Bölüm 1: Genel Bilgiler

Şirket Adı (isteğe bağlı) ……..

1. **Şirketiniz esas olarak hangi ülkede faaliyet göstermektedir?**
    1. Bulgaristan
    2. Estonya
    3. Yunanistan
    4. Norveç
    5. İspanya
    6. Türkiye
    7. Diğer ülkeler (Belirtiniz): _____
2. **Pazarınızın coğrafi kapsamı nedir?**

    - Yerel (yalnızca tek bir ülkede faaliyet gösteriyor)
    - Bölgesel (belirli bir bölgede, örneğin AB, Kuzey Amerika'da birden çok ülkede faaliyet gösteriyor)
    - Küresel (dünya genelinde faaliyet gösteriyor)

3. **Aşağıdaki kategorilerden hangisi kuruluşunuzun birincil sektörünü en iyi şekilde tanımlar?**

    - İmalat
    - Enerji
    - Su
    - Ulaşım & Lojistik
    - Kimya
    - Gıda & İçecek
    - Sağlık & İlaç
    - Finansal Hizmetler & Sigorta
    - Kamu Yönetimi
    - Bilişim & Telekomünikasyon
    - Petrol & Gaz
    - Savunma & Uzay
    - Diğer (belirtiniz): _____

4. **Şirketinizin tahmini çalışan sayısı nedir?**

    - 1–9
    - 10–49
    - 50–250
    - 251–1000
    - 1.001–5.000
    - 5.001–15.000

- 15.000'den fazla
- Bilmiyorum

5. **Kuruluşunuzun tahmini yıllık geliri (EUR cinsinden) nedir?,**(Lütfen birini seçiniz)
   - €0 – €1 milyon
   - €1 milyon – €5 milyon
   - €5 milyon – €10 milyon
   - €10 milyon'un üzerinde

6. **Kuruluşunuzdaki göreviniz nedir?**
   (Lütfen pozisyonunuzu en iyi tanımlayan seçeneği işaretleyin)
   - Üst Düzey Yönetim (örn. CEO, CFO, CISO)
   - Kıdemli Yönetim (örn. Direktör, Başkan Yardımcısı)
   - Orta Kademe Yönetim (örn. Müdür, Takım Lideri)
   - Teknik/Profesyonel (örn. Mühendis, Analist, Yazılımcı)
   - Mavi Yaka / Nitelikli İşçi (örn. Operatör, Teknisyen, Bakım Personeli)
   - Teknik Olmayan / Destek Personeli (örn. İK, İdari, Müşteri Hizmetleri)
   - Diğer (lütfen belirtiniz): _____

7. **Çalışma alanınızın temel odağı nedir?**
   (Lütfen birini seçiniz)
   - Operasyonel Teknoloji (OT) ve Endüstriyel Kontrol Sistemler
   - Bilgi Teknolojileri / İşletme tarafı
   - Her iki taraf
   - Diğer (lütfen belirtiniz): _____

8. **Operasyonel Teknoloji (OT) ile ilgili herhangi bir siber güvenlik düzenlemesi veya standardına (örneğin IEC 62443) uymanız gerekiyor mu?**
   (Lütfen birini seçiniz)
   - Emin değilim
   - Hayır, herhangi bir resmi siber güvenlik düzenlemesine veya standardına tabi değiliz
   - Evet, resmi düzenlemelere veya sektörel standartlara uymamız gerekiyor
     Eğer evet ise, lütfen hangi düzenleme veya standartlar olduğunu belirtiniz:
     _____
   - Evet, müşterilerimiz veya iş ortaklarımız tarafından belirlenen siber güvenlik gereksinimlerine uyuyoruz

Eğer evet ise, lütfen hangi gereksinim veya standartlar olduğunu belirtiniz:
_____

