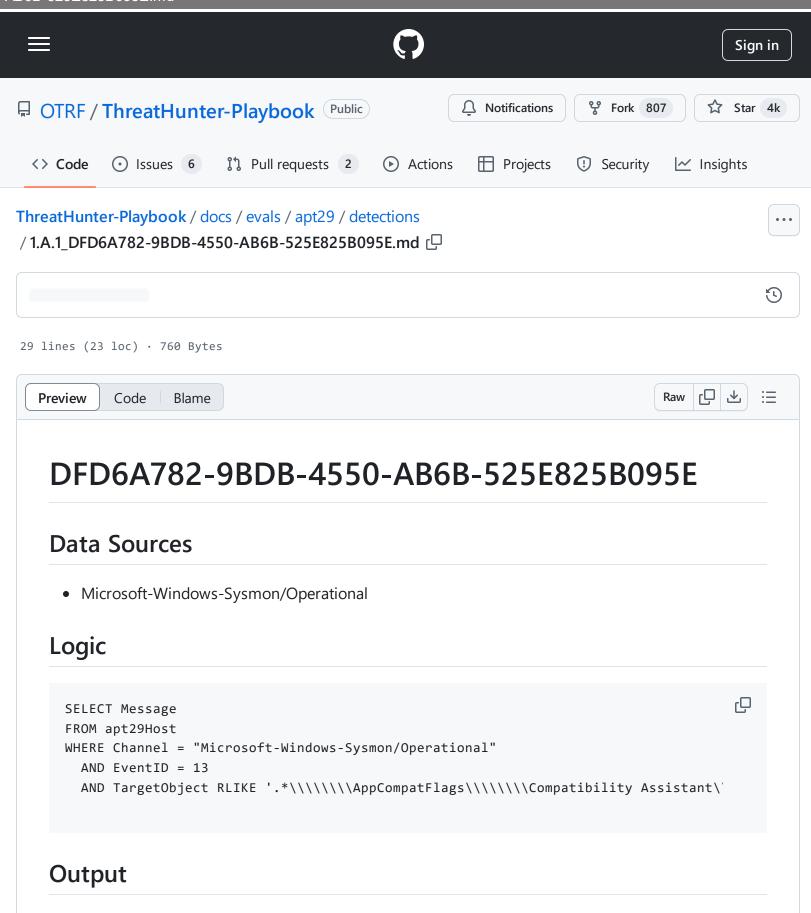
ThreatHunter-Playbook/docs/evals/apt29/detections/1.A1_DFD6A782-9BDB-4550-AB6B-525E825B095E.md at 2d4257f630f4c9770f78d0c1df059f891ffc3fec · OTRF/ThreatHunter-Playbook · GitHub - 31/10/2024 20:09 https://github.com/OTRF/ThreatHunter-

Playbook/blob/2d4257f630f4c9770f78d0c1df059f891ffc3fec/docs/evals/apt29/detections/1.A.1_DFD6A782-9BDB-4550-AB6B-525E825B095E.md



ThreatHunter-Playbook/docs/evals/apt29/detections/1.A1_DFD6A782-9BDB-4550-AB6B-525E825B095E.md at 2d4257f630f4c9770f78d0c1df059f891ffc3fec · OTRF/ThreatHunter-Playbook · GitHub - 31/10/2024 20:09

https://github.com/OTRF/ThreatHunter-

Playbook/blob/2d4257f630f4c9770f78d0c1df059f891ffc3fec/docs/evals/apt29/detections/1.A.1_DFD6A782-9BDB-4550-AB6B-525E825B095E.md

Q

Registry value set:

RuleName: -

EventType: SetValue

UtcTime: 2020-05-02 03:01:29.278

ProcessGuid: {47ab858c-cc06-5eac-9402-000000000400}

ProcessId: 1144

Image: C:\windows\system32\svchost.exe

TargetObject: HKU\S-1-5-21-1830255721-3727074217-2423397540-1107\Software\Microsof

Details: Binary Data