



CyberArts™

*Her ne yaparsak yapalım
içinde “sanat” hep var olacak!*



cyberartspro

CyberArts Felsefesi





Söz konusu siber hizmetler olduğunda
tüm kurumlar her şeyin en iyisini talep
eder ve her şeyin en iyisini de hak eder.

Siber dünyadaki tecrübelerimizi,
sanatçı hassasiyeti ve titizlięi ile
alıřan dięer kurum ve kiřilerle bir
araya gelerek, sıradanlık deęil sanat
talep eden kurumların hizmetine
sunuyoruz.





**İhtiyacınız olan
sıradanlık mı
sanat mı?**



BİLGİ GÜVENLİĞİ

Hukuk, Siber Güvenlik ve Yönetişim disiplinlerini bir araya getirerek tam uyum ve sürdürülebilirlik.



SİBER GÜVENLİK BAŞKANLIĞI VE SİBER GÜVENLİK KANUNU

Türkiye Cumhuriyeti Cumhurbaşkanlığı'na bağlı olarak 8 Ocak 2025 tarihinde kurulan Siber Güvenlik Başkanlığı, 19 Mart 2025'te yürürlüğe giren 7545 Sayılı Siber Güvenlik Kanunu ile güçlendirilmiştir.

Cezai Yaptırımlar;

Yükümlülöklere uyulmaması halinde 15 yıla varan hapis cezaları ile yıllık brüt satış hasılatının %5'ine kadar para cezaları mümkün.



Bütüncül Siber Güvenlik Paketleri

“12 Ay boyunca ihtiyaç duyduğunuz
temel hizmetler bir arada”



Kağıt Üstü Uyumdan Gerçek Güvenliğe Bütünleşik Bilgi Güvenliği ve Siber Güvenlik Olgunluk Yönetimi

Çözümümüz; stratejik hedefleri, ISO 27001 veya KVKK gibi uyumluluk gerekliliklerini, Sızma Testi (Pentest) gibi teknik operasyonlardan gelen somut kanıtlarla birleştirir. Böylece risk odaklı, ölçülebilir ve sürdürülebilir bir yol haritasına sahip olursunuz.

Neden Bütünleşik Yaklaşım?

Geleneksel yöntemlerde BT, Hukuk ve İç Denetim birimleri genellikle birbirinden kopuk silolar halinde çalışır.

1. Bu durum üç temel soruna yol açar:
2. Parçalı Bakış Açısı
3. Statik Raporlar
4. Yanlış Önceliklendirme

İhtiyaca Yönelik Ölçeklenebilir Çözümler

Kurumunuzun büyüklüğü ve mevcut olgunluk seviyesi ne olursa olsun, size uygun, kullanabileceğiniz bir yol haritası belirledik.

5. Temel Uyum ve Farkındalık (Başlangıç Seviyesi)
6. Kurumsal Dönüşüm (Orta Seviye)
7. Kurumsal Olgunluk (İleri Seviye)
8. Yanlış Önceliklendirme

Nasıl Çalışıyoruz? Bütünleşik Yönetim Döngüsü

Hizmetimiz tek seferlik bir proje değil, sürekli iyileşen bir döngüdür;

Kurumsal hedeflerinize uygun GRC kontrol ağacını tasarlayıp risk analizleri ve sızma testleriyle mevcut durumu ölçüyor, bulguları iş süreçleri ve risklerle eşleştirerek boşlukları kapatacak öncelikli bir yol haritası sunuyoruz.

Sonuç: Yaşayan Bir Güvenlik Programı

Siber güvenlik, bir varış noktası değil, bir yolculuktur.

“Bütünleşik GRC ve Siber Güvenlik Olgunluk Yönetimi” hizmetimizle, kurumunuza özel Dinamik Risk ve Olgunluk Kaydı oluşturarak, güvenliği reaktif bir zorunluluktan, proaktif bir iş avantajına dönüştürüyoruz.

ENERJİ SEKTÖRÜNDE EPDK SGYM VE EKS SIZMA TESTİ

Enerji Piyasası Düzenleme Kurumu (EPDK), kritik altyapıları korumak amacıyla iki temel ve zorunlu düzenlemeyi hayata geçirmiştir;

1. Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli (SGYM) Yönetmeliği
2. Enerji Sektöründe Kullanılan EKS İçin Güvenlik Analiz ve Test Usul ve Esasları

Bu yönetmelikler, enerji şirketleri için artık bir tavsiye değil, operasyonel süreklilik ve ulusal güvenlik için bir zorunluluktur.

