Bilgi ve İletişim Güvenliği Rehberine Uyum Önerileri

Türk Telekom
Değerli Hissettirir

Bilgi ve İletişim Güvenliği Rehberi

Günümüzde dijital teknolojilerin hızla gelişimi ve son dönemlerde gerçekleştirilen siber saldırılar artık devletler düzeyinde ve daha yıkıcı olmasıyla birlikte veri ve dijital altyapılarının güvenliği çok daha kritik hale gelmiştir.

İlgili kurumlar tarafından uyulması gereken güvenlik tedbirlerini içeren, 30823 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Cumhurbaşkanlığı Genelgesi ülke çapında bilgi güvenliği seviyesini artırmaya yönelik önemli bir adımdır.

Amacı

Erişilebilirliği, bütünlüğü veya gizliliği ihlal edildiğinde kamu düzenini ve milli güvenliği tehdit edebilecek kritik veri ve bilgilerin korunması için gerekli güvenlik tedbirlerinin belirlenmesi ve uygulanması hedeflenmiştir.

Kapsamı

Bilgi işlem birimi bulunduran veya ilgili hizmetleri üçüncü partilerden temin eden, devlet kurum ve kuruluşları ve kritik altyapı hizmeti veren organizasyonları kapsamaktadır.

- Enerji
- Su Yönetimi
- Ulaştırma
- Finans & Bankacılık
- Sağlık
- Kritik altyapı işleten Özel Hukuk İşletmeleri

Bilgi ve İletişim Güvenliği Tedbirleri

Varlık Gruplarına Yönelik

- Ağ Ve Sistem Güvenliği
- Uygulama Ve Veri Güvenliği
- Taşınabilir Cihaz Ve Ortam Güvenliği
- IoT Güvenliği
- Farkındalık

Uygulama ve Teknolojilere Yönelik

- Kişisel Veri Güvenliği
- Anlık Mesajlaşma Güvenliği
- Bulut Bilişim Güvenliği
- Kripto Uygulamaları Güvenliği
- Kritik Altyapı Güvenliği

