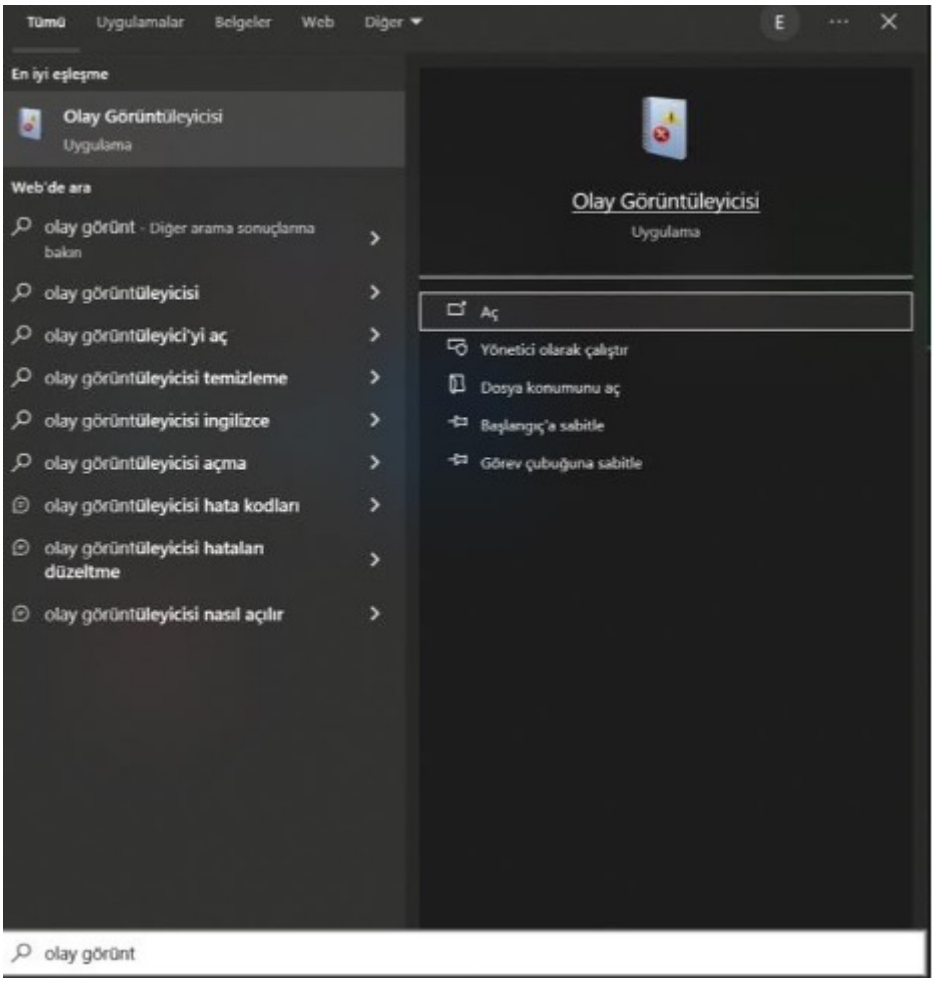
