VOO IT SOLUTIONS

BİLGİ GÜVENLİĞİ HİZMETLERİ

sec IT Teknoloji Çözümleri

IT Güvenliğiniz Emin Ellerde

SIEM & Monitoring | SOC Hizmetleri | Siber Güvenlik Danışmanlığı

Göremiyorsanız, koruyamazsınız!

NEDEN SİBER GÜVENLİK?

Tehditler Artık Kaçınılmaz

%43

Siber saldırılar KOBİ'leri de hedef alır

287

Bir bilgisayar korsanının sisteminizde siz fark etmeden ortalama keşif süresi (gün)

₺12M+

Olay başına ortalama veri ihlali maliyeti

Olay müdahalesi ve adli analiz masrafları, regülatör cezaları, müşteri bildirimi ve itibar kaybı, hukuki süreçler, iş kesintisi kayıpları

%95

İhlallerde insan hatasının payı

Orta-Büyük Ölçekli İşletmeler İçin Gerçek Risk

KOBİ'lerin büyük bir kısmı ciddi bir siber saldırının ardından ağır mali zarara uğruyor. Büyük firmalarınnın çoğunda bile siber güvenlik ekibi olmayabiliyor — Voo Bilişim olarak bu boşluğu doldurmayı hedefliyoruz.

Kaynak: IBM Cost of Data Breach Report, Verizon DBIR

SIEM NEDİR?

Security Information and Event Management

SIEM tek başına bir ürün değil, bir güvenlik disiplinidir.

Firewall, sunucu, switch, VPN gibi onlarca farklı sistemden gelen logları tek noktada toplayan SIEM; korelasyon motoruyla tehditleri tespit eder, güvenlik ekibine aksiyon alabilecekleri bilgileri sunar.

SIEM NEDEN GEREKLİDİR?

Göremediğinizi Koruyamazsınız

Görünürlük

Ortalama 20 cihazdan günde milyonlarca log üretilir. İnsan gözüyle izlemek imkânsızdır.

Korelasyon

Tek başına anlamsız olaylar, birlikte değerlendirildiğinde saldırıyı ortaya çıkarır.

Kanıt & Uyumluluk

KVKK, ISO 27001 ve denetim süreçleri için tarihsel log kaydı zorunludur.

İçeriden Tehdit

Çalışan davranış anomalileri (dosya silme, yetkisiz erişim) erken tespit edilir.

Erken Uyarı

Fidye yazılımı harekete geçmeden önce davranışsal belirtiler yakalanır.

Trend Analizi

Tekrarlayan olaylar görünür hale gelir, altyapı güçlendirme kararları verilebilir.

MONİTORİNG NEDEN ÖNEMLİDİR?

Altyapınızın Nabzını Tutun

Zabbix + Grafana

İzleme Platformu

- CPU, RAM, disk kullanımı
- Servis durumu izleme
- Ağ bant genişliği
- Özel eşik değeri uyarıları
- Tarihsel trend grafikleri

Kesinti Öncesi Tespit

Disk dolmadan, servis çökmeden önce uyarı alırsınız.

Performans Optimizasyonu

Darboğazları görerek kaynakları verimli kullanırsınız.

Kapasite Planlaması

Büyüme trendlerini izleyerek altyapı yatırımlarını önceden planlarsınız.

"DNS servisimiz durdu" — Bu uyarıyı Monitör eden yazılımdan mı öğrenmek istersiniz, yoksa çalışanlarınızın şikayetinden mi?

HİZMET PAKETLERİ

İhtiyacınıza Göre Ölçeklenebilir Çözümler

Paket 1

ISO 27001 / GDPR / KVKK UYUMLULUĞU

- ✓ Log toplama & saklama (2 yıl)
- ✓ Wazuh + Grafana dashboard
- ✓ Bildirim (e-posta/Slack/Teams vd.)
- ✓ Aylık özet rapor
- ✓ Agent kurulum rehberliği

Bu hizmet, teknik ekibi olan ve izleme/uyarı süreçlerini kendi içinde yönetmek isteyen firmalara yöneliktir. Log analiz danışmanlığı bu kapsamda yer almamaktadır.

Paket 2

KAPSAMLI SIEM KULLANIMI

- ✓ Paket 1 + SIEM Korelasyon
- ✓ Kural seti tanımı
- ✓ Her alert için açıklama notu
- ✓ Aylık tehdit raporu
- ✓ 5x8 saat danışmanlık

Sistemlerine özel kurallar tanımlamak, bu kurallara uygun uyarıları görüntülemek ve e-posta üzerinden destek almak isteyen firmalar için tasarlanmıştır.

