

Sysmon Nedir?

- [Sysmon nedir?](#)

Sysmon nedir?

"System Monitor" kelimelerinin kısaltması olan Sysmon, Microsoft'un geliřtirdiđi bir gvenlik yazılımıdır. Sysmon,Windows iřletim sistemi zerinde alıřan bir hizmet olarak kullanılır ve sistemdeki olayları izlemek, gvenlik tehditlerini tespit etmek ve sorun gidermek iin tasarlanmıřtır. Bu yazılım, zellikle bilgisayar ađlarını ve sistemleri koruma amacıyla kullanılır. Sysmon, birok nemli sistem olayını ayrıntılı bir řekilde kaydeder. Bu kayıtlar; gvenliktehditlerini izleme, tespit etme ve analiz etme konusunda nemli bilgiler sađlar.

Sysmon; Hizmet ve src yklemeleri, Kayıt defteri deđiřiklikleri, Ađ bađlantıları ve bađlantı kesmeleri, Hizmet ve src yklemeleri, Dosya deđiřiklikleri ve izinsiz eriřim giriřimleri, Gl řifrelemeyi kullanarak veri řifreleme iřlemleri, Oturum ama ve oturumu kapatma iřlemleri gibi bir dizi olayı gnlđe kaydeder. Bu gnlkler gvenlik analizleri tarafından sorun giderme srelerinde kullanılabilir.