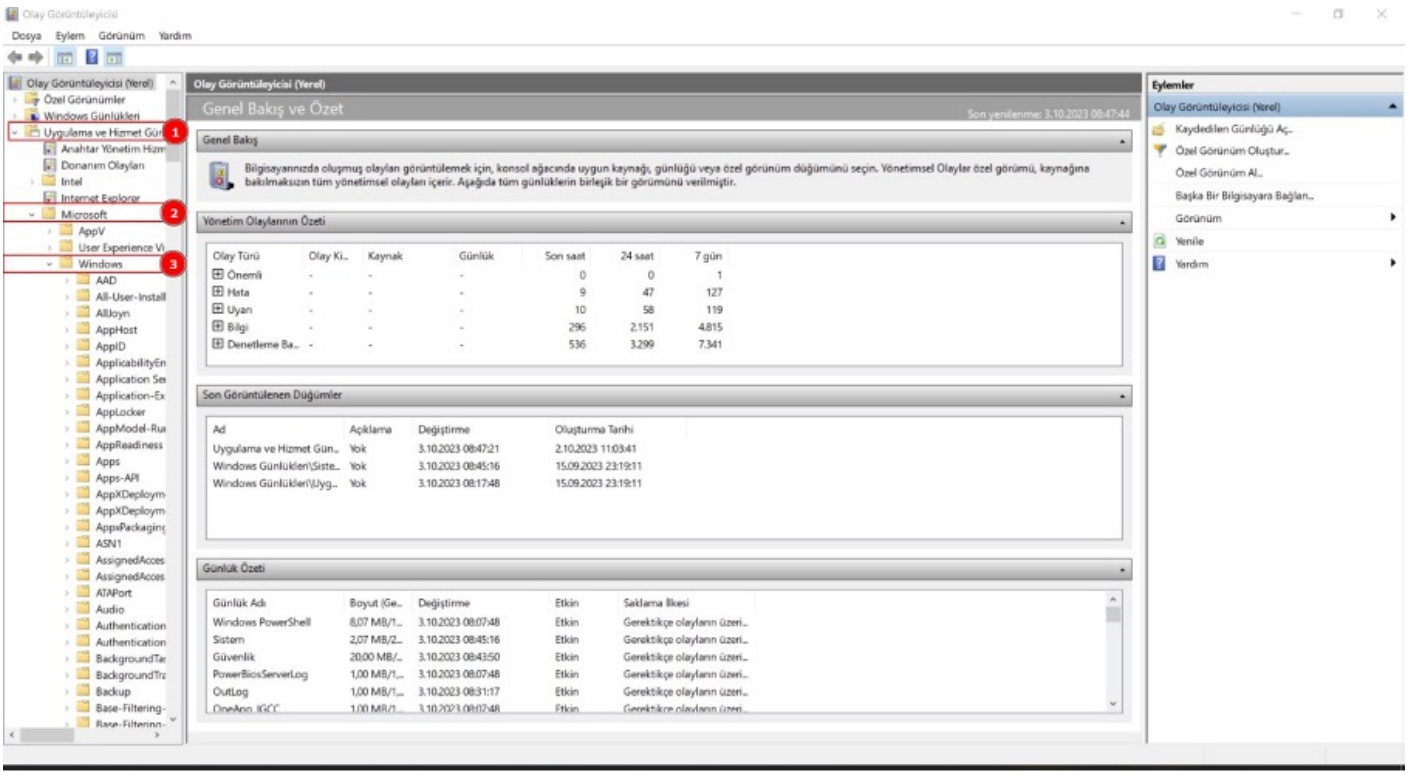
Kullanım

