CrownJewel-1,MFT、evtx(MFTECmd、Timeline Explorer、gigasheet),VSS、NTDS

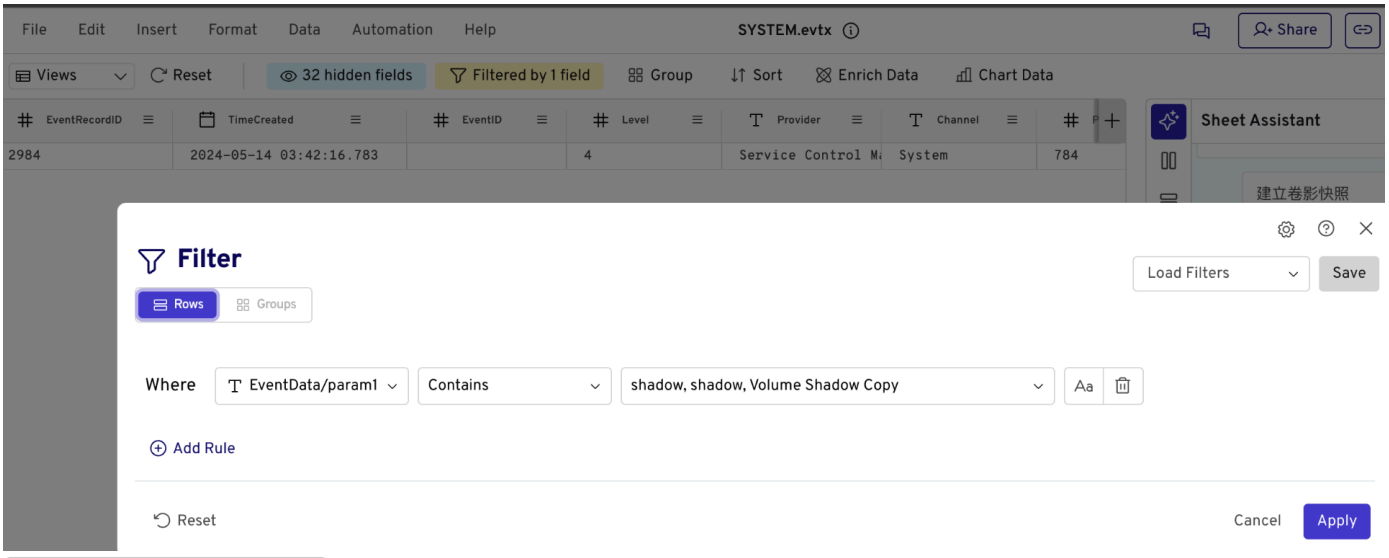
```
Sherlock Scenario
Our SIEM alerted us to a suspicious logon event which needs to be looked at immediately . The alert details were that the IP Address and the Source Workstation name were a mismatch .You are provided a network capture and event logs from the surrounding time around the incident timeframe. Corelate the given evidence and report back to your SOC Manager.
* * *
About CrownJewel-1
In this very easy sherlock, you will learn how to detect NTDS.dit dumping which is one of the most critical Active directory attacks. You will get your hands on event logs and MFT to respond to an attack where the attacker utilized vssadmin utility to dump the NTDS.dit database.
```

文件：SYSTEM.evtx、SECURITY.evtx、Microsoft-Windows-NTFS.evtx、$MFT
使用工具：https://app.gigasheet.com/、MFTECmd

```
指令：
MFTECmd.exe -f "C:\Users\TSO\Downloads\$MFT" --csv "C:\Users\TSO\Downloads\LOG"
```

Task 1

Attackers can abuse the vssadmin utility to create volume shadow snapshots and then extract sensitive files like NTDS.dit to bypass security mechanisms. Identify the time when the Volume Shadow Copy service entered a running state.

