KATEGORİ 1 · UYUM VE SÜRDÜRÜLEBİLİRLİK DANIŞMANLIKLARI

ISO 27019 & SGYM Uyum ve Sürdürülebilirlik Danışmanlığı

OT / EKS

Enerji sektörünün OT ve EKS dinamiklerini merkeze alan; ISO 27001 çatısına ISO 27019, IEC 62443 ve EPDK SGYM gereksinimlerini entegre ederek endüstriyel siber dayanıklılık mimarisi inşa eden danışmanlık.

ISO 27019 danışmanlığı | EPDK SGYM uyum | IEC 62443 | OT güvenliği | SCADA güvenliği | Purdue modeli

KATEGORİ
Uyum ve Sürdürülebilirlik Danışmanlıkları

TİPİK SÜRE
Tipik program 8–12 ay · Saha ve tesis sayısına göre ölçeklenir

KİMLER İÇİN
Elektrik dağıtım ve üretim şirketleri, doğal gaz dağıtım kuruluşları, rafineriler, iletim operatörleri, OSB elektrik dağıtım lisansı sahipleri ve kritik altyapı işleten sanayi tesisleri.

1 Hizmetin Tanımı

Bu hizmet, klasik BT güvenliği gereksinimlerinin ötesine geçerek enerji sektörünün kalbi olan Operasyonel Teknoloji (OT) ve Endüstriyel Kontrol Sistemleri (EKS) dinamiklerini merkeze alan kapsamlı bir danışmanlık ve yönetişim modelidir. Temel ISO 27001 BGYS'nin üzerine endüstriyel standartların (ISO 27019, IEC 62443) ve EPDK Siber Güvenlik Yetkinlik Modeli (SGYM) idari ve teknik gereksinimlerinin entegre edilmesiyle oluşturulur.

2 Neden Gereklidir?

Enerji altyapıları; devlet destekli siber tehdit aktörlerinin, fidye yazılımı gruplarının ve tedarik zinciri saldırılarının birincil hedefindedir. Klasik BT güvenlik yaklaşımları SCADA, PLC, RTU gibi endüstriyel sistemlerin "süreç bütünlüğü" ve "operasyonel kesintisizlik" ilkeleriyle örtüşmez. Enerji üretim, iletim ve dağıtım süreçlerinin fiziksel dünyadaki yıkıcı etkilere (üretim durması, çevre felaketi, can güvenliği riski) karşı korunması hayati önem taşır. Ayrıca EPDK regülasyonlarına ve 7545 sayılı Kanun'a uyum sağlamak; idari para cezaları ile lisans iptali gibi ağır yaptırımların önüne geçmek için sektöre özel standartlaştırılmış bir model şarttır.

YAPTIRIM VE RİSK EŞİĞİ
EPDK mevzuatı kapsamında idari para cezası ve lisans süreçlerinde yaptırım; 7545 sayılı Kanun kapsamında 1.000.000 ₺ – 10.000.000 ₺ aralığında idari para cezası riski bulunmaktadır.

3 Yasal ve Normatif Dayanak

EPDK Siber Güvenlik Yetkinlik Modeli (SGYM) Yönetmeliği — 6 Haziran 2023 | 7545 sayılı Siber Güvenlik Kanunu | ISO/IEC 27019 | IEC 62443 serisi | EKS Güvenlik Usul ve Esasları | NIST SP 800-82

4 Sağladığı Katma Değer

Operasyonel süreklilik ve fiziksel emniyet

OT ortamlarında “sıfır kesinti” (availability) ve “can güvenliği” (safety) önceliklendirilerek, üretim hatlarını riske atmayan matematiksel bir risk modellemesi ve çözüm mimarisi sunulur.

Hibrit ve bütünleşik güvenlik mimarisi

ISO 27001’in yönetsel çatısı ile IEC 62443 serisinin teknik derinliği birleştirilir. BT ve OT ağları arasındaki sınırlar uluslararası Purdue Modeline göre netleştirilerek yanal siber saldırıların (lateral movement) önüne geçilir.

Regülasyonlara tam ve sürdürülebilir uyum

EPDK SGYM, BİGR ve KVKK uyumluluğu sağlanır. Süreçler kişilerden bağımsız, kurumsal hafızaya dayalı ve ölçülebilir bir yapıya kavuşturulur.

Proaktif kriz ve olay yönetimi yeteneği

Hem saha mühendislerinin teknik müdahale refleksleri (Red/Purple Teaming, tehdit avcılığı) hem de yönetim kademesinin stratejik kriz yönetimi (masa başı tatbikatları) uygulamalı olarak test edilerek geliştirilir.

5 Hizmet Kapsamı ve Metodoloji

Genel bakış: PURDUE REFERANS MIMARISI — BÖLGE VE KANAL AYRIMI SEVIYE 4-5 Kurumsal BT / ERP İş uygulamaları, ofis ağı DMZ Endüstriyel DMZ Veri diyodu, sıçrama sunucusu, tek yönlü aktarım SEVIYE 3 Operasyon Yönetimi Tarihçi, OT-SOC, yama ve yedekleme SEVIYE 2 Denetleyici Kontrol SCADA/HMI, mühendislik istasyonu SEVIYE 1 Temel Kontrol PLC, RTU, IED SEVIYE 0 Saha Cihazları Sensör, aktüatör, akıllı sayaç

AŞAMA 1

Proje Başlangıcı ve Mevcut Durum Analizi

BT ve OT ağ sınırlarının çizilmesi, kapsam dokümantasyonunun (SoA) hazırlanması. ISO 27019, EPDK SGYM ve BİGR referans alınarak kurumun mevcut olgunluk seviyesinin ve eksikliklerinin analizi.

