

CyDecSys

Siber Güvenlik

Karar Destek Sistemi



- Bütünleşik siber güvenlik durum tespit, analiz ve karar destek sistemidir.
- Bilgisayar ağlarının siber güvenlik resmini sunarak durumsal farkındalık oluşturur.
- Karar vericilere analiz sonuçları ile destek sağlar.

CyDecSys

Siber Güvenlik Karar Destek Sistemi

Ana Özellikler

- Ağ topolojisi oluşturulması ve ağdaki varlıkların tespiti ile durumsal farkındalık yaratılması
- Ağ topolojisi ve varlıklar üzerindeki zafiyetlerin tespiti ile saldırı yüzeyinin belirlenmesi
- Zafiyetlerin ağ ve varlıklar üzerinde yarattığı risklerin ayrıntılı analizi (Temel ve tehdit tabanlı metodolojik risk algoritmaları ile)
- Saldırı ağacı üzerinde tehdit tabanlı ve çok adımlı saldırı simülasyonu
- Koruyucu önlem senaryoları ile risk analizi
- Zafiyet analizi yapabilmek için zenginleştirilmiş ve doğrulanmış zafiyet veri tabanı

Ağ Keşfi, Cihaz ve Zafiyet Tarama

- Fiziksel ağ topolojisinin (alt ağlar, aktif ağ cihazları ve yapılandırmaları) keşfi
- Ürün spesifik ve açık protokol (SNMP vb.) tabanlı yöntemlerle ağ keşfi
- Ağ üzerindeki cihazların, yazılımların, açık port ve servislerin tespiti
- Zafiyetlerin dağıtık mimaride yüksek performanslı olarak taranması ve tespiti

Siber Güvenlik Risk Analizi ve Simülasyonu

- Tehditlerin tanımlanması ve yönetimi
- Çok adımlı saldırı yollarının tespit edilmesi ve saldırı ağacı ile gösterimi
- Cihaz, zafiyet, alt ağlar, ürünler vb. bileşenlerin risklerinin temel ve tehdit bazlı istatistiksel gösterimi
- Zafiyetlerin giderilmesine yönelik koruyucu önlemlerin sonuçlarının simüle edilmesi
- Koruyucu önlem senaryoları ile sağlanabilecek iyileştirmenin / risk değişiminin incelenebilmesi

Zenginleştirilmiş Zafiyet Veri Tabanı

- Zafiyet verilerinin ilişkilendirilmesi, sınıflandırılması, hata ayıklaması ve zenginleştirilmesi ile oluşturulan zafiyet veri tabanı
- Zafiyet, zayıflık, ürün, istismar (exploit) vb. bilgilerin ilişkilendirilmesi
- Zafiyetlerin istismarı için ayrıcalık ön koşulları ve olası sonuçlarının (makine öğrenimi gibi yöntemlerle) üretilmesi
- Zafiyetlerin analizi için detaylı sorgu yeteneği