Güvenlik Sıkılaştırmalarına Yönelik

- İşletim Sistemi
- Veri Tabanı
- Sunucu

Bilgi ve İletişim Güvenliği Temel Prensipleri

İnsan

- Personel Yetkinliği
- Bilgi Erişim Yetkilendirme
- Asgari Yetki Tanımlama

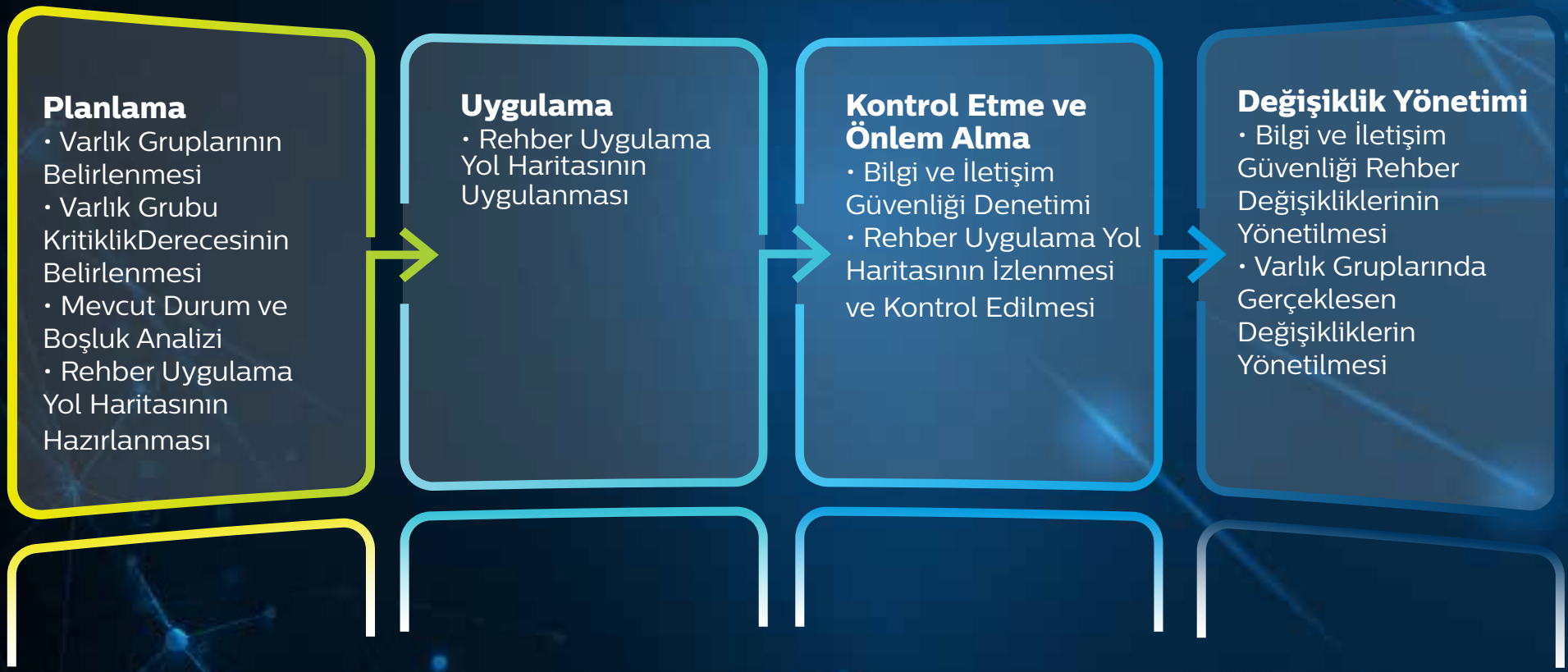
Teknoloji

- Katmanlı Koruma
- Saldırı Yüzey Optimizasyonu
- Yerli & Milli Ürün Kullanımı
- Mükerrer Çalışma ve Yatırım Optimizasyonu

