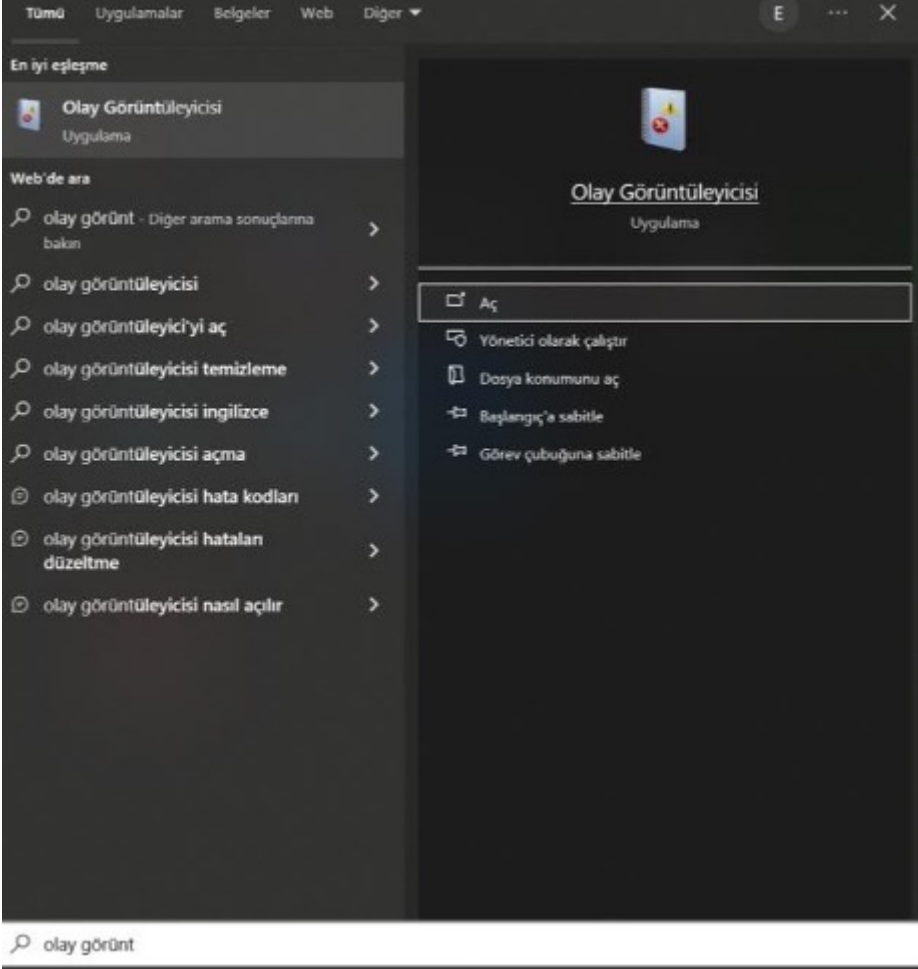


Kullanım

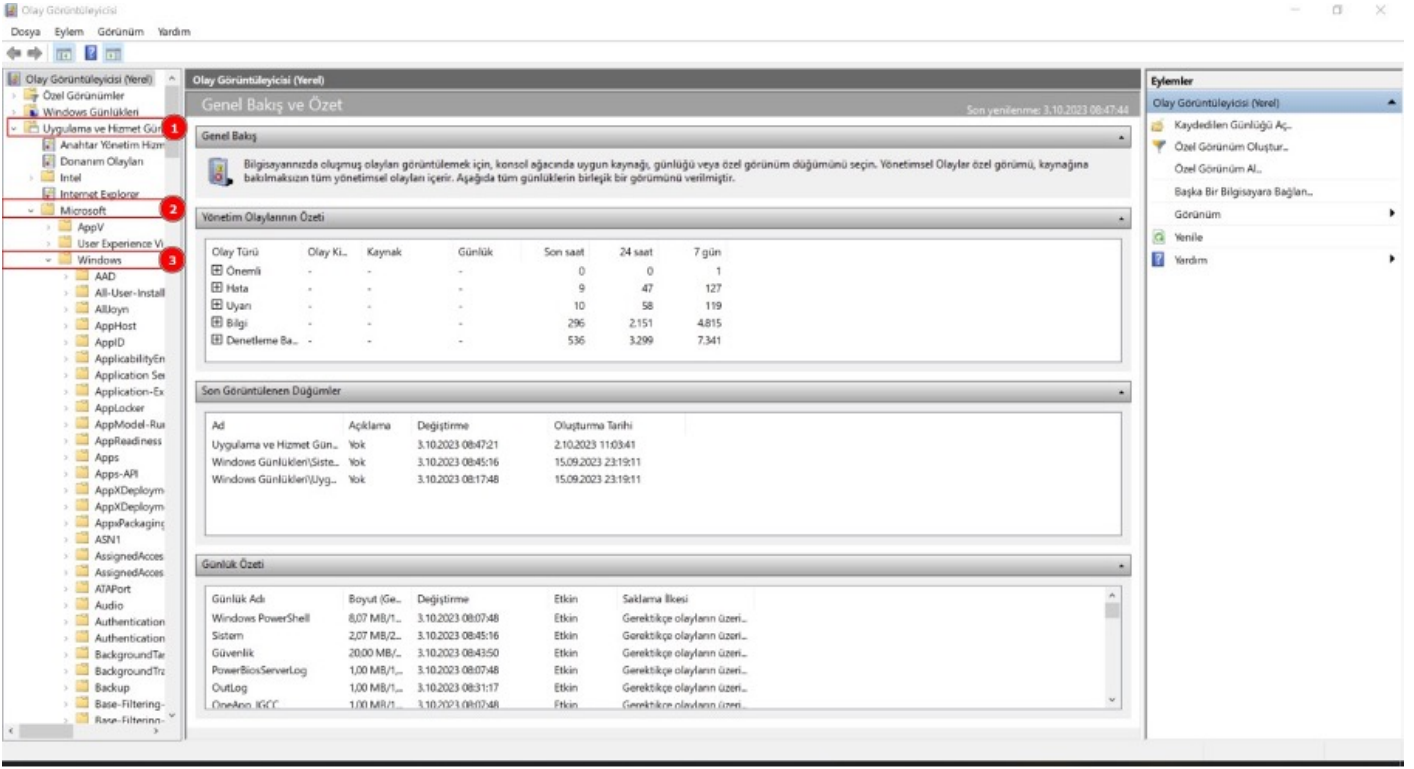
- [Kullanım](#)
- [Event ID](#)
- [Sysmon'da Olayları