AŞAMA 2

EKS/OT Varlık ve Risk Yönetimi

SCADA, PLC, RTU ve akıllı sayaçları kapsayan detaylı OT varlık envanterinin oluşturulması. ISO 27005 ve IEC 62443-3-2 (Zone & Conduit) metodolojisiyle üretim sürekliliği odaklı tehdit, zafiyet ve risk analizlerinin gerçekleştirilmesi.

AŞAMA 3

Yönetişim, Politika ve Süreç Tasarımı

OT ortamlarına özel güvenli uzaktan erişim, yama yönetimi, tedarikçi güvenliği ve USB kullanım politikalarının yazılması. Endüstriyel senaryolara dayalı Olay Müdahale (IRP) ve İş Sürekliliği / Felaket Kurtarma (BCP/DRP) planlarının oluşturulması.

AŞAMA 4

Teknik Mimari Tasarımı ve Çözüm Danışmanlığı

Purdue referans mimarisine uygun OT ağ segmentasyonu (DMZ, veri diyotları), üçüncü taraflar için Sıfır Güven (Zero Trust) IAM/PAM süreçleri ve endüstriyel protokolleri (Modbus, IEC 104) anlayan OT-SOC/SIEM izleme mimarisi danışmanlığı. Ürün tedariği veya konfigürasyonu hariçtir; mimari yönlendirme yapılır.

AŞAMA 5

Test, Simülasyon ve Tatbikatlar

Üretimi riske atmadan MITRE ATT&CK for ICS çerçevesinde teknik siber saldırı simülasyonları (lateral movement, endüstriyel protokol manipülasyonu). Karar vericiler için stratejik siber kriz masa başı tatbikatları ve manuel operasyona geçiş (BIA/DRP) testleri.

AŞAMA 6

İleri Seviye Farkındalık ve Eğitim

Saha personeli için ISO 27019 standartlarında EKS farkındalık eğitimleri. Mühendisler için güvenli PLC kodlama, derin paket analizi ve endüstriyel tehdit avcılığını içeren ileri düzey teknik EKS savunma eğitimleri.

AŞAMA 7

Denetim, YGG ve Belgelendirme Desteği

Sertifikasyon öncesi ISO 27019 ve EPDK normlarında iç denetim, bulgular için DÖF takibi, YGG raporlaması ve resmî belgelendirme kuruluşunun Aşama 1–2 denetimlerinde refakat edilmesi.

6 Teslimatlar, Çıktılar ve Başarı Kriterleri

TESLİMATLAR VE ÇIKTILAR

- ✓ ISO 27019 & SGYM Uyum Boşluk (Gap) Analizi Raporu
- ✓ EKS/OT Varlık Envanteri Kayıtları ve Matematiksel Risk İşleme Matrisi
- ✓ Uygulanabilirlik Bildirgesi (SoA) ve entegre BGYS politika/prosedür seti
- ✓ Endüstriyel Olay Müdahale (IRP) ve İş Sürekliliği (BCP/DRP/BIA) planları
- ✓ Purdue Modeli ağ segmentasyonu ve güvenlik teknolojileri mimari tasarım dokümanı
- ✓ Teknik simülasyon (Red/Purple Team) sonuçları ve masa başı tatbikat raporu
- ✓ İç denetim raporu, DÖF kayıtları ve YGG yönetici özeti sunumu
- ✓ Personel farkındalık ölçüm ve eğitim tamamlama raporları

HEDEFLENEN ÇIKTI / BAŞARI KRİTERİ

- ✓ Uluslararası geçerliliğe sahip ISO 27001 belgesi, enerji sektörüne özel ISO 27019 ek kontrollerini de kapsayacak şekilde edinilir.
- ✓ EPDK SGYM yükümlülükleri, kâğıt üzerinde değil sahada fiilen işleyen teknik ve idari kontrollerle karşılanarak resmî denetimlere eksiksiz hazır hâle gelinir.
- ✓ APT grupları ve sabotaj dâhil en gelişmiş endüstriyel saldırılara karşı operasyonel emniyetini koruyabilen, kriz refleksleri test edilmiş dirençli bir endüstriyel altyapı elde edilir.

7 Sık Sorulan Sorular

OT ağımızda test yapmak üretimi durdurur mu?

Hayır. Tüm teknik faaliyetler üretim sürekliliğini önceliklendiren OT'ye özgü metodolojilerle, mümkün olan yerlerde pasif dinleme ve test yatağı üzerinden yürütülür; aktif testler yalnızca planlı duruşlarda ve yazılı mutabakatla yapılır.

SGYM seviyemizi kim belirliyor?

Seviye, kuruluşun kritiklik sınıfına bağlı olarak yönetmelikçe belirlenir ve EBİS üzerinden EPDK'ya bildirilir. Danışmanlık, hedef seviyeye ulaşmak için gereken kontrol setini kurar.

IEC 62443 ile ISO 27019 çakışıyor mu?

Hayır, tamamlayıcıdırlar. ISO 27019 yönetsel çerçeveyi ve enerji sektörüne özgü kontrolleri, IEC 62443 ise bölge/kanal mimarisi ve güvenlik seviyeleri gibi teknik derinliği sağlar.

8 Etiketler

ISO 27019 danışmanlığı · EPDK SGYM uyum · IEC 62443 · OT güvenliği · SCADA güvenliği · Purdue modeli · Zone and Conduit · EKS varlık envanteri · MITRE ATT&CK for ICS · veri diyodu

Bu hizmet, tam hizmet kataloğunun bir parçasıdır. Diğer 11 hizmet ve bütüncül paketler hakkında bilgi için Genel Broşür'e başvurabilirsiniz. Bu doküman bilgilendirme amaçlıdır; hukuki mütalaa veya taahhüt niteliği taşımaz.