infoblox.

# EN ÖNEMLİ 7 NEDEN DNS MTTRs GÜVENLİK UZMANLARI İÇİN

**DNS artık sadece ağ oluşturma için değil.**

DNS, genişleyen ağ altyapınızın güvenliğini sağlamak ve Ortalama Yanıt Verme Sürenizi (MTTR) azaltmak için ilk savunma hattı olarak giderek daha hayati bir önem taşıyor.

## KRITIK GÜVENLIK SORUNLARIYLA KARŞI KARŞIYASINIZ:

### Genişleyen saldırı yüzeyi

WFA ve çoklu bulut ihtiyaçları arttıkça, malware, C2, lookalikes ve diğer tehditlerin mevcut savunma yöntemlerini atlatması daha kolay hale geliyor.

### Kullanıcı ve cihaz kör noktaları

Güvenlik araçları, çoklu bulut ve IoT/OT dahil olmak üzere tüm ağ kullanıcıları ve cihazlarının tümleşik ve gerçek zamanlı görüntüsüne sahip değil.

### Hayati kaynakların eksikliği

Güvenlik yöntemlerindeki açıklar ve bunun sonucunda SecOps üzerinde oluşan yük, kritik uyarıların her gün gözden kaçtığı anlamına geliyor veya haftalık olarak.

### Yavaş araştırma ve düzeltme

Kullanıcı ve cihaz bilgilerine erişimin uzun sürmesi, yapılması gereken diğer sorguları da geciktirir. Dolayısıyla tehditlerin bekleme sürelerini uzatarak işletmenizi daha fazla zarara maruz bırakır.

**$4M**

Ortalama maliyeti bir veli ihlalinin

**270+**

Ortalama olarak saat tehditleri tanımlayın ve kontrol altına alın

**92%**

Komuta ve kontrol için DNS'den tehditleri tanımlamak ve kontrol altına almak

## DNS ALGILAMA VE YANITLAMASI BU ZORLUKLARI VE DAHA FAZLASINI ÇÖZMENIZE YARDIMCI OLUR:

1. **Tehditleri daha erken tespit edin**
   DNS sorgularını kullanıcı ve cihazla eşleme IPAM kullanarak gerçek zamanlı etkinlik DNS tabanlı uygulama keşfi.
2. **Saldırıları daha hızlı durdurun**
   Kimlik avı, fidye yazılımı ve kötü amaçlı yazılımları engellemek için gelişmiş tehdit istihbaratını kullanın, C2, DGA, veri aktarımı ve diğerleri daha erken.
3. **Sistemleri her yerde koruyun**
   Bulutlar arasında savunma yaparak genişleyen saldırı yüzeyini koruyun ve IoT/OT dahil olmak üzere uçta.
4. **Ortaya çıkan tehditleri engelleyin**
   Küresel tehdit avcılığından yararlanarak şüpheli alan adlarını algılayın ve 3 ay kadar önceden engelleyin.
5. **Lookalike alan adlarını kapatın**
   DNS sorgularında AI/ML analizlerini kullanarak DGA'ları, veri sızıntılarını ve sofistike Lookalike alan adlarını daha hızlı algılayın.
6. **Güvenlik yatırımlarınızın getirisini otomatize edin**
   DNS verilerini SOC araçlarıyla paylaşmak için ekosistem entegrasyonlarını otomatikleştirin ve SecOps'un uyarıları daha iyi önceliklendirmesine ve iş yükünü en aza indirmesine olanak tanır.
7. **Daha az kaynak kullanın**
   Tehditleri daha erken görüp durdurmak için ağ ve güvenlik bilgilerini birleştirin ve SecOps'tan maksimum faydayı alın.

# DNS MTTRs

**Infoblox'un nasıl çalıştığı hakkında daha fazla bilgi edinin DNS Algılama ve Yanıtlama**

proaktif güvenliğinizi geliştirerek ve kuruluşunuzda Ortalama Yanıt Süresini hızlandırarak kuruluşunuz genelinde ortalama yanıt süresi.

**Göz atın Forrester Total Economic Impact™ çalışmasına göz atın**