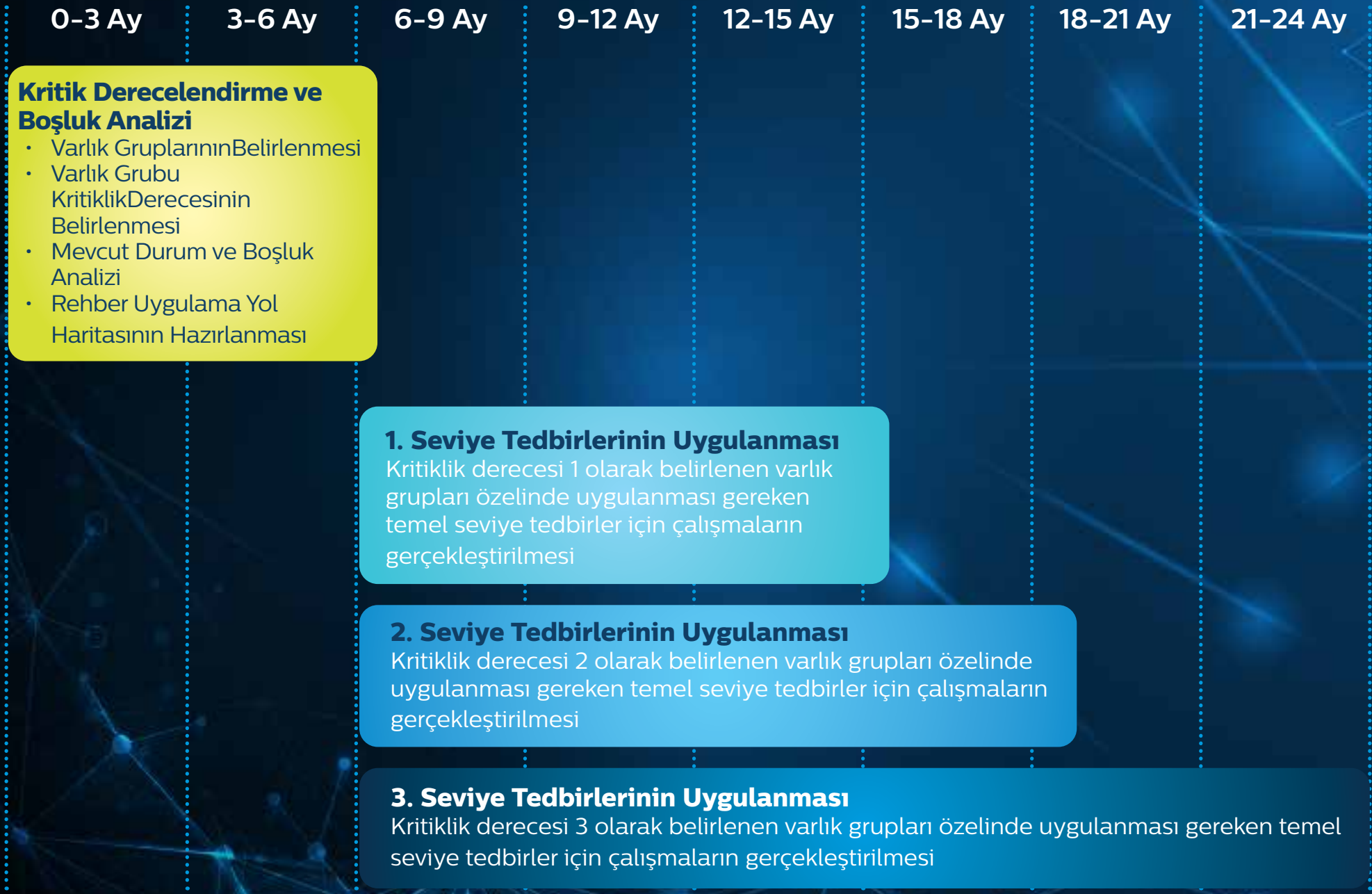
Süreç

- Güvenlik Temelli Tasarım
- Kişisel Veri Güvenliğine Göre Tasarım
- İş Hedefleriyle Uyumlu Güvenlik Tasarımları

Bilgi ve İletişim Güvenliği Rehberine Uyum Süreci



Rehber Uyum Planı



Rehbere Uyum Sürecinde Türk Telekom 7/24 Yanınızda

1. Seviye Tedbirler

- DDOS Atak Önleme
- DDOS7+
- Temel Siber Güvenlik
- APT
- SSL VPN
- 5651 Loglama
- 7/24 Olay Yönetimi
- KVKK Danışmanlığı
- Eğitim ve Farkındalık Faaliyetleri
- Sızma Testi
- EDR/MDR
- Sunucu Barındırma
- Bulut Sunucu ve Yedekleme Çözümleri
- Hizmet olarak yazılım çözümleri (Saas)

2. Seviye Tedbirler

- DDOS Atak Önleme
- DDOS7+
- Temel Siber Güvenlik
- APT
- WAF
- NAC
- SIEM Çözümleri
- Siber İstihbarat
- Siber Güvenlik Merkezi
- Güvenlik Simülasyon
- Red Team

3. Seviye Tedbirler

- DDOS Atak Önleme
- DDOS7+
- WAF
- 5651 Loglama
- DLP
- SIEM Çözümleri
- Siber Güvenlik Merkezi
- Güvenlik Simülasyon
- Red Team

Bilgi Güvenliği ve İletişimi Rehberine Yönelik Servislerimiz

Varlık Grubu Kritiklik Derecesinin Belirlenmesi

Varlık gruplarının belirlenmesinin ardından oluşabilecek güvenlik ihlallerinin etki alanları ve veri hacmi dikkate alınarak kritiklik dereceleri belirlenmesi için boşluk analiz çalışmaları planlanmalıdır.

İşlenen Veri Boyutu

- Bütünlük
- Gizlilik
- Erişebilirlik

Etki Alanı Boyutu

- Bağımlı Varlıklar
- Etkilenen Kişi Yüzeyi
- Finansal
- Sektörel Etki
- Marka Değeri

Bilgi Güvenliği ve İletişimi Rehberine Yönelik Servislerimiz

Varlıkların Belirlenip Kritiklik Seviyelerine Göre Önceliklendirilmesi

KVKK Danışmanlık Hizmeti

KVKK Danışmanlığı hizmetimiz ile müşterilerimizin KVK uyum süreçlerini tamamlanması için ihtiyaç duydukları desteği ve yönlendirmeyi sağlıyoruz.

Kişisel Verilerin Korunması Kanunu Nedir?

Kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemeyi amaçlamaktadır.

Kimler Kanuna Tabidir?

Herhangi bir nedenle kişisel veri işleyen tüm kurum ve kuruluşların süreçlerini KVKK Kanununa uygun hale getirme zorunluluğu bulunmaktadır.