HASH Değerlerine Göre İnceleme ve Yorumlama](#)

Kullanım

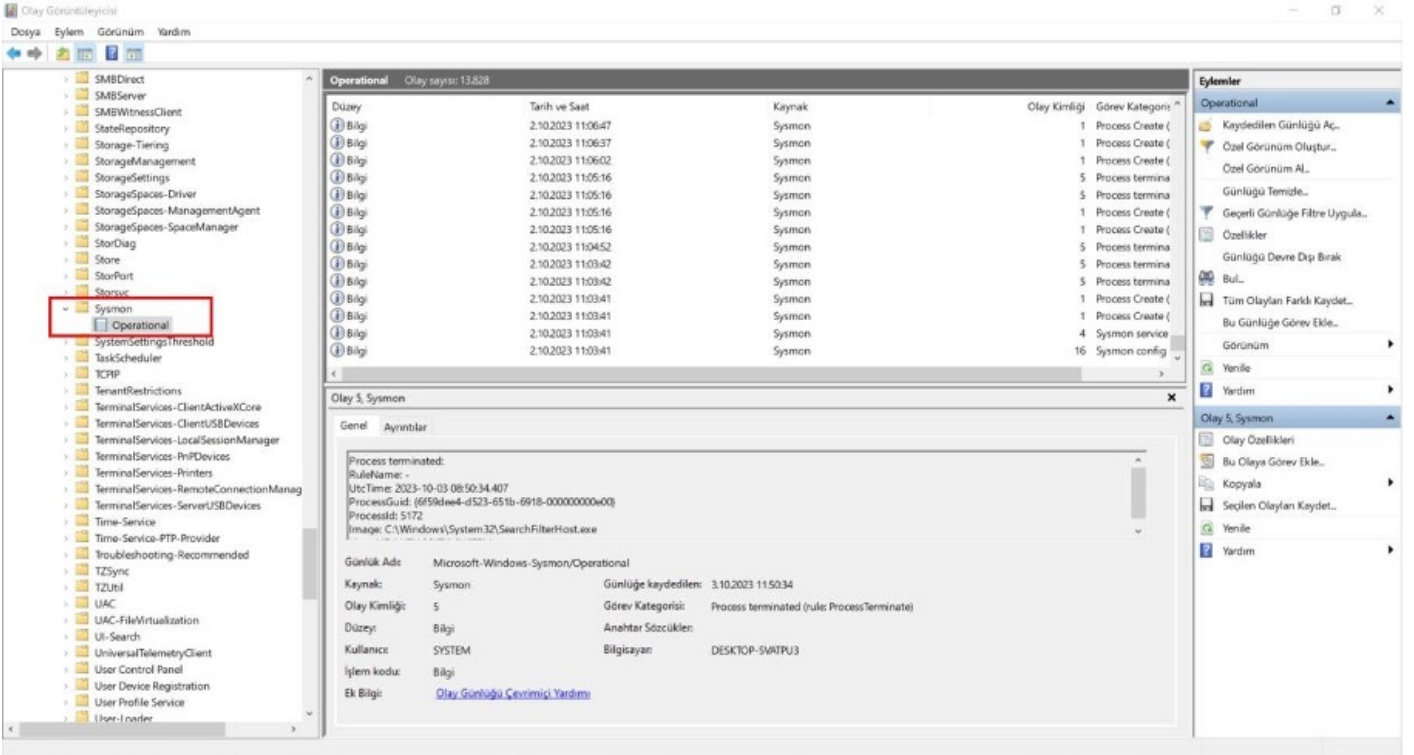
Başlat menüsünden olay görüntüleyicisi açılır.