9. **Aşağıdaki hangi Operasyonel Teknoloji (OT) sistemleriyle kuruluşunuz doğrudan üretim veya imalat açısından ilgilidir?**
(Lütfen uygun olan tüm seçenekleri işaretleyin)
   - Herhangi bir OT sistemi kullanmıyoruz *(Bu seçenek işaretlenirse anket sona erer)*
   - SCADA (Denetleyici Kontrol ve Veri Toplama)
   - DCS (Dağıtılmış Kontrol Sistemleri)
   - PLC (Programlanabilir Mantıksal Denetleyiciler)
   - F&S (Yangın ve Gaz Sistemleri)
   - PLM (Ürün Yaşam Döngüsü Yönetimi) Ağ Geçitleri
   - Diğer (lütfen belirtiniz): _____
   - Şirketimizde OT sistemleri var ancak hangileri olduğunu bilmiyorum

Anket, "Herhangi bir OT (Operasyonel Teknoloji) sistemi kullanmıyoruz" seçeneği işaretlenirse sona erecektir.

Bölüm 2: Siber Güvenliğin Yönetimi

1. **Kuruluşunuzun karşılaştığı en önemli siber güvenlik zorlukları nelerdir?**
(En fazla 3 seçenek işaretleyiniz)
   - Bilmiyorum.
   - Yeterli nitelikli siber güvenlik personelinin olmaması
   - Siber güvenlik girişimleri için yetersiz bütçe
   - Güvenliği zor olan eski OT (Operasyonel Teknoloji) sistemleri
   - Siber güvenlik düzenlemeleri ve standartlarına uyum sağlama
   - Artan sayıda ve karmaşık siber tehditler
   - Çalışanlarda siber güvenlik farkındalığının eksikliği
   - BT ve OT ağlarının güvenli entegrasyonunda yaşanan zorluklar
   - Diğer (lütfen belirtiniz): _____

2. **Kuruluşunuz OT (Operasyonel Teknoloji) ortamlarında siber tehditleri nasıl tespit ediyor? (Tüm geçerli seçenekleri işaretleyiniz)**
   - Bilmiyorum
   - Aktif izleme yapılmıyor
   - Tehdit istihbarat servisleri
   - Manuel denetimler
   - Periyodik güvenlik denetimleri
   - Sürekli izleme (otomatik araçlarla)

- Diğer (lütfen belirtiniz): _____

3. **Kuruluşunuzda OT siber güvenliği nasıl yönetilmektedir?**
(Lütfen birini seçiniz)
   - Bilmiyorum
   - Aktif olarak yönetilmiyor
   - Dış hizmet sağlayıcılar tarafından yönetiliyor
   - Dahili genel BT güvenlik ekibi tarafından yönetiliyor
   - Özel bir OT siber güvenlik ekibi tarafından yönetiliyor
   - İç personel ve dış hizmet sağlayıcıların bir kombinasyonu ile yönetiliyor
   - Diğer (lütfen belirtiniz): _____

4. **Kuruluşunuzda OT (Operasyonel Teknoloji) personeline özel siber güvenlik eğitimi veriliyor mu?**
(Lütfen birini seçiniz)
   - Bilmiyorum
   - Hayır, şu anda OT siber güvenlik eğitimi uygulanmamaktadır,
   - Hayır, ancak OT siber güvenlik eğitimi uygulanması planlanmaktadır
   - Evet, ancak esas olarak BT'ye yönelik siber güvenlik eğitimi verilmektedir
   - Evet, düzenli ve yapılandırılmış OT'ye özel siber güvenlik eğitimi verilmektedir
   - Evet, düzenli ve yapılandırılmış hem BT hem de OT'ye özel siber güvenlik eğitimi verilmekte

Bölüm 3: (Soru 2.4'e verilen cevap "Evet" ise)