Kullanım

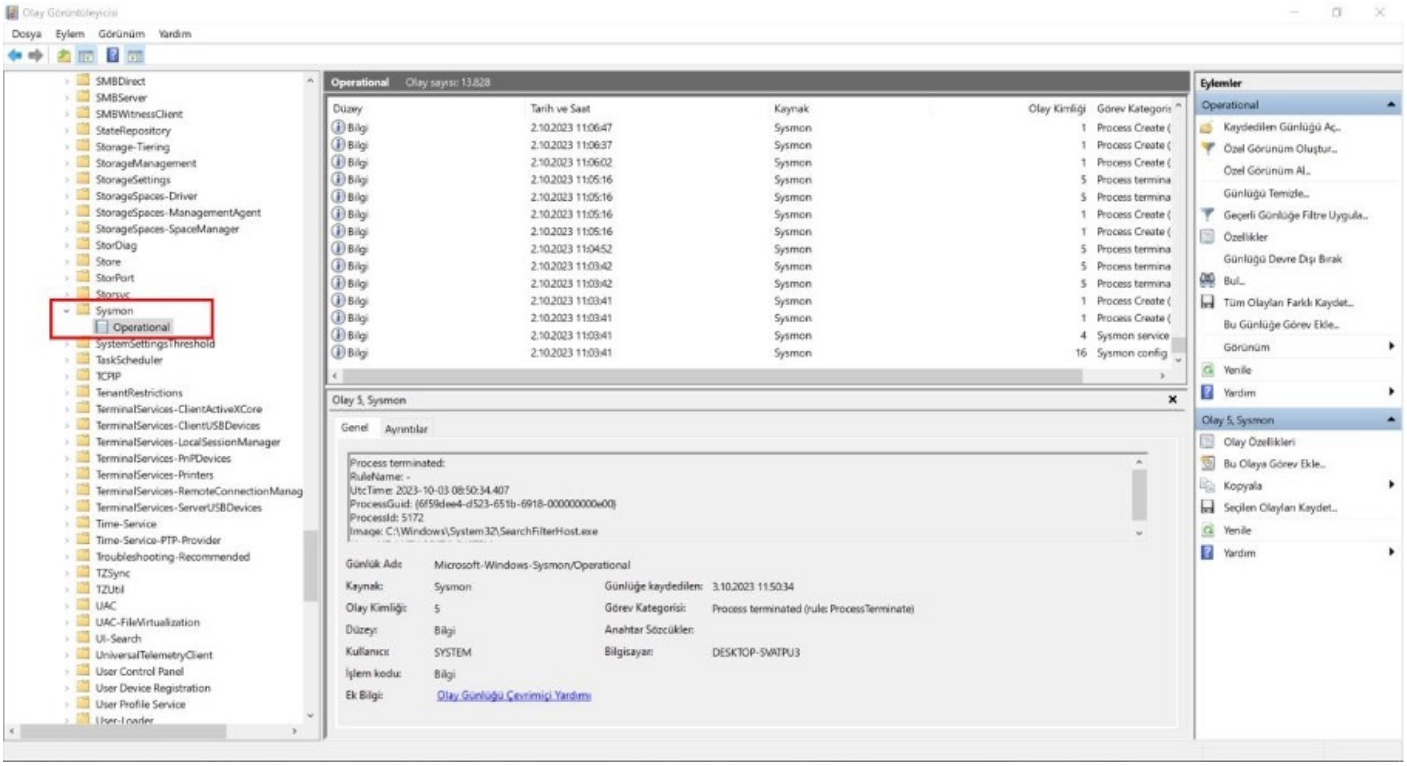
Başlat menüsünden olay görüntüleyicisi açılır.



