Avantajları ve Dezavantajları

- Avantajları
- Dezavantajları

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.

Dezavantajları

Yanlış Pozitifler

Sysmon, karmaşık güvenlik olayları hakkında ayrıntılı bilgi sağlar, ancak bu aynı zamanda yanlış pozitiflerin ortaya çıkma olasılığını artırabilir. Yanlış pozitifler, güvenlik profesyonellerinin zamanını boşa harcayabilir.

Yüksek Veri Hacmi

Sysmon, çok sayıda güvenlik olayını izlediği için büyük miktarda veri üretebilir. Bu veriyi toplamak, depolamak ve analiz etmek, kaynak ve bant genişliği gerektirebilir.

Yapılandırma Karmaşıklığı

Sysmon'un tam olarak yapılandırılması ve ayarlanması, deneyim ve bilgi gerektirebilir.Yanlış yapılandırma, eksiklikler veya hatalar güvenlik açıklarına yol açabilir.

Performans Etkisi

Sysmon'un sürekli olarak çalışması, sistem performansına küçük bir etki yapabilir. Bu, özellikle yüksek trafikli sistemlerde veya düşük kaynaklı sistemlerde bir sorun olabilir.

Sistem Uyumu

Sysmon, özellikle eski veya sınırlı kaynaklara sahip sistemlerde çalışmayabilir.