1. **Kuruluşunuzda hangi gruplar OT (Operasyonel Teknoloji) ile ilgili siber güvenlik eğitimi almaktadır?**
(Tüm geçerli seçenekleri işaretleyiniz)
   - Bilmiyorum
   - Yeni başlayan çalışanlar (işe alım sürecinde)
   - Üst düzey yönetim
   - OT personeli (örneğin mühendisler, teknisyenler, operatörler)
   - OT sistemleriyle ilgilenen BT personeli
   - Orta ve üst kademe yönetim
   - OT ortamına erişimi olan teknik olmayan personel
   - Diğer (lütfen belirtiniz): _____

2. Eğitim nasıl verilmektedir?
(Tüm geçerli seçenekleri işaretleyiniz)

- Yüz yüze atölyeler ve seminerler
- Çevrim içi eğitim modülleri
- Uygulamalı laboratuvarlar ve simülasyonlar
- Sertifikasyonlar ve dış kurslar
- İş başında eğitim ve mentorluk
- Hibrit model (yüz yüze + çevrim içi)
- Diğer (lütfen belirtiniz): _____
- Hiçbiri
- Bilmiyorum

3. Kuruluşunuzun OT siber güvenlik eğitim programlarında aşağıdaki konulardan hangileri yer almaktadır?
(Tüm geçerli seçenekleri işaretleyiniz)

- OT'ye özgü tehditlerin ve zafiyetlerin tanınması
- Kimlik avı, sosyal mühendislik ve parola güvenliği farkındalığı
- OT/BT ağ güvenliğinin yönetimi (örneğin segmentasyon, güvenlik duvarı yapılandırması)
- OT siber güvenlik standartlarının anlaşılması ve uyum (örneğin IEC 62443, NIST)
- OT sistemlerinin sıkılaştırılmasına ve güvenli iletişim protokollerine dair temel bilgiler
- Olay bildirim protokolleri ve müdahale prosedürleri
- Temel OT siber güvenlik araçlarının kullanımı
- OT'ye özel olaylara müdahale
- OT güvenlik olaylarının ve günlük verilerinin analizi
- OT sistemlerinde zafiyet taramaları ve sızma testleri
- Güvenli OT mimarilerinin tasarımı
- Kötü amaçlı yazılım araştırması ve olay sonrası analiz
- OT Güvenlik Operasyon Merkezi'nde (SOC) çalışma veya yönetme
- OT sistemlerinin ve güvenliğinin yasal çerçevesi
- OT sistemlerinin ve güvenliğinin yönetimi
- Diğer (lütfen belirtiniz): _____
- Hiçbiri
- Bilmiyorum

4. Kuruluşunuz OT siber güvenlik eğitiminin etkinliğini nasıl değerlendirmektedir?
(Tüm geçerli seçenekleri işaretleyiniz)

- Eğitim sonrası testler veya sınavlar

- Performans göstergelerinin izlenmesi (örneğin olay müdahale süresi, kimlik avı testi sonuçları)
- Çalışan geri bildirimleri veya anketlerin toplanması
- Eğitim sonuçlarının denetimi, değerlendirilmesi veya resmi gözden geçirilmesi
- Resmi bir değerlendirme süreci yok
- Diğer (lütfen belirtiniz): _____,
- Uygulanamaz
- Bilmiyorum

5. Kuruluşunuzda hangi OT siber güvenlik eğitimlerine ve bilgilendirmeye ihtiyaç vardır? (Tüm geçerli seçenekleri işaretleyiniz)

- OT'ye özgü tehditler ve zafiyetler
- OT ortamının güvenliği için kriptografi ve anahtar yönetimi
- Kimlik avı, sosyal mühendislik ve parola güvenliği
- OT/BT ağ güvenliği (örneğin segmentasyon, güvenlik duvarı ayarları)
- OT siber güvenlik standartlarına uyum (örneğin IEC 62443, NIST)
- OT uygulamaları için güvenli kodlama, güvenli yapılandırma ve sistem sıkılaştırma
- OT ortamlarında sızma testleri ve zafiyet değerlendirmeleri
- Kötü amaçlı yazılımlar ve olay sonrası müdahale süreçler
- Güvenlik operasyonları: olay müdahalesi, günlük analizi ve SOC faaliyetleri
- Diğer (lütfen belirtiniz): _____
- Hiçbiri
- Emin değilim / Biliyorum

