Kaspersky Endüstriyel Siber Güvenlik Eğitimi ve Farkındalık Programları

www.kaspersky.com/ics
#truecybersecurity

Kaspersky Endüstriyel Siber Güvenlik Eğitimi ve Farkındalık Programları

Bu yenilikçi eğitim programları aracılığıyla Kaspersky Lab'in Endüstriyel Siber Güvenlik bilgilerinden, deneyimlerinden ve tehdit istihbaratından faydalanın.

Siber güvenlik olaylarının %80'i insan hatasından kaynaklanmaktadır. Bu olaylar kritik sistemlerin arızalanmasına ve endüstriyel süreçlerin durmasına yol açtığında insan hatası, pahalı hatta ölümcül sonuçlara neden olabilir.

Tehdit ortamının sürekli olarak geliştiği ve insanların zayıflıklarından faydalanan hedefli saldırıların arttığı bir ortamda en önemli savunma aracınız, siber açıdan güvenli uygulamaları kendiliğinden ve içgüdüsel olarak uygulayan çalışanlarınızdır.

Bunu başarmak için çalışanlarınız, tehlikelerle ilgili temel bilgilere sahip olmalı ve nasıl güvenli bir şekilde çalışacağını bilmelidir. Ayrıca doğrudan BT/OT siber güvenlik alanlarında çalışanlar, önleme ve tespit becerilerinin yanı sıra etkili tehdit yönetimi ve risk azaltma konusunda gelişmiş becerilere sahip olmalıdır.

Kaspersky Industrial CyberSecurity Training and Awareness kursları, kritik altyapı operatörleri, hizmet sağlayıcıları ve üretim işletmelerinin endüstriyel ortamlarını, siber olayların ve saldırıların neden olduğu kesintilere ve hasarlara karşı daha iyi koruyabilmeleri için özel olarak geliştirilmiştir.

Kurslar (Tüm eğitim kursları İngilizce olarak sunulur)

<table>
<tr><th>Siber Güvenlik Farkındalığı</th><th colspan="2">Siber Güvenlik Becerileri Geliştirme ve Eğitim</th></tr>
<tr><td>Mühendisleriniz/
Endüstriyel Üretim Çalışanlarınız İçin:</td><td>BT/OT Uzmanları İçin:</td><td>BT/OT Güvenlik Uzmanları İçin:</td></tr>
<tr><td>Temel Siber Güvenlik</td><td rowspan="3">Gelişmiş Endüstriyel
Endüstriyel Siber Güvenlik</td><td>Uzmanlar İçin ICS Sızma Testi</td></tr>
<tr><td>Yönetim için:</td><td rowspan="2">Uzmanlar İçin ICS Adli Bilişim</td></tr>
<tr><td>Endüstriyel Siber Güvenlik Oyunları</td></tr>
</table>

Endüstriyel Siber Güvenlik Farkındalığı

Endüstriyel üretim, kontrol odası veya arka ofis dahil olmak üzere endüstriyel bilgisayarlı sistemlerle etkileşim kuran tüm çalışanlar ve yöneticileri için yerinde ve çevrimiçi interaktif eğitim modülleri ve siber güvenlik oyun eğitimi.

Kuruluşlar, siber güvenlik farkındalık programlarına milyonlarca lira harcamasına rağmen çok az sayıda Bilgi Güvenliğinden Sorumlu Yönetici sonuçlardan memnundur. Peki bu memnuniyetsizliğin nedeni nedir?
Siber güvenlik farkındalık eğitimlerinin çoğu genele yönelik, çok uzun, çok teknik ve temelde negatif eğitimlerdir. Bu tür eğitimler insanların güçlü yönlerine, karar alma becerilerine ve öğrenme yeteneklerine hitap etmediği için eğitim sonuçları verimsiz olabilir. Ayrıca bu eğitimler, endüstriyel iş gücünün gerçek dünyada karşılaşabileceği siber güvenlik sorunlarını yansıtmaz.

Bu nedenle kuruluşlar, çalışma ortamlarına özgü sorunlara odaklanmanın yanı sıra ölçülebilir ve değerli bir yatırım getirisi sağlayan daha gelişmiş davranışsal destek yaklaşımları (kurumsal kültür geliştirme gibi) aramaktadır.

Kaspersky Lab Industrial CyberSecurity Awareness kursları şu şekilde çalışır:

- Davranışın değiştirilmesi: "Siber güvenliğe önem veriyorum, çünkü buradaki herkes önem veriyor. Siber güvenlik işimin bir parçasıdır" düşüncesini uyandıran bir kurumsal ortam oluşturarak bireyin güvenli ve sorumlu şekilde çalışma kararlılığını güçlendirme.
- Motivasyonel yaklaşımı, oyunlaştırmayı, öğrenme tekniklerini, gerçek hayatta karşılaşılan endüstriyel durumlara dayalı saldırı simülasyonlarını ve kapsamlı interaktif siber güvenlik beceri eğitimini bir araya getirir.