KVKK'ya aykırılık halinde yaptırımlar ve cezalar nelerdir?

Veri güvenliğine aykırı durumda 29.503 TL'den 1.966.862 TL'ye kadar idari para cezası verilebilir. TCK 135 Kişisel verileri hukuka aykırı olarak kaydeden kimseye 1 yıldan 3 yıla kadar hapis cezası verilir.

Türk Telekom Olarak Neler Sunuyoruz?

KVKK yükümlülüklerinin hazırlanmasından farkındalık eğitimlerine kadar tüm süreci kapsayan hizmet içeriği

KVKK alanında deneyimli danışmanlık ekibiyle hizmet verilmesi

TL cinsinden peşin ve taksitli ödeme seçenekleriyle ödeme kolaylığı

Bilgi Güvenliği ve İletişimi Rehberine Yönelik Servislerimiz

Ağ ve Sistem Güvenliği

Temel Siber Güvenlik Paketi

Paket kapsamında Güvenlik Duvarı, İçerik Filtreleme, Antivirüs ve IPS hizmetlerinden omurga seviyesinde ve paylaşımlı modelde sunulmaktadır.

Gelişmiş Tehdit Önleme (APT)

Sıfırıncı gün ataklarına karşı omurga düzeyinde koruma sağlamaktadır. Dosya bazlı trafik analizi yaparak tehditlerin ağınıza bulaşması engellenir.

Veri Sızıntısı Önleme (DLP)

Data Loss Prevention(DLP) teknolojileri verinin bulunduğu depolama alanlarında ya da verinin transferi sırasında oluşabilecek kayıpları önlemektedir.

Veri Tabanı Aktivite İzleme (DAM)

Database Activity Monitoring (DAM), veri tabanında meydana gelen içerik değişimleri, erişim sağlayan kullanıcıların takibi gibi aktiviteleri izleyerek raporlama yapabilmektedir.

DDOS Atak Önleme

Türk Telekom paylaşımlı networkünde coğrafi yedekli yapıda kurulu altyapı ile farklı katmanlardaki DDOS ataklarına karşı koruma sunulmaktadır.

Yerel Ağ Erişim Kontrolü (NAC)

NAC, belirlenmiş güvenlik ilkeleriyle bir kuruluşun ağına erişimi kontrol etmek için üretilmiş ağ güvenliğini sağlamaktadır.

Bilgi Güvenliği ve İletişimi Rehberine Yönelik Servislerimiz

Uygulama Güvenliği

Web Uygulama Güvenik Duvarı (WAF)

Uygulama katmanında görev alarak son kullanıcı ile web sunucuları arasında oluşan trafik için filtreleme ve denetleme yaparak tehditleri engellemektedir.

DDOS7+

Uygulama protokollerini kullanarak yapılan DDOS ataklarına karşı Türk Telekom paylaşımlı networkünde kurulu cihazlar üzerinden sürekli koruma sağlayan hizmettir.

Bilgi Güvenliği ve İletişimi Rehberine Yönelik Servislerimiz

Uç Nokta ve Kullanıcı Güvenliği

Paylaşımlı SSL VPN

Sistemlerinize şirket ağı dışından yapılacak bağlantılarda, kullanıcıları doğrulayarak güvenli bir şekilde sistemlere erişimleri sağlanır.

Mobil Cihaz Yönetimi (MDM)

Mobil cihazların işletim sistemlerini ve uygulamaları denetleyerek zararlı yazılımlara ya da bağlantılara karşı mobil cihazınızın güvenliğini sağlanmaktadır.

Uç Nokta Güvenliği (Mcafee)

Uç cihaz güvenliği ile PC, MAC, akıllı telefon ve tabletler için virüslere, casus yazılımlara korsanlara, çevrimiçi sahtekarlıklara ve kimlik hırsızlıklarına yönelik koruma sağlanır.

Bilgi Güvenliği ve İletişimi Rehberine Yönelik Servislerimiz

Siber Güvenlik Merkezi

Kurumların siber tehditlere karşı günlük operasyonlarını çok yönlü ve uzman kadromuz ile tek noktadan kolaylaştırmak amacı ile Siber Güvenlik Merkezi Yönetim Hizmetimizi sunuyoruz.