EPDK UYUMLU HİZMETLERİMİZ

1. SGYM Danışmanlığı ve Sektörel Denetim Hizmetleri
2. EPDK Uyumlu EKS/OT Sızma Testleri ve Güvenlik Analizi
3. Risk Değerlendirme ve Aksiyon Planı Raporlaması

EPDK UYUMLU EKS SIZMA TESTİ METODOLOJİMİZ

1. Ağ ve Mimari Yapının İncelenmesi: Saldırı Yüzeyinin Haritalanması
2. Sosyal Mühendislik: İnsan Faktörünün Testi
3. Zafiyet Tarama: Kırılgan Noktaların Sessizce Tespiti
4. Zararlı Yazılım Analizi: Anomali Avcılığı
5. Kablosuz Ağ Testleri: Görünmeyen Saldırı Kanalları
6. Sömürü (Exploit) Testleri: Açığın Gerçek Etkisini Görme



UYUM DANIŞMANLIĞI

İyileştirme ve Sertifikasyon

- Kontrollerin iyileştirilmesi, güncellenmesi
- Sertifikasyon hazırlık kontrolleri

Uygulama

- Kontrollerin uygulanması
- Politika ve prosedürler

Organizasyon

- Uyum süreçlerini başlatan ekiplerin belirlenmesi
- Roller ve sorumlulukların belirlenmesi

Kontrol ve Denetim

- İç Denetimler
- Tedarikçi Denetimleri
- Gözden Geçirme

Planlama

- Varlık Grupları
- Mevcut Durum & Hedeflenen Durum
- Boşluk Analizi
- Uygulama Yol Haritası

DENETİM

Planlama

- Denetim ekibinin belirlenmesi
- Organizasyonun anlaşılması
- Süreçlerin incelenmesi
- Denetim kapsamının belirlenmesi
- Denetim programının oluşturulması

Uygulama

- Denetim yöntemlerinin uygulanması
- Denetim kanıtlarının toplanması
- Uygulama süreçlerinin etkinliğinin değerlendirilmesi
- Tedbirlerin etkinliğinin değerlendirilmesi
- Bulguların tespiti, değerlendirilmesi ve izlenmesi

Raporlama

- Denetim raporunun hazırlanması
- Bulguların raporlanması
- İnsan kaynağı, süreçler ve teknoloji gereksinimlerinin ortaya konulması
- Olgunluk seviyesine ilişkin değerlendirmeler
- Çözüm önerileri
- Entegre sistem girişleri

SÜRDÜRÜLEBİLİRLİK DANIŞMANLIĞI

Aylık Faaliyetler

- Düzeltici Faaliyetlerin takibi ve yönetimi
- Bültenler
- Kontrollerin uygulanmasına yönelik destek
- Olay İhlallerinin takibi ve yönetimi

Altı Aylık Faaliyetler

- Varlık Envanterinin güncellenmesi
- Risk Analizi & Boşluk Analizi gözden geçirme
- Boşluk Analizi sonucuna göre Bilgi Güvenliği tedbirlerinin gözden geçirilmesi ve ilave tedbirler alınması

Yıllık Faaliyetler

- Denetim ve sertifikasyon hazırlığı
- Farkındalık Eğitimi
- Politika & Prosedürlerinin güncellenmesi
- İç Denetim & Tedarikçi Denetimi
- Üst Yönetim toplantılarına katılım

TEDARİKÇİ DEĞERLENDİRMESİ

Tedarikçi Değerlendirmesi (Denetim ve Değerlendirme) faaliyetleri, bilgi güvenliği önlemlerinin alınmasını ve tedarik zinciri süreçleri ile uygulamalarında güvenli bir yapı oluşturulmasını amaçlar. Bu faaliyetler kapsamında, operasyonel ve iş yönetimi süreçlerinde tedarikçilerle çalışan kuruluşların; doğrudan veya dolaylı olarak sorumlu oldukları üçüncü taraf şirketlerden kaynaklanabilecek riskleri izlemeleri ve en aza indirmeleri gerekmektedir.

Tedarikçi güvenlik hizmeti ile taraflarca tanımlanan süreçler, varlıklar, işlenen veriler ve sistem erişim işlemleri doğru ve detaylı bir şekilde kontrol edilir, tedarikçilerden kaynaklanabilecek güvenlik zafiyetleri belirlenir ve bu zafiyetler için çözüm önerileri sunulur. Tedarikçi güvenlik değerlendirme hizmeti, tedarik zincirinden kaynaklanan veri, hizmet, operasyon, işgücü, zaman, itibar ve finansal kayıplar ile hukuki yaptırımların önlenmesini sağlar.