Paket 3

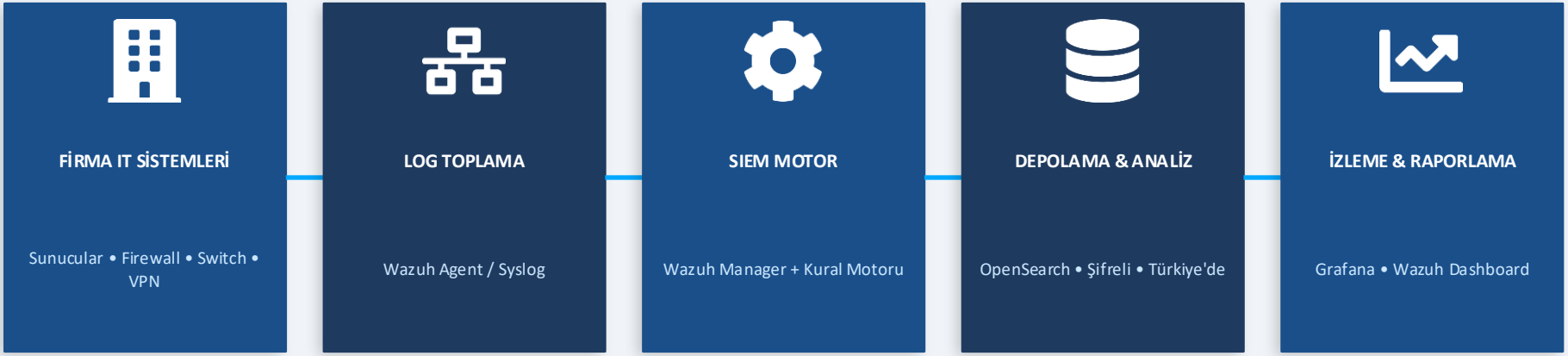
YÖNETİLEN SOC

- ✓ Paket 2 + 7x24 proaktif SOC izleme
- ✓ Tanımlı bildirim SLA
- ✓ Log zinciri olay analizi
- ✓ Sınırsız danışmanlık
- ✓ Aylık tehdit istihbarat brifingi

SOC hizmetini tamamen dış kaynaktan almak isteyen firmalar
Paket 3+ (sistemlere müdahale) için satış birimimizle görüşebilirsiniz.

MİMARİ VE VERİ GÜVENLİĞİ

Altyapınız Bizde Güvende



Tenant İzolasyonu

Her müşteri verisini ayrı index ve RBAC rolleriyle koruma altına alıyoruz.

Türkiye'de Barındırma

Tüm altyapı Türkiye'dedir. Yurt dışına veri transferi yapılmaz.

KVKK Uyumu

Veri İşleyen sıfatıyla KVKK yükümlülüklerini karşılayan prosedürler uygulanır.

Veri Sürekliliği

Günlük snapshot, haftalık tam yedekleme. RTO: 4 saat, RPO: 24 saat.

ÜCRETLENDİRME MODELİ

Neye Göre Fiyatlandırıyoruz?

Cihaz / Agent Sayısı

İzlenen sunucu, güvenlik duvarı ve ağ cihazı adedi. Fiyatlandırma cihaz sayısına dayanır.

Log Hacmi

Log hacmi (EPS) ücretlendirmeyi etkilemez.

Hizmet Paketi

Pasif izleme yaklaşımından aktif SOC modeline geçildikçe insan kaynağı ihtiyacı ve SLA taahhüt seviyesi artar; bu durum ücretlendirmeye yansır.

Sözleşme Süresi

12 veya 24 aylık taahhütlerde yıllık fiyatlandırma ile tasarruf sağlanır.

✦ *Sabit aylık ücret — sürpriz fatura yok. Kurulum bedeli tek seferdir. Teklif için teknik ön değerlendirme toplantısı yeterlidir.*

NEDEN VOO BİLİŞİM?

Farkımızı Ortaya Koyan 6 Unsur

Siber Güvenlik Odağında Hizmet

Sadece log toplamıyor, güncel tehditleri takip ediyor ve anlıyoruz. 15 yıl üzerindeki tecrübemizi yansıtıyoruz.

Firmanıza Özel Tasarım

Diğer SIEM'lerin karmaşıklığınının aksine anlaşılır ve kolay yönetim.

KVKK Uyumlu

Verileriniz Türkiye'de, hukuki çerçevede işleniyor.

Aksiyon Önerisi İçeren Bildirimler

Sadece uyarmıyor, ne yapmanız gerektiğini söylüyoruz.

Şeffaf SLA

Bildirim sürelerini yazılı taahhütle sunuyoruz.

Ölçeklenebilir

İhtiyaçlarınız arttıkça paketinizi yükseltebilirsiniz.

SONRAKİ ADIMLAR

Hemen Başlayalım

01

Teknik Ön Değerlendirme

Sistem envanterinizi ve ihtiyaçlarınızı birlikte değerlendiriyoruz.

02

Paket Seçimi ve Teklif

Cihaz sayınıza ve paket seçiminize göre kişiselleştirilmiş teklif hazırlıyoruz.

03

Sözleşme ve KVKK

MSA ve Veri İşleme Sözleşmesi imzalanır.

04

Onboarding (3-7 İş Günü)

Tenant kurulumu, agent deployment ve kabul testi tamamlanır.

destek@voo.com.tr | +90 (212) 222 34 56 | www.voo.com.tr - www.secit.com.tr