Mevcutta SIEM altyapınız varsa ve bu altyapının yönetimi konusunda profesyonel bakış açısına ihtiyaç duyuyorsanız size özel paketler ile 7/24 Türk Telekom hizmeti yanınızda.

Türk Telekom Siber Güvenlik Portföyü

Paylaşımlı Güvenlik Hizmetleri

- DDOS Atak Önleme
- Cloud DDOS
- DDOS7+
- Gelişmiş Tehdit Önleme(APT)
- Web Uygulama Güvenlik Duvarı (WAF)
- Güvenlik Duvarı
- Aktif Savunma(IPS)
- İçerik Filtreleme
- Antivirüs

Siber Güvenlik Merkezi

- 7/24 Güvenlik Olay İzleme
- SIEM Danışmanlık
- Paylaşımlı SIEM
- Siber İstihbarat
- SOAR
- Güvenlik Test
- Risk & Uyumluluk
- Güvenlik Cihaz Yönetimi

Siber Güvenlik Çözümleri

- Atanmış Siber Güvenlik Servisleri
- Ağ ve Network Güvenlik Servisleri
- Kimlik Erişim Güvenliği
- UTM Çözümleri
- NAC
- DLP
- Uç Nokta Güvenliği
- Siber Güvenlik Eğitimleri
- Danışmanlık Hizmetleri

Türk Telekom Paylaşımlı Güvenlik Hizmetlerinde Öncü Olmaya Devam Ediyor

Türkiye'nin en geniş siber güvenlik ürün portföyüne sahibiz.

Türkiye'de ilk ve tek omurga seviyesinden uygulama katmanlı DDOS ataklara karşı DDOS7+ hizmetini sunuyoruz.

Volümetrik DDOS atakları açısından Türkiye'nin en büyük koruma kapasitesine sahibiz.

Tüm ulus için siber güvenlik stratejisi ile ilk bulut tabanlı APT ve WAF hizmetini müşterilerimizle buluşturuyoruz.

Türkiye'deki ilk ve tek bilinmeyen ataklara karşı koruma sağlayan APT(Gelişmiş Tehdit Önleme Hizmetini) omurga seviyesinden sunuyoruz.

Türk Telekom Siber Güvenlik Merkezi ile veri gizliliği ve bütünlüğünü korurken, kritik altyapıların kesintisiz çalışması için 7/24 hizmet sağlıyoruz.

Türk Telekom Milli Çözümler Üretiyor ve Yerli Üreticileri Destekliyor

Türk Telekom Siber Güvenlik Merkezi uzman mühendisleri tarafından hazırlanmış yerli milli DDOS Atak Simülasyonu ve Phishing Atak Simülasyonu ile müşterilerimizin olgunluk seviyelerinin ölçümlenmesine olanak sağlıyoruz.

Yerli ve milli SIEM çözümü ile müşterilerimize paylaşımlı SIEM hizmeti sunuyoruz.

Türkiye'de ilk yerli milli WAF hizmeti ile web uygulamalarınız proaktif yönetiyor ve 7/24 izliyoruz.

Yerli ve milli istihbarat çözümü ile müşterilerimize temel ve gelişmiş istihbarat verilerini sunuyoruz.

Siber Güvenlik Özel Çözümleri ile Siber Tehditlere Karşı Türk Telekom 7/24 yanınızda!

- 50’den fazla üretici ve çözüm ortağı ile iş geliştirme aktiviteleri
- Altyapı güvenliğinden uygulama güvenliğine kadar yeni teknolojilerle farklılaşan çözümler
- Güvenlik alanında uzmanlaşmış danışman kadromuz ile sektörel çözümler
- DLP,MDM,UTM, NAC, EDR,DAM, KVKK ve SIEM teknolojileri özelinde en uygun çözümün modellenerek farklı ticari modellerle alternatif oluşturma

Detaylı bilgi için satış yöneticiniz ya da bayiniz ile görüşebilirsiniz.

444 5 444 I turktelekom.com.tr
TT Mobil Telekomünikasyon A.Ş.
İşletme Merkezi
Gayrettepe Mahallesi. Yıldız Posta Caddesi. No:40 PK: 34349
Beşiktaş, İstanbul

Sicil No / Mersis No
506680/0859038032300012