO eğitimi)

Genel BT uzmanları için güçlü siber güvenlik ve birinci seviye olay müdahalesi becerileri geliştiren etkileşimli eğitim

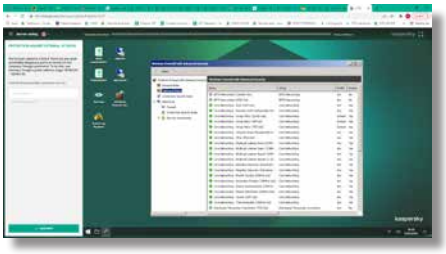
Güçlü bir kurumsal siber güvenlik duruşu oluşturmak, ilgili tüm çalışanlara konu hakkında sistematik eğitimler vermeden mümkün değildir. Çoğu işletme iki seviyede siber güvenlik eğitimi ve öğretimi sağlamaktadır: BT güvenlik ekipleri için uzmanlık eğitimi ve BT dışı çalışanlar için güvenlik farkındalığı. Kaspersky her ikisi için de kapsamlı bir takım ürünler sunar. Bu durumda eksik kalan nedir? BT ekipleri, hizmet masaları ve teknik açıdan gelişmiş diğer personel için standart farkındalık programları yeterli değildir. Ancak, bu kişilerin birer siber güvenlik uzmanına dönüşmesine de gerek yoktur – böyle bir süreç çok pahalı ve zaman alıcı olacaktır.

Eğitim formatı

Eğitim tamamen çevrimiçidir. Eğitime katılanların sadece internete erişimlerinin olması ve bilgisayarlarında Chrome arama motorunun yüklü olması yeterlidir. 6 modülün her biri kısa bir teorik genel bakış, pratik ipuçları ve öğrencilere günlük işlerinde BT güvenlik araçlarını ve yazılımlarını nasıl kullanacaklarını öğreten belli başlı becerileri kapsayan 4 ila 10 alıştırmadan oluşmaktadır.

Eğitimin bir yıla yayılması amaçlanmıştır. Önerilen ilerleme hızı haftada 1 egzersiz şeklindedir – her egzersizin tamamlanması 5 ila 45 dakika sürer.

Eğitimin mevcut sürümü Windows kurumsal ortamını hedeflemektedir.



Eğitimin veriliş yöntemi:
Bulut veya SCORM formatı

Birinci Seviye Olay Müdahalesi

Kaspersky, genel kurumsal BT uzmanları için piyasada bir ilk niteliğindeki çevrimiçi beceri eğitimini başlatıyor. Eğitim, 6 modülden* oluşmakta:

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

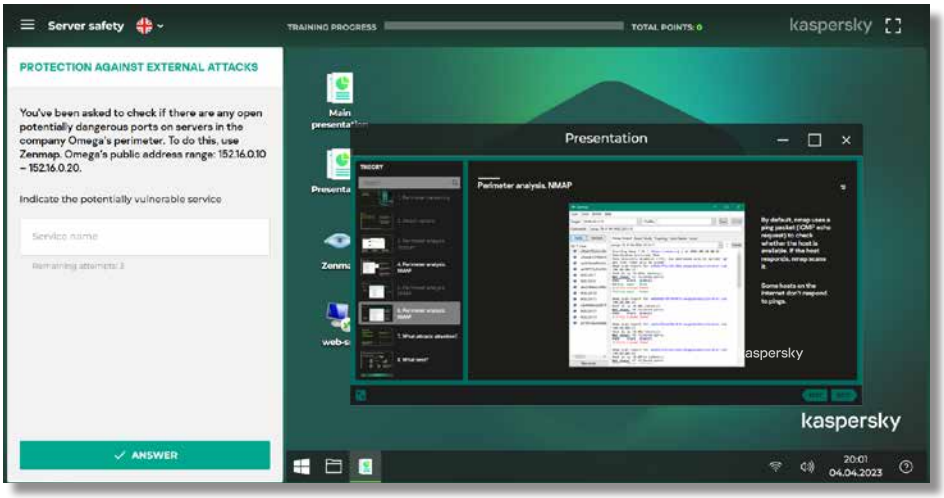
Program, BT uzmanlarını, zararsız görünen bir olay sırasında yaşanabilecek olası bir saldırı senaryosunu nasıl tanıyabilecekleri ve böyle bir olayı BT güvenliği ekibine devretmek için olay verilerini nasıl toplayacakları konusunda pratik becerilerle donatır. Aynı zamanda, tüm BT ekibi üyelerinin güvenlik savunmasının ilk hattı olarak oynadıkları rolü vurgulayarak BT ekibi üyelerini kötü amaçlı faaliyetlerin belirtilerini bulma konusunda daha dikkatli olmaya teşvik eder.