CyberArts™

www.cyberartspro.com

Siber Gvenlik Sanatları

Gardınızı CyberArts ile alın



YÖNETİLEBİLİR SİBER GÜVENLİK HİZMETLERİ

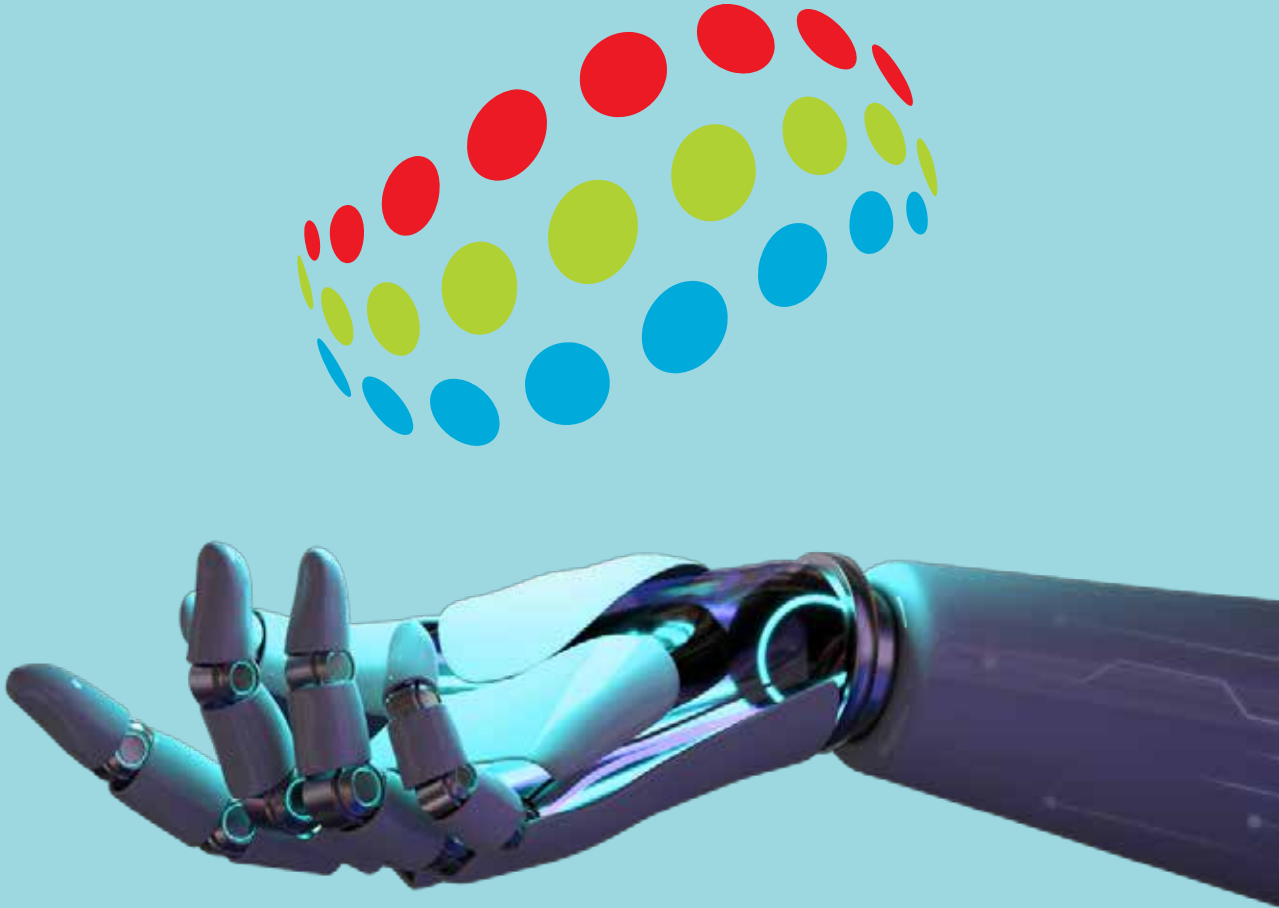
- Sızma Testi ve Zaafiyet Analizi
- Siber Tatbikat
- Siber Kriz Yönetimi
- Siber Tehdit İstihbaratı
- Siber Olay Müdahale ve Adli Bilişim Analizi
- Kanıt/İz Analizi

Sosyal Mühendislik

- Siber Güvenlik Eğitimleri
- Uygun Teknolojilerin Belirlenmesi, Kurulması ve Desteği
- Mevcut Çözümler ile Entegrasyon
- Aylık Değerlendirme Toplantıları ve Raporlama



**En iyi teknoloji ve hizmetleri
titizlikle seiyoruz ve uçtan uca
tamamlayıcı bir portföy sunuyoruz.**





ALTYAPI VE AĞ GÜVENLİĞİ

- NDR
- NAC
- SD-WAN
- Firewall
- ZTNA
- Active Directory
- HSM
- Kripto Sistemleri
- Ağlararası Güvenli Geçiş Sistemleri
- EKS Güvenliği

