# Security Onion Nedir ve Nasıl Kurulur?

## Security Onion Nedir?

Security Onion, ağ güvenliği izleme, tehdit avı ve günlük analizi için kullanılan ücretsiz ve açık kaynaklı bir Linux dağıtımıdır. IDS (Saldırı Tespit Sistemi), NSM (Ağ Güvenliği İzleme) ve log yönetimi gibi birçok güvenlik aracı içerir. Özellikle kurum ağlarında anormallikleri tespit etmek ve analiz etmek için kullanılır. İçerisinde Zeek, Suricata, Wazuh, TheHive, Kibana, Elasticsearch gibi güçlü araçlar barındırır.

## Neden Security Onion Kullanılır?

- Ağ trafiğini gerçek zamanlı izleyebilmek için  
- Saldırı tespiti ve olay müdahalesi yapmak için  
- Olay günlüklerini merkezi olarak toplamak ve analiz etmek için  
- Tehdit istihbaratını entegre edip saldırıları analiz etmek için

## Kurulum Adımları

1. Security Onion ISO dosyasını resmi web sitesinden indirin: https://securityonion.net  
2. ISO dosyasını bir USB'ye yazdırın ya da sanal makine (VMware, VirtualBox) için kullanın.  
3. Sistemi başlatın ve GUI arayüzü ile kuruluma başlayın.  
4. Ağ yapılandırmasını yapın (genellikle bir yönetim arabirimi ve bir izleme arabirimi gerekir).  
5. Rolünüzü seçin (standalone, manager, sensor vs.).  
6. Sistem otomatik olarak gerekli bileşenleri yükleyecektir.

## Security Onion Başlatma

Kurulumdan sonra sistem açıldığında otomatik olarak arka planda bileşenler çalışır. Ancak elle başlatmak ya da durumu görmek için şu komutlar kullanılabilir:

Security Onion servislerini başlatmak:  
sudo so-start  
  
Servis durumunu kontrol etmek:  
sudo so-status  
  
Web arayüzüne erişim (örneğin Kibana):  
https://<IP-adresiniz>