

TEST VE İZLEME

Endpoint Security İzleme Hizmeti

Bilgisayar, sunucu ve mobil cihaz gibi uç noktalarınızı gelişmiş uç nokta güvenliği (EDR/XDR) çözümleriyle izleyip tehditleri erken tespit etmenize destek oluyoruz.

6

kapsam alanı

5

adımlı yöntem

6

teslim edilen çıktı

// NEDEN ÖNEMLİ?

Neden önemli?

Saldırıların büyük bölümü bir uç noktada başlar: bir ortalama e-postası, zararlı bir dosya, ele geçirilmiş bir hesap. Uç nokta görünürlüğü olmadan saldırının nerede ve nasıl ilerlediğini anlamak zordur. Marka bağımsız çalışır, mevcut altyapınıza uygun çözümü birlikte seçeriz.



İzleme operasyonunun kurum içinde mi yoksa dışarıdan mı yürütüleceği kapsamınıza göre belirlenir. Görüşmede ihtiyacınızı birlikte netleştiririz.

// KİMLER İÇİN?

Bu hizmet kimler için uygun?



Uzaktan veya hibrit çalışan ekipleri olan kuruluşlar



Klasik antivirüsten gelişmiş koruma modeline geçmek isteyenler



Fidye yazılımı riskini azaltmak isteyenler



Uç noktalarda merkezi görünürlük arayan BT ekipleri

// KAPSAM

Neleri kapsıyor?

**Uç nokta envanteri ve risk**

Cihaz türlerinizi, işletim sistemlerinizi ve riskleri çıkarınız.

**EDR/XDR seçimi ve kurulumu**

İhtiyacınıza uygun çözümü seçmenize ve devreye almanıza destek oluruz.

**Politika ve sertleştirme**

Cihaz güvenlik politikalarını ve temel sertleştirme ayarlarını tanımlarız.

**İzleme ve uyarı ayarı**

Panoları ve uyarıları kurar, yanlış alarmları azaltırız.

**Olay triyajı**

Uyarıların incelenmesi, önceliklendirilmesi ve müdahale adımlarını tanımlarız.

**SIEM ve SOC entegrasyonu**

Uç nokta verilerini merkezi izleme altyapınızla ilişkilendiririz.

Saldırgan gibi düşünür, savunmacı gibi inşa ederiz.

// ÇALIŞMA YÖNTEMİ

Nasıl ilerliyoruz?

1

Mevcut durum ve ihtiyaç analizi

Cihaz envanterini, mevcut korumayı ve beklentileri değerlendiririz.

2

Çözüm seçimi ve mimari

Ürün bağımsız olarak size uygun çözümü ve mimariyi belirleriz.

3

Kurulum ve politika

Pilot gruplarla başlayıp çözümü kademeli olarak yaygınlaştırırız.

4

İzleme ve uyarı ayarı

Uyarıları ve panoları ortamınıza göre ayarlarız.

5

Operasyon ve iyileştirme

Düzenli raporlama ve gözden geçirmelerle izleme sürecini geliştiririz.

// ÇIKTILAR

Neler teslim ediyoruz?



Uç nokta envanteri



Politika ve sertleştirme dokümanı



Olay triyaj ve müdahale iş akışı



Çözüm ve mimari önerisi



İzleme panoları



Düzenli izleme raporları

// GÖRSEL ANLATIM

Konuya özel görseller

Uç nokta izleme mimarisi

Her cihazdaki ajan telemetriyi merkeze iletir; konsol tehditleri tespit eder ve yanıt aksiyonlarını tetikler.

**Görünürlük**

Her cihazdan sürekli telemetri toplanır.

Davranış bazlı tespit

İmzası olmayan tehditler de olağandışı davranıştan yakalanır.

Hızlı yanıt

Şüpheli cihaz ağdan izole edilir, zararlı etkinlik geri alınır.

Bir uç nokta olayında müdahale akışı

Şüpheli davranıştan düzeltmeye kadar adımlar.

**Dakikalar önemli**

Tespitten izolasyona geçen süre, olayın yayılmasını belirler.

Tüm filoda tarama

Bulunan göstere diğer cihazlarda da aranır.

Öğrenen sistem

Olay sonrası tespit kuralları iyileştirilir.

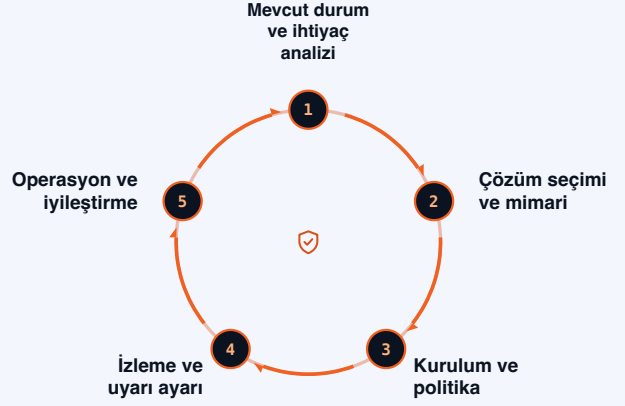
// GÖRSEL ÖZET

Hizmete genel bakış

KAPSAM HARİTASI



UYGULAMA DÖNGÜMÜZ



// TEK ÇATI ALTINDA

Diğer hizmetlerimiz

- | | | |
|---|--|--|
|  ISO 27001 Danışmanlığı |  ISO 22301 Danışmanlığı |  ISO 14298 Danışmanlığı |
|  KVKK Uyum Danışmanlığı |  Siber Güvenlik Danışmanlığı |  Risk Yönetimi Danışmanlığı |
|  Sızma Testi |  Düzenli Zafiyet Tarama ve Yönetimi |  DoS, DDoS Testleri ve Koruma Hizmeti |
|  SOC / SIEM Kurulumu |  Güvenli Yazılım Geliştirme |  Bilgi Güvenliği Farkındalık Programı |
|  Olay Müdahale Hazırlığı | | |

// İLETİŞİM

Bize ulaşın

İhtiyacınızı ve mevcut durumunuzu paylaşın; size uygun kapsamı ve yol haritasını birlikte belirleyelim. Bilgi formumuzu doldurabilir veya doğrudan bize ulaşabilirsiniz.

Troy Bilgi Teknolojileri Ticaret Limited Şirketi

Atatürk Mah. Vedat Günyol Cad. 44M/2

Ataşehir / İstanbul

T 0-216-575 5222 **E** info@troybilgiteknolojileri.com



Hizmet sayfası ve bilgi formu için QR kodu okutun