CITO eğitimi neden etkilidir?

- İnteraktif: bilgisayar için herhangi bir risk oluşturmadan gerçek süreçler simüle edilir
- Bilginin yanı sıra beceri de kazandırır: yaparak öğrenme
- Sezgisel öğrenme süreci: güvenilir navigasyon ve ipuçları
- Genel BT personelinin iş yerlerinde karşılaştığı tüm ana BT güvenliği konularını ve sorunlarını kapsar

Öğrenme süreci

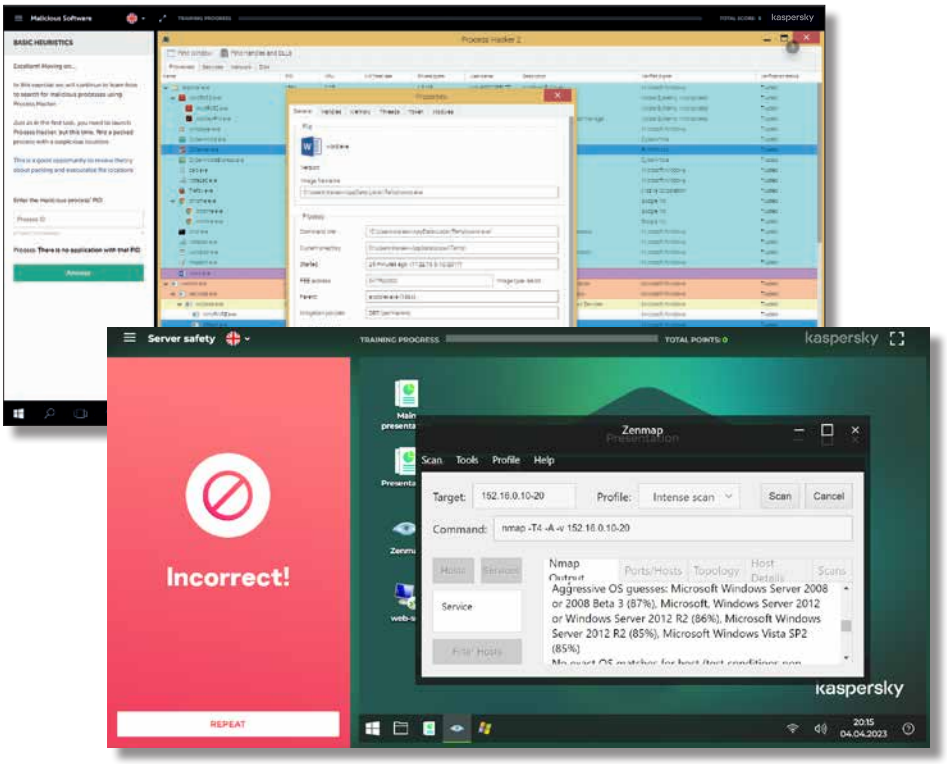
Her bir öğrenme alıştırması bloğu iki bölümden oluşur: eğitim ve eğitimde açıklanan gerçek süreçleri simüle eden görevler üzerinden gerçekleştirilen uygulamalar.



* güncel konu listesi için lütfen cito.kaspersky.com adresini inceleyin

Dersi bitirdiğinizde lütfen görevi tamamlayın

Eğer iyi bir performans gösterdiyseniz, bir sonraki alıştırma bloğuna yönlendirilirsiniz. Eğer performansınız çok iyi değilse, ipuçlarını kullanabilir veya bilgilerinizi tazelemek için ders materyalini tekrar okuyabilirsiniz

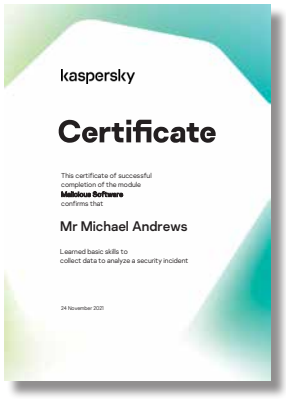


Bu eğitim kimler için?

