

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 interface. The left pane shows the 'Operational' log selected. The main pane shows a list of events with columns for 'Düzye' (Level), 'Tarih ve Saat' (Date and Time), 'Kaynak' (Source), and 'Olay Kimliği' (Event ID). The 'Olay Kimliği' column is highlighted with a red box. The 'Olay 1, Sysmon' event is selected, and its details are shown in the 'Ayrıntılar' (Details) pane. The details pane shows the 'Olay Kimliği' (Event ID) as 1, which is also highlighted with a red box. The 'Görünüm' (View) pane on the right shows the 'Operational' log 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\

User: NT AUTHORITY\NETWORK SERVICE

LogonGuid: {6F59dee4-9862-651a-e403-000000000000}

Günlük Adı: Microsoft-Windows-Sysmon/Operational

Kaynak: Sysmon

Günlüğe kaydedilem: 3.10.2023 14:18:29

Olay Kimliği: 1

Görev Kategorisi: Process Create (rule: ProcessCreate)

Düzye: Bilgi

Anahtar Sözcükler:

Kullanıcı: SYSTEM

Bilgiyay:

İşlem kodu: Bilgi

Ek Bilgi: [Olay Günlüğü Çözümleme Yardımı](#)

Revision #1

Created 27 January 2024 16:03:03 by Ertan Sözer

Updated 27 January 2024 16:04:09 by Ertan Sözer