🛡️ Güvenlik Çözümleri

Dijital Varlıklarınızı Uçtan Uca Siber Güvenlik ile Koruyun

Günümüzde siber tehditler, kurumlar için en kritik operasyonel risklerden biri haline gelmiştir. **Teknoser**, bilgi varlıklarınızı, BT altyapınızı ve dijital süreçlerinizi koruyan kapsamlı güvenlik çözümleri sunar. Amacımız yalnızca güvenlik sağlamak değil; iş sürekliliğini korumak, kurumsal itibarı güvence altına almak ve operasyonel bütünlüğü sağlamaktır.

Network güvenliğinden uç nokta korumasına, e-posta güvenliğinden veri kaybı önlemeye kadar geniş bir siber güvenlik portföyüne sahibiz. Mevcut altyapınıza entegre ettiğimiz erişim kontrolü ve güvenlik izleme sistemleriyle kurumunuza özel, çok katmanlı bir savunma mimarisi oluşturuyoruz.

Her çözüm sektörünüze, kurum ölçeğinize ve risk profilinize göre özel olarak tasarlanır.

🔐 IT Güvenlik Çözümleri

Dijital Kuruluşu Kapsamlı Şekilde Koruyan Yaklaşım

Siber tehditler artık daha gelişmiş, daha hızlı ve daha yıkıcı. Geleneksel güvenlik önlemleri tek başına yeterli değil. Teknoser, dijital varlıklarınızın her zaman görünür, kontrol edilebilir ve korunur olmasını sağlayan uçtan uca BT güvenlik mimarisi sunar.

🌐 Ağ Güvenliği (Network Security)

Modern ağ güvenliği yalnızca firewall kurulumundan ibaret değildir. Teknoser, Zero Trust prensipleriyle tüm ağ altyapınızı uçtan uca korur.

Ağ Güvenliği Yetkinliklerimiz:

- 🔥 Yeni Nesil Firewall (NGFW) çözümleri
- 🌐 SASE / SSE mimarileri
- 🛡️ IPS / IDS sistemleri
- 🧠 Uygulama farkındalığı
- 🚫 URL filtreleme
- 🔍 SSL inceleme
- 📤 Veri Kaybı Önleme (DLP) politikaları
- 🧩 Mikro-segmentasyon

💻 Uç Nokta Güvenliği (EDR / XDR)

Uç noktalar siber saldırıların en sık hedef aldığı katmandır. Teknoser, gelişmiş tehdit analizi ve uçtan uca görünürlük sağlayan çözümler sunar.

Öne Çıkan Özellikler:

- 🛡️ EDR / XDR platform entegrasyonu
- 🔎 Davranışsal analiz & tehdit tespiti
- 🔒 Fidye yazılımı (ransomware) koruması
- 👁️ Uçtan uca görünürlük
- ⚙️ Otomatik yanıt aksiyonları
- 🆔 Kimlik odaklı koruma

🧩 Kimlik ve Erişim Yönetimi (IAM)

Doğru kullanıcının doğru kaynağa doğru zamanda erişmesi, siber güvenliğin temelidir.

Teknoser IAM Hizmetleri:

- 🔐 MFA, SSO ve Zero Trust erişim
- ⌨️ Ayrıcalıklı Erişim Yönetimi (PAM)
- 👤 Kullanıcı yaşam döngüsü yönetimi
- 🧠 Kimlik bazlı güvenlik kontrolleri

📧 E-Posta ve Uygulama Güvenliği

Siber saldırıların büyük çoğunluğu e-posta üzerinden başlar.

Sunduğumuz Çözümler:

- 🎣 Anti-phishing
- 🧪 Sandbox analiz
- ✉️ E-posta Gateway güvenliği
- ☁️ O365 & Google Workspace koruması

- 🧹 İçerik filtreleme
- 🛡️ Alan adı koruması (DMARC / DKIM / SPF)

☁️ Bulut Güvenliği

Kurumlar hibrit ve çoklu bulut yapısına geçtikçe güvenlik daha karmaşık hale geliyor. Teknoser, bulut dönüşümünüzü güvenli şekilde gerçekleştirmeniz için tam kapsamlı çözümler sunar.

Uzmanlık Alanlarımız:

- 🔭 CSPM / CWPP
- 🔥 Bulut firewall çözümleri
- 🔐 Zero Trust bulut erişimi
- 🔌 API güvenliği
- 🖥️ İş yükü (workload) koruma
- 📦 Container & Kubernetes güvenliği

🧪 Zafiyet Yönetimi & Penetrasyon Testleri

Proaktif güvenliğin temeli görünürlüktür.

