

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, there is a tree view of event 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: Microsoft® Windows® Operating System
- Company: Microsoft Corporation
- OriginalFileName: svchost.exe
- CommandLine: C:\Windows\System32\svchost.exe -k netsvc -p -s NetSetupSvc
- CurrentDirectory: C:\Windows\system32\
- User: NT AUTHORITY\SYSTEM
- LogonId: {6f59d4e4-9862-651a-e703-000000000000}
- LogonId: 0x3e7
- TerminalSessionId: 0
- IntegrityLevel: System
- Hashes: SHA256: A0D683A6910A8B8F0E28B557FAD00BA98166794932AF2ACA069D9AA19EABFE88
- ParentProcessId: {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 event details, there is a summary section:

- Günlük Adı: Microsoft-Windows-Sysmon/Operational
- Kaynak: Sysmon
- Günlüğe kaydedilen: 3.10.2023 14:16:06
- Olay Kimliği: 1
- Görev Kategorisi: Process Create (rule: ProcessCreate)
- Düzye: Bilgi
- Anahtar Sözcükler:
- Kullanıcı: SYSTEM
- Bilgisayar: DESKTOP-SVAKPLU3
- İşlem kodu: Bilgi
- Ek Bilgi: [Olay Günlüğü Çevrimiçi Yardımı](#)

The screenshot shows the VirusTotal analysis results for the file 'svchost.exe'. The file is identified as 'File distributed by Microsoft'. The analysis shows that the file is not detected by any of the 47 engines. The file size is 54.02 KB and the last analysis date is 16 minutes ago. The file is marked as 'peexe', 'assembly', 'overlay', 'signed', 'detect-debug-environment', 'idle', '64bits', and 'known-distributor'. The Community Score is 0/172.

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

Revision #2

Created 27 January 2024 16:04:19 by Ertan Sözer

Updated 27 January 2024 16:05:17 by Ertan Sözer