SCADA'nın Siber Güvenlik Yazılımları ile Entegre Edilmesi

Endüstriyel otomasyon sistemlerinin merkezinde yer alan SCADA yazılımları, sahadaki cihazlarla tesis operasyonlarını izlemek ve kontrol etmek için kritik rol oynar. Bu sistemlerin internet ve kurumsal ağlarla giderek daha fazla entegre olması, siber tehditlere karşı güvenlik önlemlerini zorunlu kılmaktadır.

SCADA sistemleri, geleneksel Bilişim Teknolojileri altyapılarından farklı olarak gerçek zamanlı verilerle çalışır ve doğrudan fiziksel süreçleri etkiler. Bu nedenle bir siber saldırı yalnızca bilgi kaybına değil, üretim durması, ekipman hasarı veya çevresel tehlikelere kadar varabilecek sonuçlara neden olabilir. Bu risklerin önlenmesi için SCADA sistemlerinin gelişmiş siber güvenlik yazılımlarıyla entegre edilmesi hayati önem taşır.

SCADA ile siber güvenlik yazılımları arasındaki entegrasyon, aşağıdaki unsurlar üzerinden gerçekleştirilir:

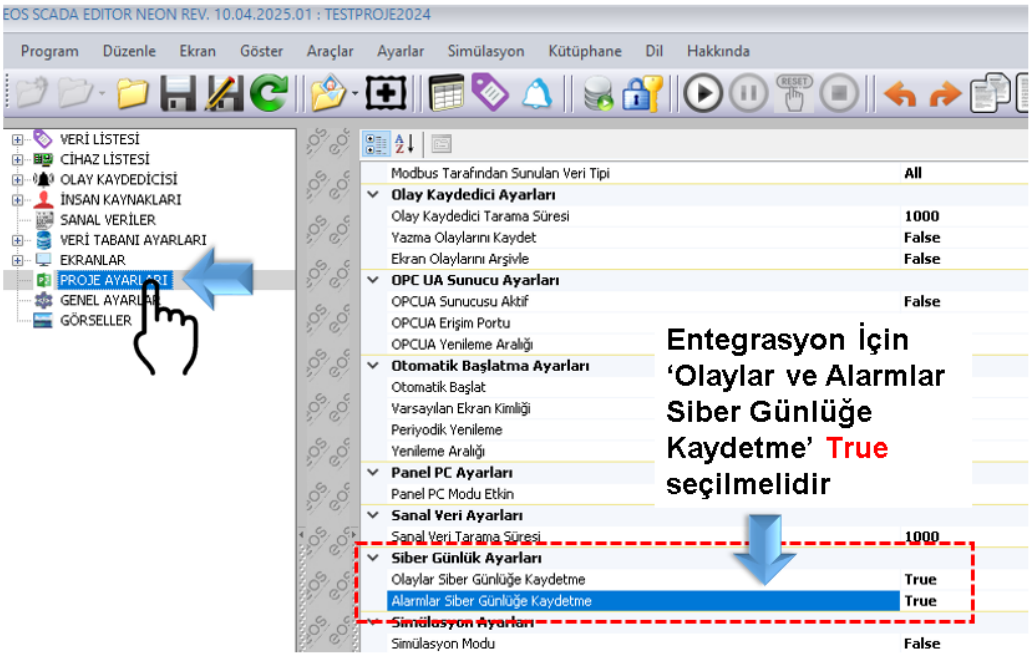
- **Ağ İzleme ve Anomali Tespiti:** SCADA ağı içerisindeki trafik, güvenlik yazılımları tarafından sürekli analiz edilerek olağan dışı davranışlar (örneğin beklenmedik komutlar, kimlik doğrulama hataları) tespit edilir.

- **Kimlik ve Erişim Yönetimi (IAM):** Kullanıcıların rollerine göre erişim hakları tanımlanır; sadece yetkili personelin kritik bileşenlere erişimi sağlanır.

- **Günlük Kayıtları ve İzleme (Log Management):** SCADA sisteminde gerçekleşen tüm olaylar merkezi güvenlik yazılımları tarafından kaydedilir, analiz edilir ve gerektiğinde uyarı üretir.

- **Güvenli Protokoller:** SCADA ile saha cihazları ve diğer sistemler arasındaki iletişim, şifreleme ile korunur.

Bu özelliği SCADA'da aktif hale getirmek için EDITOR yazılımına proje yüklenerek, Proje Ayarlarına tıklanmalı ve **Siber Günlük Ayarları** altında bulunan ***Olaylar Siber Günlüğe Kaydetme*** ve ***Alarmlar Siber Günlüğe Kaydetme***; **True** olarak seçilmelidir.



Proje saklanarak, işlem tamamlanmalıdır.

DİKKAT: SCADA sisteminin güvenlik yazılımlarıyla entegrasyonu, yalnızca bilgi güvenliği değil; aynı zamanda operasyonel verimlilik, süreklilik ve itibarı korumak için de stratejik bir adımdır. Entegre ve proaktif bir güvenlik yaklaşımı, modern endüstriyel tesislerin en güçlü savunma hattını oluşturur.