Kapsamımız:

- 🔎 Sürekli zafiyet taraması
- 💥 Penetrasyon testleri
- 🎯 Red Team değerlendirmeleri
- ⚙️ OT zafiyet analizi
- 📊 Risk skorlaması & raporlama

⭐ Teknoser BT Güvenlik Değer Önerisi

- 🧩 Üretici bağımsız çözümler
- 🖼️ Geniş siber güvenlik uzman kadrosu

- 🛰️ SOC entegrasyonu
- TR Türkiye geneli mühendislik & saha desteği
- 🏗️ Uçtan uca mimari tasarım
- 📈 Sürekli izleme, raporlama & iyileştirme

🏭 OT Güvenlik Çözümleri (Endüstriyel Siber Güvenlik)

Endüstriyel Ortamlarda Güvenlik Artık Bir Seçenek Değil — Zorunluluk

Enerji, üretim, ulaşım ve kritik altyapılar gibi OT ortamları operasyonun kalbidir. Bu sistemlere yapılacak bir siber saldırı; üretim kaybına, operasyonel duruşlara ve hatta fiziksel zararlara neden olabilir.
Teknoser, Türkiye'nin lider OT güvenlik entegratörlerinden biri olarak endüstriyel ortamların görünür, izole, güvenli ve dayanıklı hale gelmesini sağlar.

🔎 OT Varlık Keşfi & Pasif İzleme

OT ortamlarındaki en büyük sorun görünürlük eksikliğidir.

Teknoser'in Sunduğu Hizmetler:

- 📡 Pasif trafik analizi ile OT varlık keşfi
- 📋 Arayüz, firmware, protokol & üretici bazlı envanter
- 🔍 Modbus, DNP3, S7, IEC104 vb. protokol analizi
- 🚨 Bilinmeyen cihaz & risk tespiti

📈 OT IDS / Anomali Tespiti

Sadece imza tabanlı tespit yeterli değildir. Davranış tabanlı anomali analizi kritik öneme sahiptir.

Yetkinliklerimiz:

- 👁️ Ağ davranış profilleme
- 🧪 Sahte komut tespiti

- 🔄 Beklenmeyen trafik akışı uyarıları
- 🔧 Süreç değişikliği tespiti
- 🛠️ ICS/SCADA odaklı tehdit tespiti

🧱 OT Segmentasyon & Güvenli Mimari Tasarımı

Teknoser, ISA/IEC 62443 standartlarına uygun ICS ağları tasarlar.

Kapsam:

- 🧩 Zone & Conduit mimarisi
- 🔐 OT DMZ tasarımı
- 🖥️ Jump Server mimarisi
- 🔥 Firewall / NGFW entegrasyonu
- 🔌 OT–IT ayrımı
- 🚫 Yanal hareket (lateral movement) engelleme

🩹 Güvenli Uzaktan Erişim (SRA)

Endüstriyel ortamlarda bakım ekipleri için uzaktan erişim ciddi risk taşır.

Sunduğumuz Çözümler:

- 🔐 Secure Remote Access (SRA)
- 🔑 MFA zorunluluğu
- 📹 Şifreli ve tamamen kayıt altına alınan oturumlar
- ✔️ Yetkilendirilmiş bakım iş akışları
- 🏭 Üretici erişim yönetimi

⚠️ OT Zafiyet & Risk Yönetimi

Patching yapılamayan OT cihazları için özel yaklaşımlar gerekir.

Öneriler:

- 🔎 OT odaklı zafiyet taramaları

- 📊 Cihaz bazlı risk skorlaması
- 🧠 Firmware, protokol & davranış analizi
- 📘 Raporlama & iyileştirme rehberi

🛡️ OT Firewall, Deception & Ağ Erişim Kontrolü

Kritik endüstriyel ortamlar için ileri seviye kontrol mekanizmaları.

Çözümler:

- 🔥 OT Firewall & ICS IPS
- 🤿 OT NAC çözümleri
- 🎭 OT Deception (honeypot / decoy sistemler)
- 📡 ICS protokol doğrulama
- 🚫 Yanal hareket engelleme

⭐ Teknoser OT Güvenlik Değer Önerisi

- 🎓 OT/ICS sertifikalı mühendislik ekibi
- ⚙️ Enerji, üretim, kamu, ulaşım & telekom deneyimi
- 🧱 Türkiye’nin en kapsamlı OT güvenlik portföylerinden biri
- 🧩 Üretici bağımsız mimari
- 🕒 24/7 operasyonel destek
- 🔄 IT–OT entegrasyon danışmanlığı
- 📐 IEC 62443 uyumlu mimari tasarım