Bu eğitim, başta hizmet masaları ve sistem yöneticileri olmak üzere kuruluşunuzda görev yapan tüm BT uzmanları için önerilmektedir. Uzman olmayan çoğu BT güvenliği ekibi üyesi de bu kurstan yarar sağlayacaktır.

Sertifikalar

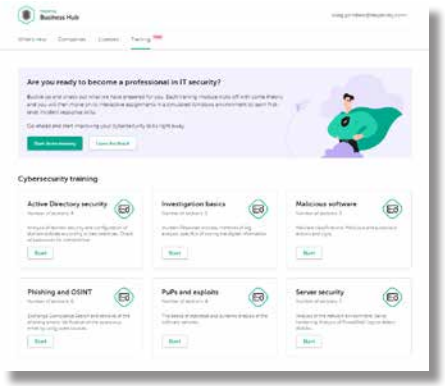
Çalışanlar, her bir modülü tamamlamalarının ardından kişisel sertifikalarını alabilir



Eğitim konuları ve eğitimin hedefleri

Modül adı	Hedef kitle	Edinilen bilgiler	Kişisel tavır	Edinilen beceriler	Modül kapsamında gerçekleştirilen uygulamalar
Kötü Amaçlı Yazılım	Sunucularda ve/veya iş istasyonlarında yönetici haklarına sahip kullanıcılar	Kötü amaçlı yazılım teknikleri ve sınıflandırması Kötü amaçlı ve şüpheli yazılım eylemleri ve belirtileri Sezgisel analiz temelleri	Kötü amaçlı yazılımlar bilgisayarın herhangi bir yerinde bulunabilir Kötü amaçlı yazılımlar hiç de hafife alınmaması gereken birçok farklı yolla verilerinizi çalabilir Bu sebeple, potansiyel tüm şüpheli olayların güvenlik ekibine bildirilmesi zorunludur	Kötü amaçlı yazılımlarla ilgili bir olay yaşanıp yaşanmadığının doğrulanması	Kötü amaçlı yazılımları tespit etmek için ProcessHacker, Autoruns, Fiddler ve Gmer araçlarının kullanılması