UÇ NOKTA KORUMASI

Server

Tablet

Laptop

Cep
Telefonu

AV

EDR

MDR

EPP

XDR

Virüs

Malware-
Zararlı

Ransomware-
Fidye

Spyware-
Casus



VERİ GÜVENLİĞİ

- Veri Şifreleme
- Veri Sızıntısı Önleme (DLP)

OLAY MÜDAHALE VE ADLİ BİLİŞİM

- Dakikalar İçinde Kanıt Toplama
- Otomatik ve Uzaktan Müdahale
- 120+ Kanıt Türü
- Hızlı Analiz ve Raporlama



GÜVENLİK BİLGİ OLAY YÖNETİMİ (SIEM)

- Büyük Veri Analizi
- Olaylara Proaktif Müdahale
- Yapay Zeka ile Davranış Analizi

GÜVENLİK ORKESTRASYON OTOMASYON & OLAYLARA MÜDAHALE (SOAR)

- Güvenlik Altyapısında Uyum & Hakimiyet
- Kapsamlı & Eşzamanlı Olay Müdahale





WEB GÜVENLİĞİ

- WEB Güvenlik Duvarı (WAF)
- IPS
- IDS
- DDoS
- DNS Katmanında Analiz

SİBER TEHDİT İSTİHBARATI (CTI)

- Dolandırıcılık & İstismar & Oltalama Takibi
- Marka Koruması
- Deep Web/Dark Web/Sosyal Medya Takibi



TEHDİT SİMÜLASYONU

- Güvenlik Açıklarını Saklama
- ASM
- Saldırı Simülasyonu
- Sürekli Tehdit Analizi
- BAS

UYGULAMA GÜVENLİĞİ

- Sıfır Güven Mimarisi
- SASE
- API Security
- Sandbox





MOBİL GÜVENLİK

- BYOD (Kendi Cihazını Getir) Risk Yönetimi
 - Cep Telefonu Kaybı Senaryoları
 - App Shielding
 - MDM
 - MAM

BULUT GÜVENLİĞİ

• Regülasyonlara Uyum

• Cloud Access Security Broker (CASB)

• Şifrelenmiş Veri

• Güvenli Bulut Erişimi



GÜVENLİ İLETİŞİM

- Webinar
- Görüntülü Görüşme

MASA TELEFONU

VOIP

IP

ARKA KAPI

TEHDİT

Rİ

SK

YÖNETİM BİLİŞİM SİSTEMLERİ

- Yönetişim ve Denetim
- Risk Analizi
- Uyumluluk Yönetimi



FİZİKSEL KİMLİK VE ERİŞİM YÖNETİMİ

- Akıllı Giriş Kartı
- Biyometrik Doğrulama
- Vücut Dili Analizi



DİJİTAL KİMLİK VE ERİŞİM YÖNETİMİ

- Passwordless Mimari
- BIOS Şifreleme
- Yapay Görü
- PAM - Ayrıcalıklı Erişim Yönetimi
- IAM - Kimlik ve Erişim Yönetimi
- MFA - Çok Faktörlü Erişim



UZAKTAN KİMLİK DOĞRULAMA VE ERİŞİM PAKETİ

Uzaktan Biyometrik Kimlik Doğrulama

- Biyometrik doğrulama başarı oranı: %99,614
- Vektör Bilgisi Kullanımı (HASH) ile Şifrelenmiş Güvenlik, Blok Zinciri Mimarisi
- Mobil, Web, Bulut Çerçevesi
- NFC, OCR, MRZ Uyumlu
- Adaptif API/SDK
- Metadata Algılama ve Raporlama (48 metadata türü)

Şifresiz Çoklu Faktörlü Kimlik Doğrulama

- Kurumsal Çoklu Faktörlü Kimlik Doğrulama (MFA)
- Tek Oturum Açma (Single Sign-On)
- Şifre Yönetimi
- Paylaşım Merkezi
- Nokta Erişim Yönetimi
- Dizin Hizmetleri

Mobil Uygulama Güvenliği

- SSL Pimleme
- Keylogger Karşıtı
- Cihaz Listesi
- Overlay Tespiti
- Kötü Amaçlı Yazılım Karşıtı
- Cihaz Parmak İzi Alma
- Merkezi Yönetim Konsolu
- Root/Jailbreak Tespiti





*Her ne yaparsak yapalım
içinde “sanat” hep var olacak!*



CyberArts™

Kurum Sertifikalarımız



Ekip Sertifikalarımız

