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.

Revision #1
Created 27 January 2024 15:55:17 by Ertan Sözer
Updated 27 January 2024 15:57:17 by Ertan Sözer