Modül adı	Hedef kitle	Edinilen bilgiler	Kişisel tavır	Edinilen beceriler	Modül kapsamında gerçekleştirilen uygulamalar
Çoğunlukla istenmeyen programlar ve dosyalar (PuPs)	Ek yazılım yükleme hakkına sahip kullanıcılar ve dışarıdan gelen dosyaları aktif olarak değerlendiren/açan kullanıcılar	Yazılım örnekleri ve şüpheli belgelerin istatiksel ve dinamik analizinin temelleri	Belgeleriniz (pdf, docx) güvenlik açıkları içerebilir İmzalanmamış dosyalar kötü amaçlı yazılım veya riskli yazılımlar içerebilir Yürütülebilen imzalanmamış tüm dosyalar kötü amaçlı ve riskli yazılımlara karşı kontrol edilmelidir Dijital imza, bir dosyanın kötü amaçlı işlevler içermediğini garanti etmez	Sistem ve sandbox olay monitörleri ile çalışma İstatiksel motorları kullanma Potansiyel olarak istenmeyen programlar ve dosyaları (PuPs) kaldırma	Yazılım örneklerinin statik (imza) ve istatistiksel (virustotal) analizi Yazılımların güvenlik açıklarını ve kötü niyetli davranışlarını bulmak için procmon'u kullanma Cuckoo sandbox ile dosya analiz etme AVZ kullanarak kötü amaçlı yazılımları kaldırmak için komut dosyaları oluşturma
Araştırma temelleri	Adli tıp incelemelerine veya güvenlik ekibi tarafından yönetilen olay müdahale faaliyetlerine destek veren BT çalışanları	Olay Müdahalesi süreci Günlük analizi yöntemleri Dijital bilgileri depolama özellikleri	Eğer bir siber güvenlik olayından şüpheleniyorsanız, derhal güvenlik ekibine bildirin ve dijital kanıt toplayın Analiz, güvenlik ekibinin gözetimi altında ve güvenlik ekibiyle işbirliği içinde yapılmalıdır	Dijital kanıt toplama NetFlow trafiği analizi Zaman çizelgesi analizi Olay günlüğü analizi	Uçucu ve uçucu olmayan verilerin toplanması (FTK-imager) Saldırının kaynağının ve bağlantılarının bulunması için günlük analizlerinin gerçekleştirilmesi (eventlogexplorer) NetFlow analizi ile yanal hareket araştırması (ntop) Autopsy kullanarak diskin analiz edilmesi
Kimlik Hırsızlığı ve Açık kaynak istihbaratı (OSINT)	Adli tıp incelemelerine veya olay müdahale faaliyetlerine destek veren BT çalışanları	Modern kimlik hırsızlığı yöntemleri E-posta başlıkları için analiz yöntemleri	Kimlik avı çok karmaşık olabilir, bu sebeple fark edilmesi zordur. Ancak, kimlik avı, manüel araştırma ile her zaman tespit edilebilir Kimlik avı e-postalarının kullanıcıların posta kutularından silinmesi gerekir	Kimlik avı e-posta analizi ve değiştirilerek gizlenmiş kimlik avı e-postalarının kullanıcıların posta kutularından silinmesi Korsanların şirketiniz hakkında ne bildiğini anlamak için açık kaynak istihbaratı	Exchange Posta Kutusundaki kimlik avı e-postalarının aranması ve kaldırılması İnternet keşfi için Recon-ng kullanımı
Sunucu güvenliği	Sunucu yöneticileri	Ağ ortamını analiz etme Sunucu güçlendirme Saldırıları tespit etmek için PowerShell günlüklerini analiz etme	Ağ çevresinin tehlikeye atılması en önemli saldırı vektörlerinden biridir. Tüm güvenlik açıklarını kapatmak imkansızdır – bir saldırının başarılı olmasını olabildiğince engellemek istiyorsanız saldırıya açık yüzeyleri azaltmanız gerekir. Böyle yapmanız, korsanları durdurmasa bile tespit edebilmeniz için size zaman kazandıracaktır.	Savunmasız ve standartlara uymayan ağ hizmetlerini arayın Sistemleri, 'varsayılan reddetme' ilkesine göre yapılandırın PowerShell günlüklerinde saldırı işaretlerini arayın	Savunmasız ağ hizmetlerini bulmak için Nmap kullanın Program denetimi için Yazılım Kısıtlama İlkelerini, ağ denetimi için Windows Güvenlik Duvarı'nı yapılandırın Event Log Explorer ile güvenlik olaylarını analiz edin
Active Directory Güvenliği	Active Directory yöneticileri	Ele geçirilen parola veri tabanında parolaları kontrol etmek için bir API kullanma Önerilere göre etki alanı ilkelerini yapılandırma Active Directory etki alanı güvenliğini analiz etme yöntemleri	Güvenlik açısından bakıldığında, varsayılan Active Directory yapılandırması en ideal yapılandırma değildir. Saldırgan, varsayılan yapılandırma karşısındaki üstünlüğünü birçok şekilde arttırabilir. Güvenlik önerilerini inceleyin, Active Directory için daha çok görünürlük sağlayan araçlar kullanın	Bir veri tabanındaki parola karmaşıklıklarını güvenli bir şekilde kontrol edin Önerilen ve gerçekteki alan (domain) politikaları arasındaki tutarsızlıkları arayın Active Directory ayarlarının güvenliğini değerlendirme	Have I Been Pwned?'ı kullanın Veri tabanında ele geçirilmiş parolaları aramak için API Mevcut alan politikalarını en iyi uygulamalarla karşılaştırmak için Policy Analyzer'ı kullanın Ping Castle raporlarını kullanın



Temel program farklılıkları

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

Kuruluşunuzun her düzeyinde çalışanların davranışlarını değiştiren eğitim
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 Endpoint Security Cloud ile entegrasyon

KES Cloud Pro kullanıcılarının doğrudan Business Hub üzerinden erişebileceği CITO eğitimi ile siber güvenlik becerilerinizi geliştirin ve özel siber güvenlik ürünlerinden en iyi şekilde yararlanın.