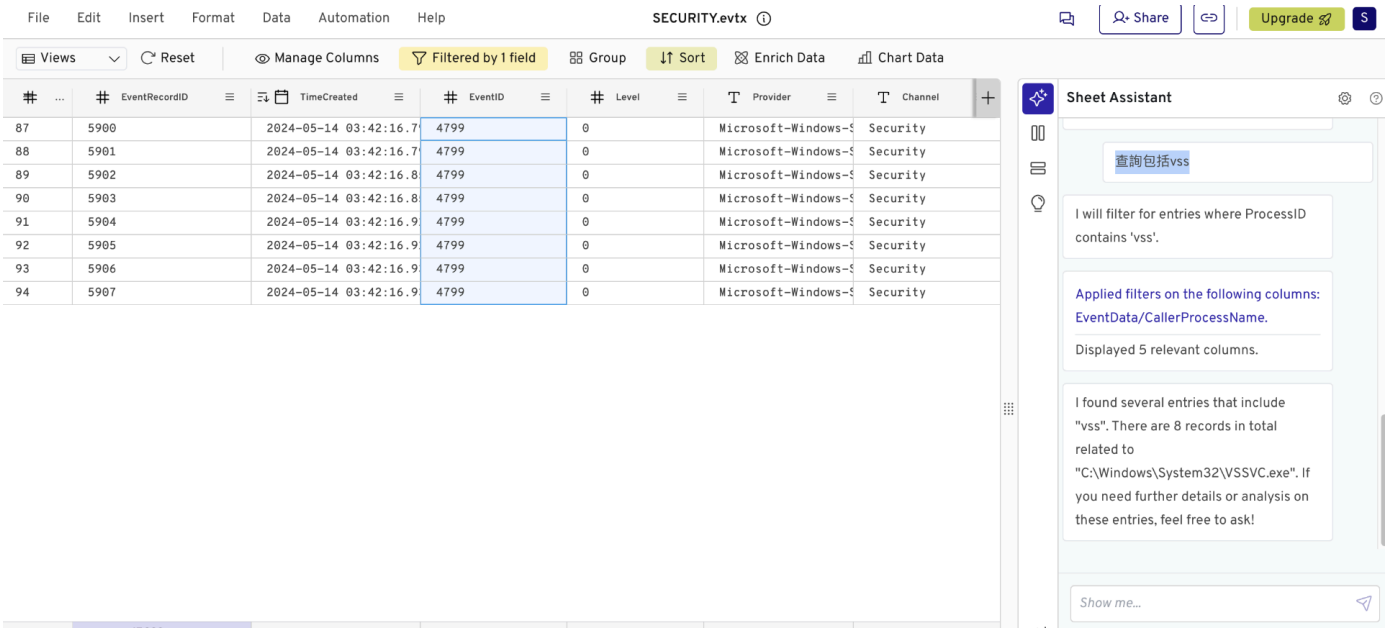


`2024-05-14 03:42:16`

Task 2

When a volume shadow snapshot is created, the Volume shadow copy service validates the privileges using the Machine account and enumerates User groups. Find the two user groups the volume shadow copy process queries and the machine account that did it.

條件：`查詢包括vss`



顯示event id ：4799

Administrators, Backup Operators, DC01$

Task 3

Identify the Process ID (in Decimal) of the volume shadow copy service process.

原先Process ID

EventData/CallerProcessId	EventData/CallerProcessName
0x1190	C:\Windows\System32\VSSVC.exe
0x1190	C:\Windows\System32\VSSVC.exe
0x1190	C:\Windows\System32\VSSVC.exe
0x1190	C:\Windows\System32\VSSVC.exe
0x1190	C:\Windows\System32\VSSVC.exe
0x1190	C:\Windows\System32\VSSVC.exe
0x1190	C:\Windows\System32\VSSVC.exe
0x1190	C:\Windows\System32\VSSVC.exe

轉換後

即時進制轉換器

寫作業需要的時候很好用，讓你在不同進位快速轉換，考試老師不會查你就用就這個

十進位 十六進位 八進位 二進位 ⇄ 十進位 十六進位 八進位 二進位

1190

4496

`4496`

Task 4

Find the assigned Volume ID/GUID value to the Shadow copy snapshot when it was mounted.

