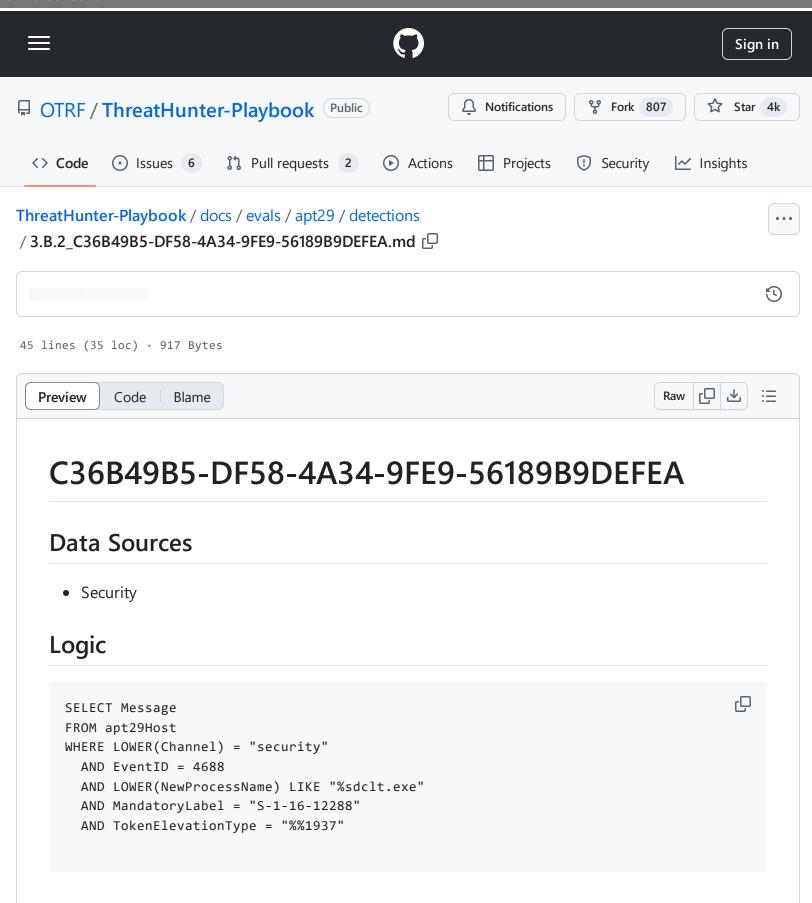
ThreatHunter-Playbook/docs/evals/apt29/detections/3.B.2_C36B49B5-DF58-4A34-9FE9-56189B9DEFEA.md at 2d4257f630f4c9770f78d0c1df059f891ffc3fec · OTRF/ThreatHunter-Playbook · GitHub - 31/10/2024 19:16 https://github.com/OTRF/ThreatHunter-

Playbook/blob/2d4257f630f4c9770f78d0c1df059f891ffc3fec/docs/evals/apt29/detections/3.B.2_C36B49B5-DF58-4A34-9FE9-56189B9DEFEA.md



ThreatHunter-Playbook/docs/evals/apt29/detections/3.B.2_C36B49B5-DF58-4A34-9FE9-56189B9DEFEA.md at 2d4257f630f4c9770f78d0c1df059f891ffc3fec · OTRF/ThreatHunter-Playbook · GitHub - 31/10/2024 19:16 https://github.com/OTRF/ThreatHunter-

Playbook/blob/2d4257f630f4c9770f78d0c1df059f891ffc3fec/docs/evals/apt29/detections/3.B.2_C36B49B5-DF58-4A34-9FE9-56189B9DEFEA.md

Output

A new process has been created.

Q

Creator Subject:

Security ID: S-1-5-18
Account Name: SCRANTON\$

Account Domain: DMEVALS

Logon ID: 0x3E7

Target Subject:

Security ID: S-1-5-21-1830255721-3727074217-2423397540-1107

Account Name: pbeesly

Account Domain: DMEVALS

Logon ID: 0x372E81

Process Information:

New Process ID: 0x195c

New Process Name: C:\Windows\System32\sdclt.exe

Token Elevation Type: %%1937

Mandatory Label: S-1-16-12288

Creator Process ID: 0xd98

Creator Process Name: C:\Windows\System32\cmd.exe
Process Command Line: "C:\windows\system32\sdclt.exe"