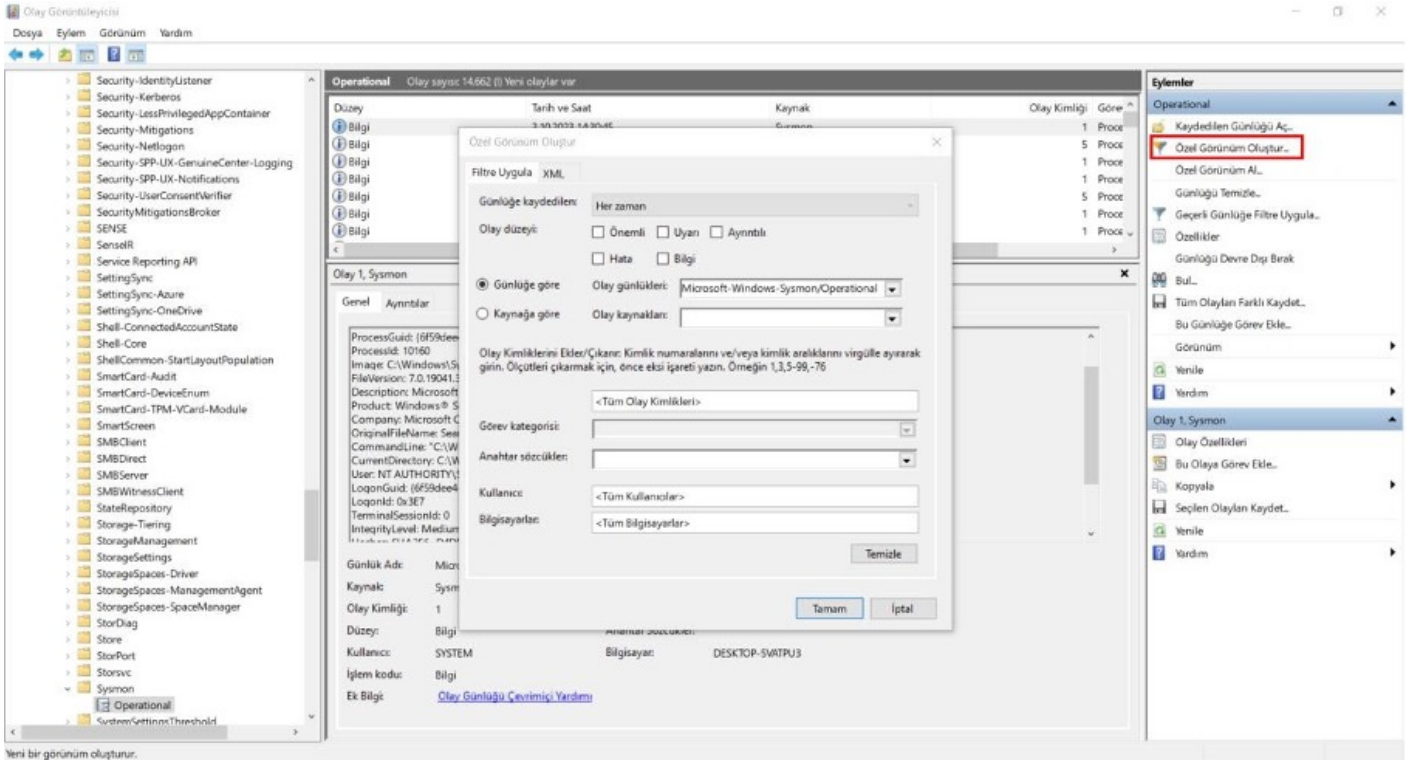
Uygulama ve hizmet günlükleri sekmesinden Microsoft alt sekmesi seçilir. Ardından windows alt sekmesi seçilir.



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 çözülmesinde bizlere yardımcı olmakla birlikte, diğer vakaların çözülmesinde 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 Oluşturulması 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.

