Sysmon nedir?

"System Monitor” kelimelerinin kısaltması olan Sysmon, Microsoft'un geliştirdiği bir güvenlik yazılımıdır. Sysmon,Windows işletim sistemi üzerinde çalışan bir hizmet olarak kullanılır ve sistemdeki olayları izlemek, güvenlik tehditlerini tespit etmek ve sorun gidermek için tasarlanmıştır. Bu yazılım, özellikle bilgisayar ağlarını ve sistemleri koruma amacıyla kullanılır. Sysmon, birçok önemli sistem olayını ayrıntılı bir şekilde kaydeder. Bu kayıtlar; güvenliktehditlerini izleme, tespit etme ve analiz etme konusunda önemli bilgiler sağlar.

Sysmon; Hizmet ve sürücü yüklemeleri, Kayıt defteri değişiklikleri, Ağ bağlantıları ve bağlantı kesmeleri, Hizmet ve sürücü yüklemeleri, Dosya değişiklikleri ve izinsiz erişim girişimleri, Güçlü şifrelemeyi kullanarak veri şifreleme işlemleri, Oturum açma ve oturumu kapatma işlemleri gibi bir dizi olayı günlüğe kaydeder. Bu günlükler güvenlik analizleri tarafından sorun giderme süreçlerinde kullanılabilir.

Revision #1
Created 27 January 2024 15:53:23 by Ertan Sözer
Updated 27 January 2024 15:53:51 by Ertan Sözer