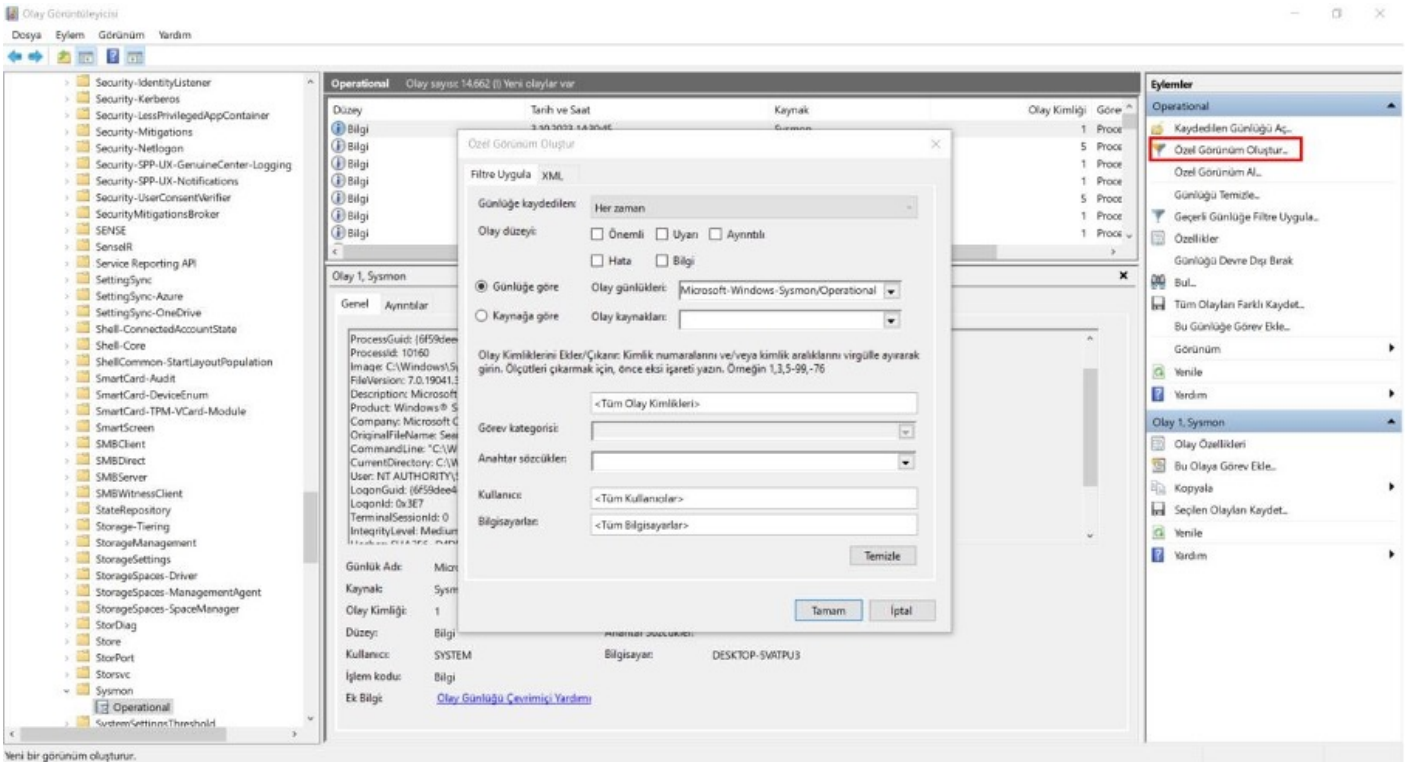
Uygulama ve hizmet günlükleri sekmesinden Microsoft alt sekmesi seçilir. Ardından windows alt sekmesi seçilir.



Windows alt sekmesinden sysmon alt sekmesi seçilir ve ardından operational seçeneği seçilir.



Oluşan log kayıtları burada görüntülenir. Sağ panelde özel görünüm oluştur butonuna tıklayınca log kayıtlarını filtrelemeye yarayan bir pencere açılmaktadır.



Bu pencere sayesinde sadece görmek istenilen loglar görüntülenebilir.

Event ID

Olay günlüğü üzerinde bulunan kayıt değerleri Event ID olarak tanımlanmaktadır. Windows sistemler üzerinde gerçekleşen işlemler sonucunda çok sayıda “Event ID” oluşmaktadır.