Ayrıntılı çalışma şekli

Kapsamlı ama basit: Eğitim, bir dizi basit alıştırma aracılığıyla temel siber hijyen kuralları, kötü amaçlı yazılım saldırıları, veri sızıntıları ve güvenli sosyal ağ kullanımı gibi çok çeşitli güvenlik sorunlarını kapsar. Öğrenme sürecini daha merak uyandırıcı ve amaca uygun hale getirmek için grup dinamikleri, interaktif modüller ve gerçek hayatta karşılaşılabilecek endüstriyel iş yeri senaryolarına dayalı oyunlar gibi öğrenme tekniklerini kullanırız.

Erişilebilir: 1 günlük Siber Güvenlik Farkındalık kursumuz, iş yerinizde veya herhangi bir mekanda gerçekleştirilebilir. Endüstriyel Siber Güvenlik Oyun programımız olan Kaspersky Industrial Protection Simulation (KIPS) ise tercihe göre çevrimiçi veya yüz yüze oynanabilir. Sürükleyici ve gerçek hayata dayalı bir öğrenme ortamı sağlamak için su arıtma, enerji üretimi veya enerji aktarımı gibi farklı endüstrilere özel KIPS versiyonları kullanılabilir.

Sürekli motivasyon: Oyunlar ve yarışmalarla öğrenme fırsatları oluştururuz ve daha sonra bu fırsatları çevrimiçi saldırı simülasyonu alıştırmaları, değerlendirmeler ve eğitim kampanyaları aracılığıyla yıl boyunca güçlendiririz.

İnançların değiştirilmesi: Çalışanlar, belirli tehditlere karşı korunmada kendi rollerinin önemini öğrenir. Bir saldırıya maruz kalmaktan nasıl kaçınabileceklerinin yanı sıra kendilerini ve iş yerlerini tehlikeden ve saldırılardan nasıl koruyabileceklerini öğrenir.

Kurumsal siber güvenlik kültürü oluşturma: Yöneticileri, güvenlik savunucuları olarak eğitiyoruz. Siber güvenliğin alışkanlık haline geldiği bir kültür, empoze edilerek değil yönetimin kararlılığıyla oluşur.

Olumlu ve işbirliğine dayalı: Güvenlik uygulamalarının genel operasyonel verimliliğe ve üretkenliğe nasıl olumlu bir katkı sağladığını gösterir ve BT/OT Güvenlik ekibi dahil olmak üzere diğer iç departmanlarla daha etkili işbirliğini teşvik ederiz.

Ölçülebilir: Günlük çalışma hayatında çalışanların siber güvenliğe karşı tutumlarını analiz eden
kurumsal değerlendirmelerin yanı sıra çalışanların becerilerini ölçmek için çeşitli araçlar sağlarız.

Siber güvenlik becerileri geliştirme ve eğitim

Bu kurslar, endüstriyel sistemlerin ve teknolojilerin güvenliği ile doğrudan ilgisi olan veya bunlara dahil olmayı düşünenler için siber güvenlik konularında ve tekniklerinde geniş bir müfredat sunmaktadır. Bu eğitimlerin tamamı, tercihe göre müşteri tesislerindeki bir sınıf içinde veya Kaspersky yerel ya da bölgesel ofislerinde verilebilir.

Katılımcılar siber suç tahmini, önleme, tespit ve yanıt konusunda "en önde" mücadele eden global uzmanlarımızın kendi deneyimleriyle ilham verdikleri çalışma ve öğrenme sürecinden faydalanır.

Kurslar hem teorik dersleri hem de uygulamalı "laboratuvar" derslerini içerir. Tamamlanan her kurstan sonra katılımcılar, bilgilerini değerlendirmek için bir değerlendirme testi tamamlamaya davet edilir.

Kurumsal uzmanlığınızı geliştirin

Bu eğitim kursları, kuruluşların siber güvenlik bilgi havuzunu üç ana alanda geliştirmesini sağlar:

- Endüstriyel kontrol sistemlerinin siber güvenliği konusunda temel bilgiler
- ICS Sızma Testi
- ICS Adli Bilişim

Uygulamalı Gelişmiş Endüstriyel Siber Güvenlik

BT/OT uzmanlarınıza tehdit ortamı ve endüstri ortamınızı hedef alan saldırı vektörleri konusunda yeni bir bakış açısı sağlar ve ekiplerinizin temel olay yanıt planı oluşturmak için gerekli tüm becerileri edinmesine yardımcı olur.

Uzmanlar İçin ICS Sızma Testi

BT/OT güvenlik uzmanlarının endüstriyel ortamlarda kapsamlı ve eksiksiz sızma testleri gerçekleştirmelerini ve uygun düzeltici eylemler için uzman önerileri sunmalarını sağlar.