在`Microsoft-Windows-NTFS.evtx`查詢差不多時間點`2024-05-14 03:42:16`以後的時間

File Edit Insert Format Data Automation Help Microsoft-Windows-NTFS.evtx

Views Reset Manage Columns Filter Group Sort Enrich Data Chart D

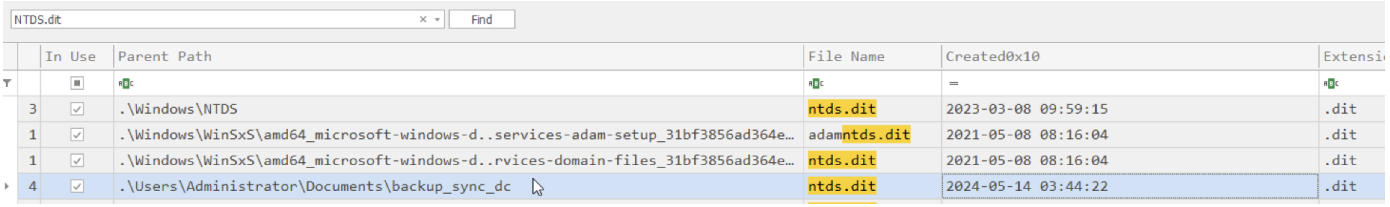
EventRecordID	TimeCreated	EventData/VolumeCorrelationId	EventID	
09	2023-03-27 14:02:42.675	C526EE1B-BA64-405C-A85B-A486EDDD36CB	10	4
10	2023-03-27 14:02:42.675	C526EE1B-BA64-405C-A85B-A486EDDD36CB	4	4
11	2023-03-27 14:02:45.714		142	4
12	2023-03-27 14:02:45.714		142	4
13	2024-05-14 03:36:52.675	17A28535-1E81-4F9F-8B4A-85BB7474B0C9	158	4
14	2024-05-14 03:36:52.676		142	4
15	2024-05-14 03:36:53.012	C526EE1B-BA64-405C-A85B-A486EDDD36CB	158	4
16	2024-05-14 03:41:38.573	17A28535-1E81-4F9F-8B4A-85BB7474B0C9	9	4
17	2024-05-14 03:41:38.573	17A28535-1E81-4F9F-8B4A-85BB7474B0C9	10	4
18	2024-05-14 03:41:38.573	17A28535-1E81-4F9F-8B4A-85BB7474B0C9	4	4
19	2024-05-14 03:41:41.605	C526EE1B-BA64-405C-A85B-A486EDDD36CB	4	4
20	2024-05-14 03:41:41.605	C526EE1B-BA64-405C-A85B-A486EDDD36CB	9	4
21	2024-05-14 03:41:41.605	C526EE1B-BA64-405C-A85B-A486EDDD36CB	10	4
22	2024-05-14 03:41:44.308		142	4
23	2024-05-14 03:41:44.353		142	4
24	2024-05-14 03:44:22.812	06C4A997-CCA8-11ED-A90F-000C295644F9	4	4
25	2024-05-14 03:44:22.813	06C4A997-CCA8-11ED-A90F-000C295644F9	9	4
26	2024-05-14 03:44:22.813	06C4A997-CCA8-11ED-A90F-000C295644F9	10	4

`{06c4a997-cca8-11ed-a90f-000c295644f9}`

Task 5

Identify the full path of the dumped NTDS database on disk.

在google找，是dit格式



`C:\Users\Administrator\Documents\backup_sync_Dc\Ntds.dit`

Task 6

When was newly dumped ntds.dit created on disk?

同上

`2024-05-14 03:44:22`

Task 7

A registry hive was also dumped alongside the NTDS database. Which registry hive was dumped and what is its file size in bytes?

`SYSTEM, 17563648`