The screenshot displays the Windows Event Viewer application. The left pane shows a tree view of event logs, with 'Operational' selected under the 'Sysmon' category. The main pane shows a list of events with columns: 'Düzye' (Level), 'Tarih ve Saat' (Date and Time), 'Kaynak' (Source), 'Olay Kimliği' (Event ID), and 'Görünüm' (View). The 'Olay Kimliği' column is highlighted with a red box. Below the list, the details of a selected event are shown in a tabbed interface. The 'Genel' (General) tab is active, displaying information about the event, including the process name, user, and command line. The 'Olay Kimliği' field is also highlighted with a red box. The right pane shows a list of event filters and actions, with 'Operational' selected.

| Düzye | Tarih ve Saat | Kaynak | Olay Kimliği | Görünüm |
|-------|--------------------|--------|--------------|---------|
| Bilgi | 3.10.2023 14:18:33 | Sysmon | 5 | Proce |
| Bilgi | 3.10.2023 14:18:33 | Sysmon | 5 | Proce |
| Bilgi | 3.10.2023 14:18:30 | Sysmon | 5 | Proce |
| Bilgi | 3.10.2023 14:18:30 | Sysmon | 1 | Proce |
| Bilgi | 3.10.2023 14:18:29 | Sysmon | 1 | Proce |
| Bilgi | 3.10.2023 14:18:29 | Sysmon | 1 | Proce |
| Bilgi | 3.10.2023 14:18:29 | Sysmon | 1 | Proce |

Olay 1, Sysmon

Genel | Ayrıntılar

Process Create:
RuleName: -
UtcTime: 2023-10-03 11:18:29.564
ProcessGuid: {6F59dee4-4885-651b-f819-000000000000}
ProcessId: 11824
Image: C:\Windows\System32\wbem\WmiPrvSE.exe
FileVersion: 10.0.19041.546 (WinBuild.160101.0800)
Description: WMI Provider Host
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: WmiPrvse.exe
CommandLine: C:\Windows\system32\wbem\wmiPrvse.exe -secured -Embedding
CurrentDirectory: C:\Windows\system32\wbem\WmiPrvse.exe -secured -Embedding
User: NT AUTHORITY\NETWORK SERVICE
LogonGuid: {6F59dee4-4885-651b-f819-000000000000}

Günlük Adı: Microsoft-Windows-Sysmon/Operational
Kaynak: Sysmon
Günlüğe kaydedildi: 3.10.2023 14:18:29
Olay Kimliği: 1
Görev Kategorisi: Process Create (rule: ProcessCreate)
Düzye: Bilgi
Anahtar Sözcükler:
Kullanıcı: SYSTEM
Bilgiyazı:
İşlem kodu: Bilgi
Ek Bilgi: [Olay Günlüğü Çözümleme Yardımı](#)

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.

The screenshot shows the Sysmon Event Viewer interface. On the left, a tree view lists various Sysmon categories. The main pane displays a list of events under the 'Operational' category. The selected event is 'Olay 1, Sysmon'. The detailed view of this event shows the following information:

- Product: windows® operating system
- Company: Microsoft Corporation
- OriginalFileName: svchost.exe
- CommandLine: C:\Windows\System32\svchost.exe -k netsvcs -p -s NetSetupSvc
- CurrentDirectory: C:\Windows\system32\
- User: NT AUTHORITY\SYSTEM
- LogonGuid: {6f59d4e4-9862-651a-e703-000000000000}
- LogonId: 0x3e7
- TerminalSessionId: 0
- IntegrityLevel: System
- Hashes: SHA256:ADD683A6910A88BF0E28B557FAD0BA998166394932ae2aca069d9aa19ea8fe88
- ParentProcessGuid: {6f59d4e4-9862-651a-e703-000000000000}
- ParentProcessId: 620
- ParentImage: C:\Windows\System32\services.exe
- ParentCommandLine: C:\Windows\system32\services.exe
- ParentUser: NT AUTHORITY\SYSTEM

Below the detailed view, additional information is provided:

- Event Name: Microsoft-Windows-Sysmon/Operational
- Source: Sysmon
- Event Category: Process Create (rule: ProcessCreate)
- Level: 1
- Category: Bilgi
- User: SYSTEM
- Operation: Bilgi
- Process Name: svchost.exe
- Process ID: 620
- Process Image: C:\Windows\System32\services.exe
- Process Command Line: C:\Windows\system32\services.exe
- Process User: NT AUTHORITY\SYSTEM

The screenshot shows the VirusTotal analysis results for the file 'svchost.exe'. The file is identified as 'File distributed by Microsoft'. The analysis shows a score of 0/72, indicating it is a known good file. The file is 54.02 KB in size and was last analyzed 16 minutes ago. The analysis was performed by the 'Community Score' engine. The file is marked as 'peace', 'assembly', 'overlay', 'signed', 'detect-debug-environment', 'idle', '64bits', and 'known-distributor'.

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