Uzmanlar İçin ICS Adli Bilişim

BT/OT güvenlik uzmanlarının, endüstriyel ortamlarda adli bilişim incelemelerini başarılı bir şekilde gerçekleştirmelerinin yanı sıra uzman analizi ve önerileri sunmalarına yardımcı olur.

Kursların ayrıntılı açıklaması

Konular	Süre	Sonuçlar/Kazanılan Beceriler
Uygulamalı Gelişmiş Endüstriyel Siber Güvenlik		
• Mevcut tehdit ortamı, güvenlik sorunları, insan faktörü, ICS ağ saldırıları konularına genel bakış • BT ve ICS ortamlarında ağ güvenliği: Özel hususlar • Önleme, tespit ve risk azaltma tekniklerinin kullanımını gösteren vaka çalışması • Endüstriyel standartlara ve düzenlemelere uygunluk • Ağ topolojileri ve ağ güvenlik teknolojilerinin çalışma şekli • Siber güvenlik rolleri ve ekip yapıları • Yaygın güvenlik hataları.	1-2 gün	• Mevcut endüstriyel siber tehditleri ve endüstrinizi ya da kuruluşunuzu hedef alan siber olaylarla nasıl mücadele edebileceğinizi anlama • Güvenlik olaylarını tanıma ve belirleme • Basit incelemeler gerçekleştirme • Etkili bir olay yanıt planı oluşturma ve uygulama. Bu kurs, son derece özel unsurlar içerir ve tercihe göre 1 veya 2 gün sürecek şekilde uyarlanabilir. Sertifika verilir.
Uzmanlar İçin ICS Sızma Testi		
• Aşağıdakiler dahil olmak üzere farklı endüstrilerde ICS bileşenlerine, mimarilerine ve dağıtımına giriş: – Elektrik üretimi ve dağıtımı – Petrol ve Gaz – Taşımacılık • Bu endüstrilerde ve diğer ICS ortamlarında kullanılan uygulamalı sızma testi teknikleri • ICS Sızma Testi Planı Oluşturma: dikkat edilmesi gereken noktalar ve kısıtlamalar • Bilgi toplama • SCADA ve PLC sistemleri güvenlik açığı analizleri • Sonuçların analizi ve raporlama • Uygulamalı Laboratuvarlar.	5 gün	• Endüstriyel kontrol sistemlerindeki güvenlik açıklarını anlama ve analiz etme • Etkili bir ICS Sızma Testi Planı Oluşturma • SCADA, PLC'ler ve diğer ICS ögeleri üzerinde güvenli ve başarılı sızma testleri gerçekleştirme • Düzeltici eylemler için uzman önerileri sunma. Sertifika verilir.
Uzmanlar İçin ICS Adli Bilişim		
• Aşağıdakiler dahil olmak üzere farklı endüstrilerde ICS bileşenlerine, mimarilerine ve dağıtımına giriş: – Elektrik üretimi ve dağıtımı – Petrol ve Gaz – Taşımacılık • ICS'in zorluklarını ve kısıtlamalarını tanıma ve bunlarla çalışma • ICS ortamlarında uygulanan Adli Bilişim teknikleri • ICS Adli Bilişim Planı Oluşturma • Manuel adli inceleme verileri toplama ve koruma: RTOS ve ICS protokolleriyle çalışma • Sistem analizi ve anormallik doğrulaması • Raporlama • Uygulamalı Laboratuvarlar.	4 gün	• ICS ortamlarında başarılı adli bilişim incelemeleri gerçekleştirme. • ICS için etkili bir Adli Bilişim Planı Oluşturma • Fiziksel ve dijital kanıtlar toplama ve bu kanıtlarla uygun şekilde ilgilenme • Adli bilişim araçlarını ve enstrümanlarını SCADA ve PLC sistemlerine uygulama • Açıkta kalan yapılara dayalı olarak izinsiz giriş belirtilerini bulma • Olayları yeniden oluşturma ve zaman damgalarını kullanma • Uzman raporları ve uygulanabilir öneriler sunma. Sertifika verilir.

Endüstriyel Kontrol Sistemleri siber güvenliği hakkında her şey için: **https://ics-cert.kaspersky.com**
Siber Tehdit Haberleri: **www.securelist.com**

#truecybersecurity

www.kaspersky.com.tr

IIC MEMBER industrial internet CONSORTIUM

OPC FOUNDATION MEMBER

CYBER SECURITY EXCELLENCE AWARDS ★ FINALIST ★ 2017

* 3. Dünya İnternet Konferansı'nda Dünya'da Lider Bilimsel ve Teknolojik İnternet Başarı Ödülü
** Çin Uluslararası Endüstri Fuarı (CIIF) 2016 özel ödülü