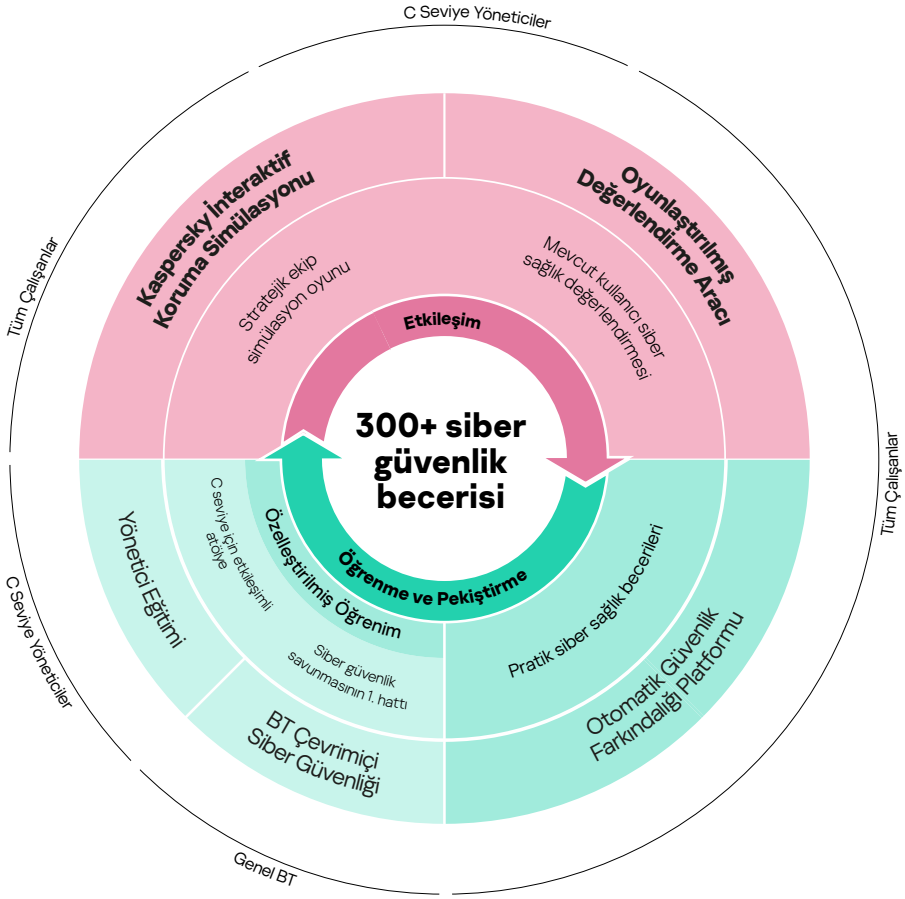
Kaspersky Security Awareness – BT güvenliği becerilerinde uzmanlaşmak için yeni bir yaklaşım

Herkes için tek bir esnek eğitim çözümü

Kaspersky Security Awareness'ın uluslararası başarı geçmişi, uzun yıllara dayanmaktadır. 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 yetişkin eğitimindeki kapsamlı deneyimiyle bir araya getiriyor.

Portföy, her seviyedeki çalışanınızın siber güvenlik farkındalığını arttıracak ve onlara kuruluşunuzun genel siber güvenliğinde kendilerine düşen rolü oynamaları yönünde öz güven kazandıracak ilgi çekici bir eğitim seçeneği yelpazesi sunmaktadır.

Davranışlardaki sürdürülebilir değişiklikler zaman aldığından yaklaşımımız, birden fazla bileşene sahip 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.



Kurumsal Siber Güvenlik: www.kaspersky.com/enterprise
Kaspersky Güvenlik Farkındalığı: www.kaspersky.com.tr/awareness
Çevrimiçi BT için Kaspersky Cybersecurity: cito.kaspersky.com

www.kaspersky.com.tr

kaspersky **GELECEĞİ YAKALAYIN**

2023 AO KASPERSKY. TESCILLI TICARI MARKALAR VE HIZMET MARKALARI, ILGILI SAHIPLERINE AITTIR.