1) Güvenlik Duvarı Hizmeti

Ağınızdaki sunucular arası ve/veya gelen-giden trafikler gerçek davranış analizleri doğrultusunda analiz edilerek olası 0.gün saldırısı, zararlı yazılımı barındıran trafikler engellenir.

2) Network Packet Broker Hizmeti

Ağ trafiği için gerekli filtreleme, tekilleştirme, çoğaltma ve paket düzeltme gibi optimizasyon işlemleri yapılarak bağlı olan sistemlere aktarımı sağlanmaktadır.

3) Otomasyon ve Orkestrasyon Hizmeti (SOAR)

SOAR sistemi ile kurumun varlık envanterindeki güvenlik cihazları arasında sağlanan entegrasyon ile alınacak loglar sistem tarafından incelenir. Güvenlik ihlali olması durumunda SOAR sistemi tarafından olay kaydı oluşturulur ve oluşturulacak senaryolar ile güvenlik zafiyetleri için otomatik olarak aksiyon alınır.

4) Olay Müdahale Hizmeti

Haftada 5 gün günde 8 saat esasına göre izleme kapsamında olan sistemlerde güvenlik olaylar için izleme yapılır.

5) Siber Tehdit İstihbarat Hizmeti

İhtiyaç duyulan tüm alan adları SSL sertifikaları bitiş (expire) süresine göre takip edilir ve olası zafiyet durumlarında kuruma bilgi verilir.

6) Sürekli Açıklık Tarama Hizmeti

En fazla 20 IP adresi veya Tam Alan Adı (Fully Qualified Domain Name –FQDN) üzerinde düzenli ve periyodik olarak zafiyet taraması gerçekleştirilir.

7) Uygulama Güvenlik Duvarı Hizmeti (WAF)

Belirlenen uygulamaların kullandığı teknolojiler, dosya uzantıları, URL'ler, parametreler incelenerek saldırı atak yüzeyleri belirlenir ve bu doğrultuda olası saldırı ve/veya veri sızıntısının önüne geçilmesi için gerekli aksiyonlar alınır.

8) Güvenli Erişim Hizmeti

Sunucuların tamamına erişim yönetim sistemi üzerinden ve tek bir noktadan RDP, SSH veya VNC kullanarak erişim sağlaması, ilgili bağlantılarının ekran kayıtlarının alınması ve erişim loğlarının saklanması sağlanır.

9) DDOS Engelleme Hizmeti

Türksat A.Ş. bünyesinde hizmet veren müşteri kaynakları için servis sağlayıcı DDoS engelleme sistemleriyle entegre çalışarak DDoS ataklarına karşı koruma sağlanır.

10) e-Posta Güvenliği Hizmeti

Belirlenen sayıda e-posta adresi (mailbox) için içeri ve dışarı yöndeki e-posta trafiğinde güvenlik denetimleri gerçekleştirilir.

11) e-Posta Sandbox Hizmeti

e-postalar ve ekleri sanal ortamlarda gerçek davranış analizleri doğrultusunda analiz edilerek olası 0.gün saldırısı, zararlı yazılım ve URL içeren bilgilerin e-posta içerisinde gelmesi engellenir.

12) Veri Tabanı Erişi Denetimi ve Güvenliği Hizmeti (DAM)

Tanımlı olan veritabanlarında DDL-DML gibi hareketlerin izlenmesi ve monitör edilmesi sağlanmaktadır.

13) Uç Nokta Tehdit Tespit ve Olay Müdahale Hizmeti (MDR)

EDR ajanının kurulu olduğu uç noktalar kapsamında, 7x24 esasına göre izleme hizmeti gerçekleştirilmektedir. Konusunda uzman olan analist ekibi altyapı içerisinde meydana gelen güvenlik olaylarını takip etmekte, tespit ve analiz ederek, olaylara müdahale etmekte ve gerekli bildirimleri yaparak iyileştirmeye devam etmektedir.

14) Akıllı Ağ Tespit ve Müdahale Hizmeti (NDR)

Belirlenen network yapısında konumlandırılan sistem ile birlikte ağ üzerinde gerçekleşen hareketler anomalilerinin yapay zeka ile tespitinin yapılması sağlanmaktadır.

15) Marka Koruma Hizmeti

Benzer alan adlarının tespiti ve bu alanların dolandırıcılık vb faaliyetlerinin belirlenmesi sağlanmaktadır.

16) Şifrelenmiş Trafik Analiz Sistemi Hizmeti (SSL VISIBILTY)

SSL/TLS bağlantıları için şifreleme/deşifreleme işlemleri yapılarak güvenlik seviyesinin artırılması sağlanmaktadır.

17) Olay Kayıt Toplama Hizmeti (SIEM)

Mevcutta yer alan varlık envanteri doğrultusunda aşağıdaki maddeler başta olmak üzere alınan parametreler üzerinden tanımlanmış güvenlik kuralları işletilir.

- Kullanıcı kimlikleri,
- Oturum açma-kapatma kayıtları,
- Veri ekleme, veri silme, veri değiştirme gibi işlemlerin tarihi ve zamanı,
- Bağlantı sağlanan ekipmanın kimliği ve yeri,
- Başarılı ya da reddedilen sistem, veri ve kaynaklara erişim kayıtları