Avantajları

Güvenlik İzleme ve Tehdit Algılama

Sysmon, birçok güvenlik olayını izleyebilir ve bu olayları detaylı bir şekildekaydedebilir. Bu, bilgisayar ağlarını ve sistemlerini izlemek ve güvenlik tehditlerini tespit etmek için çok faydalıdır.

Özelleştirilebilirlik

Sysmon, kullanıcıların ihtiyaçlarına göre özelleştirilebilir. İzlenmesi gereken belirli olayları seçebilir, kayıt seviyelerini ayarlayabilir ve güvenlik politikalarını uyarlayabilirsiniz.

Detaylı Bilgi

Sysmon, izlediği olaylar hakkında detaylı bilgi sağlar. Bu, güvenlik profesyonellerinin olayları daha iyi anlamalarını ve analiz etmelerini sağlar.

Uygulama Bağımsız

Sysmon, Windows işletim sistemi üzerinde çalışan bir hizmet olarak bağımsızdır ve farklı uygulamalarla uyumlu çalışabilir.

Ücretsiz

Sysmon, Microsoft tarafından ücretsiz olarak sunulan bir araçtır.

Revision #1
Created 27 January 2024 15:54:11 by Ertan Sözer
Updated 27 January 2024 15:55:13 by Ertan Sözer