**🔍 Sysmon Nedir?**

**Sysmon (System Monitor)**, Microsoft’un Sysinternals araçları arasında yer alan, sistemdeki olayları detaylı bir şekilde izlemeyi sağlayan bir güvenlik izleme aracıdır.

**✅ Temel Özellikleri:**

* İşlem oluşturma (Process Creation) takibi
* Ağ bağlantıları (Network Connections) izleme
* Dosya oluşturma (File Creation) takibi
* DLL yükleme izleme
* WMI etkinlikleri, Pipe kullanımı, Registry değişiklikleri vb.
* SHA256 hash üretimiyle dosya analizi
* Güvenlik olaylarının Windows Event Log’a kaydı (Event Viewer altında: **Applications and Services Logs → Microsoft → Windows → Sysmon → Operational**)

**🎯 Kullanım Alanları:**

* Zararlı yazılım tespiti (malware analysis)
* Olay müdahale (incident response)
* Tehdit istihbaratı toplama
* Adli bilişim analizleri (forensics)
* İç tehditlerin izlenmesi

**🧩 SysmonView Nedir?**

**SysmonView**, Sysmon’un loglarını görsel arayüzle analiz etmeye yardımcı olan bir GUI (grafiksel arayüz) uygulamasıdır.

**✅ Özellikleri:**

* Sysmon loglarını okunabilir ve filtrelenebilir biçimde sunar
* Belirli Event ID’lere göre filtreleme yapma
* İşlem ağacı gösterimi
* JSON ve XML logları kolayca yorumlama

Sysmon Kurulumu (Windows için geliştirilmiş bir araçtır)

**🔧 1. Sysmon'u İndir**

* Resmi Sysinternals linki:  
  🔗 https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon
* ZIP dosyasını indirip çıkarın (Sysmon64.exe veya Sysmon.exe içerir).

**🔧 2. SysmonView’i Çalıştır**

* SysmonView.exe dosyasını çift tıklayıp çalıştırın.
* İlk açılışta Sysmon loglarını otomatik olarak okuyacaktır.

**Kullanım Arayüzü:**

* Soldaki menüden Event ID filtreleri uygulanabilir
* Sağ kısımda olay detayları ve süreç ilişkileri gösterilir
* JSON görünümü, filtreleme ve zaman çizelgesi (timeline) sunar

**Örnek Çıktı:**