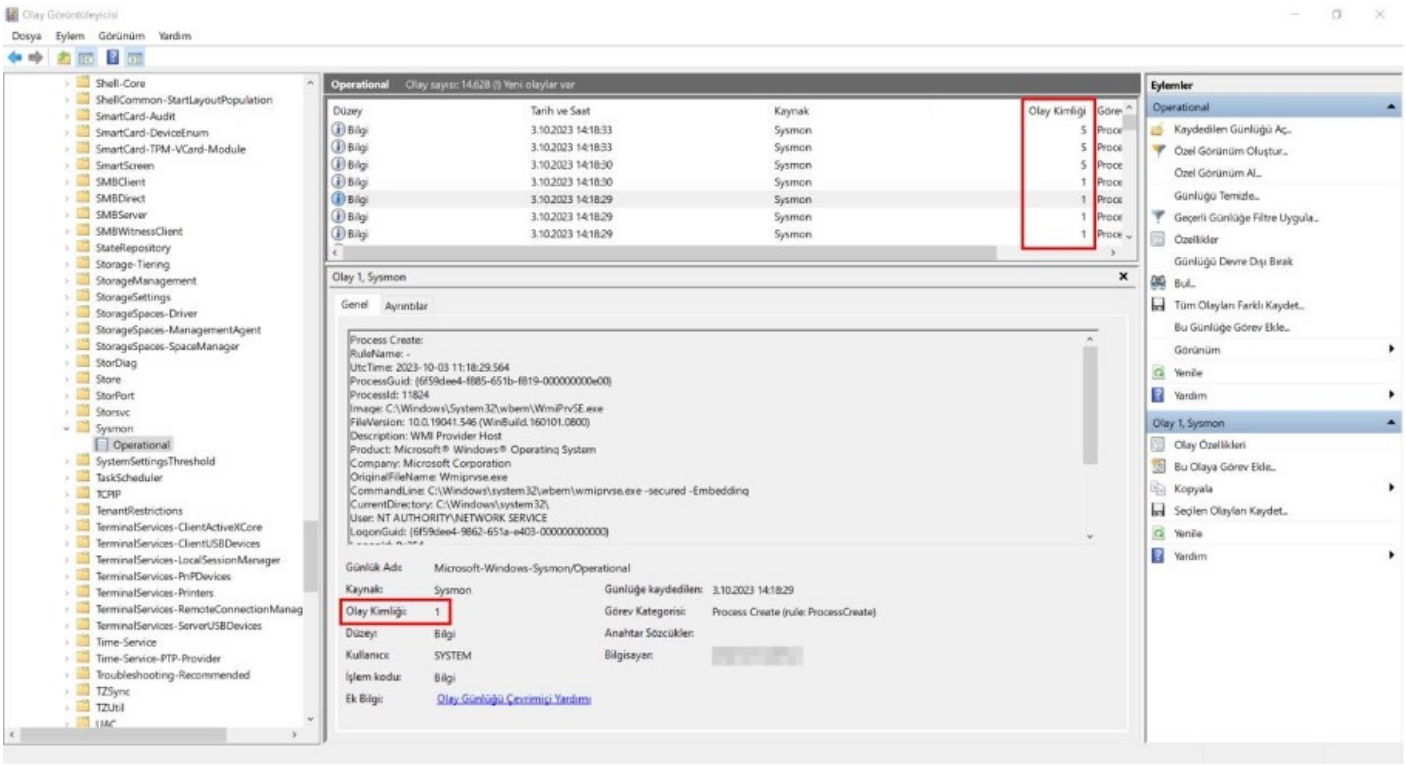
Oluşan bu Event ID’ler çok fazla ve farklı ID değerlerine sahip olduğu için olay incelemelerinde oldukça zor olmaktadır.

Windows Olay Kimlikleri (Event ID) çoğu olayın çözümlenmesinde bizlere yardımcı olmakla birlikte, diğer vakaların çözümlenmesinde de bizlere kolaylık sağlamaktadır.

Log kayıtlarının bulunduğu yerde olay kimliği kısmında Event ID'ler bulunmaktadır. Bu ID numaralarının her birinin farklı anlamı bulunmaktadır.