6. Kuruluşunuzda hangi grupların OT ile ilgili siber güvenlik eğitimi alması gerekmektedir? (Tüm geçerli seçenekleri işaretleyiniz)

- Bilmiyorum
- Yeni başlayan çalışanlar
- Üst düzey yönetim
- OT personeli (örneğin mühendisler, teknisyenler, operatörler)
- OT sistemleriyle ilgilenen BT personeli
- Orta ve üst kademe yönetim
- OT ortamına erişimi olan teknik olmayan personel
- Diğer (lütfen belirtiniz): _____

7. OT siber güvenliği ile ilgili karşılaştığınız zorluklar, ihtiyaçlar veya en iyi uygulamalar hakkında paylaşmak istediğiniz başka bir şey var mı?

……

Bölüm 3: (Soru 2.4'e verilen cevap "Hayır" ise)

1. **Kuruluşunuzda hangi OT siber güvenlik eğitimlerine ve bilgilendirmeye ihtiyaç vardır? (Lütfen tüm geçerli seçenekleri işaretleyiniz)**
   - OT'ye özgü tehditlerin ve zafiyetlerin tanınması
   - Kimlik avı, sosyal mühendislik ve parola güvenliği farkındalığı
   - OT/BT ağ güvenliğinin yönetimi (örneğin segmentasyon, güvenlik duvarı yapılandırması)
   - OT siber güvenlik standartlarının anlaşılması ve uyum (örneğin IEC 62443, NIST)
   - OT sistemlerinin sıkılaştırılmasına ve güvenli iletişim protokollerine dair temel bilgiler
   - Olay bildirim protokolleri ve müdahale prosedürleri
   - Temel OT siber güvenlik araçlarının kullanımı
   - OT'ye özgü olaylara müdahale
   - OT güvenlik olaylarının ve günlük verilerinin analizi
   - OT sistemlerinde zafiyet taramaları ve sızma testleri
   - Güvenli OT mimarilerinin tasarımı
   - Kötü amaçlı yazılım analizi ve olay sonrası inceleme
   - OT Güvenlik Operasyon Merkezi'nde (SOC) çalışma veya yönetme
   - OT sistemlerinin ve güvenliğinin yasal çerçevesi
   - OT sistemlerinin ve güvenliğinin yönetimi
   - Diğer (lütfen belirtiniz): _____
   - Hiçbiri
   - Bilmiyorum
2. **Eğitim nasıl verilmesini tercih edersiniz? (Tüm geçerli seçenekleri işaretleyiniz)**
   - Yüz yüze atölyeler ve seminerler
   - Çevrim içi eğitim modülleri
   - Uygulamalı laboratuvarlar ve simülasyonlar
   - Sertifikasyonlar ve dış eğitim programları
   - İş başında eğitim ve mentorluk
   - Hibrit model (yüz yüze + çevrimiçi)
   - Diğer (lütfen belirtiniz): _____
   - Hiçbiri
   - Bilmiyorum
3. **Kuruluşunuzda hangi grupların OT ile ilgili siber güvenlik eğitimi alması gerekmektedir? (Tüm geçerli seçenekleri işaretleyiniz)**
   - Bilmiyorum
   - Yeni başlayan çalışanlar

- Üst düzey yönetim
- OT personeli (örneğin mühendisler, teknisyenler, operatörler)
- OT sistemleriyle ilgilenen BT personeli
- Orta ve üst kademe yönetim
- OT ortamına erişimi olan teknik olmayan personel,
- Diğer (lütfen belirtiniz): _____

4. OT siber güvenliği ile ilgili karşılaştığınız zorluklar, ihtiyaçlar veya en iyi uygulamalar hakkında paylaşmak istediğiniz başka bir şey var mı?

……