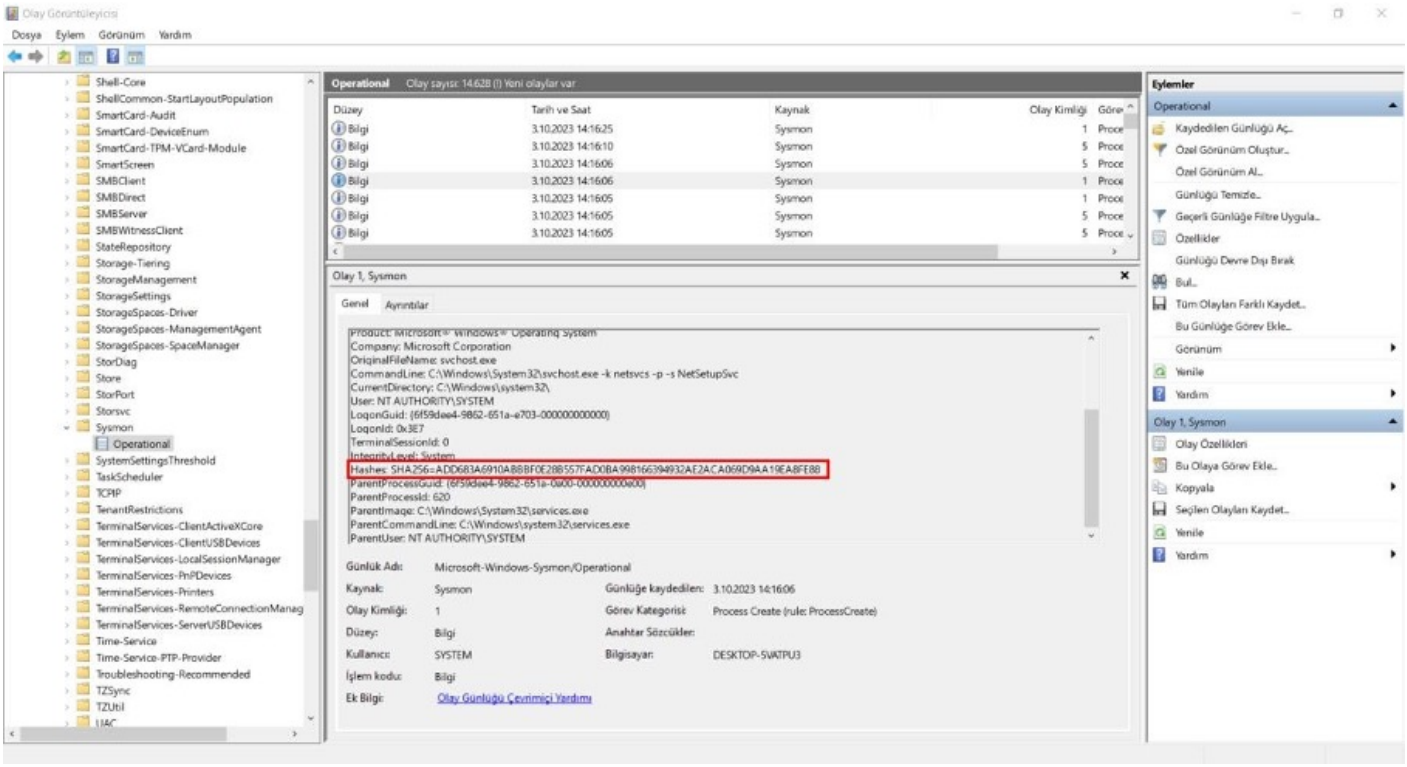
ID	Anlamı
1 ProccesCreate	İşlem başlatıldı
2 FileCreateTime	Dosya oluşturma süresi
3 NetworkConnect	Ağ bağlantısı algılandı
4 n/a	Sysmon hizmet durumu değişikliği(filtrelenemez)
5 Process Terminate	Süreç sonlandırıldı
6 DriverLoad	Sürücü Yüklendi
7 ImageLoad	Resim yüklendi
8 CreateRemoteThread	Uzak Konu Oluşturılması algılandı
9 RawAccessRead	Ham Erişim Okuması algılandı
10 ProcessAccess	İşlem erişildi
11 FileCreate	Dosya oluşturuldu
12 RegistryEvent	Kayıt defteri nesnesi eklendi veya silindi
13 RegistryEvent	Kayıt defteri değeri kümesi
14 RegistryEvent	Kayıt defteri nesnesi yeniden adlandırıldı
15 FileCreateStreamHash	Dosya akışı oluşturuldu
16 n/a	Sysmon yapılandırma değişikliği(filtrelenemez)
17 PipeEvent	Adlandırılmış kanal oluşturuldu
18 PipeEvent	Adlandırılmış boru bağlandı

Event ID bir üst panelde olay kısmında olay kimliği sütununda görünmektedir. Bir olay hakkında daha detaylı bilgialmak için olaya tıklanması yeterli olacaktır.



Sysmon’da Olayları HASH Değerlerine Göre İnceleme ve Yorumlama

Olay kayıtları alındığında bir çok işleme ait hash bilgiside alınır. Bir işlemin şüpheli olup olmadığı bu hashler yardımıyla anlaşılabilir. Herhangi bir olaya tıklandığında hash bilgisi virustotal tarzı hizmetler yardımıyla şüpheli olup olmadığı anlaşılabilir.



Virustotal ile incelenen bu olayın normal bir durum olduğu bu şekilde anlaşılabilir.