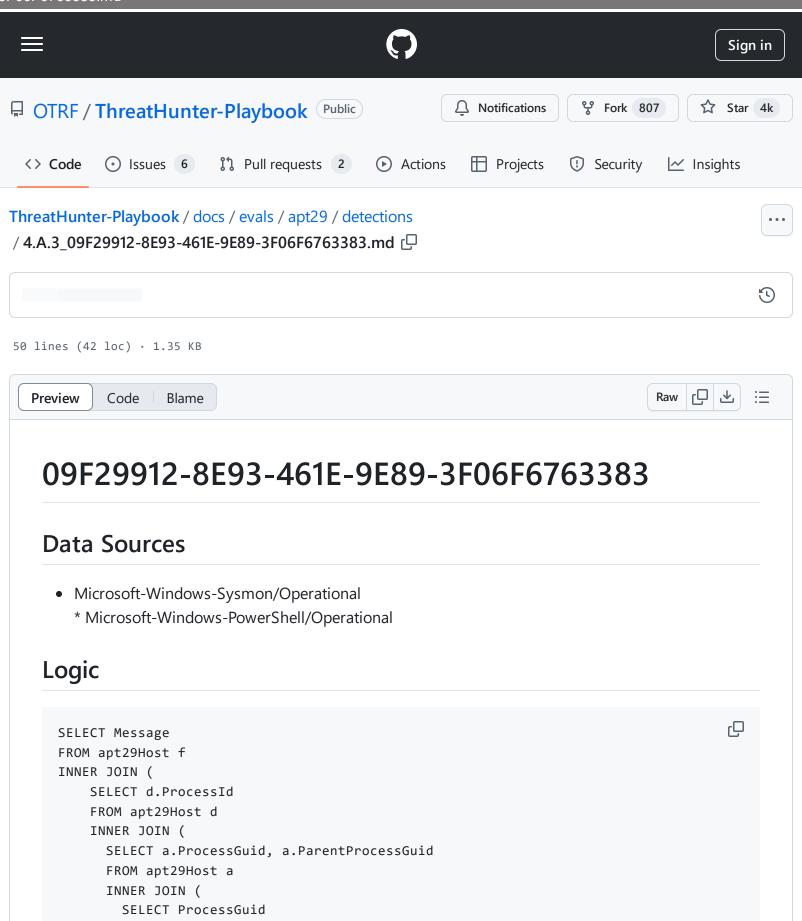
ThreatHunter-Playbook/docs/evals/apt29/detections/4.A3_09F29912-8E93-461E-9E89-3F06F6763383.md at 2d4257f630f4c9770f78d0c1df059f891ffc3fec · OTRF/ThreatHunter-Playbook · GitHub - 31/10/2024 17:00

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

Playbook/blob/2d4257f630f4c9770f78d0c1df059f891ffc3fec/docs/evals/apt29/detections/4.A.3_09F29912-8E93-461E-9E89-3F06F6763383.md



ThreatHunter-Playbook/docs/evals/apt29/detections/4.A3_09F29912-8E93-461E-9E89-3F06F6763383.md at 2d4257f630f4c9770f78d0c1df059f891ffc3fec · OTRF/ThreatHunter-Playbook · GitHub - 31/10/2024 17:00

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

Playbook/blob/2d4257f630f4c9770f78d0c1df059f891ffc3fec/docs/evals/apt29/detections/4.A.3_09F29912-8E93-461E-9E89-3F06F6763383.md_

```
FROM apt29Host
        WHERE Channel = "Microsoft-Windows-Sysmon/Operational"
            AND EventID = 1
            AND LOWER(Image) LIKE "%control.exe"
            AND LOWER(ParentImage) LIKE "%sdclt.exe"
      ) b
     ON a.ParentProcessGuid = b.ProcessGuid
     WHERE a.Channel = "Microsoft-Windows-Sysmon/Operational"
        AND a.EventID = 1
        AND a.IntegrityLevel = "High"
    ) c
   ON d.ParentProcessGuid= c.ProcessGuid
    WHERE d.Channel = "Microsoft-Windows-Sysmon/Operational"
     AND d.EventID = 1
     AND d.Image LIKE '%powershell.exe'
) e
ON f.ExecutionProcessID = e.ProcessId
WHERE f.Channel = "Microsoft-Windows-PowerShell/Operational"
    AND f.EventID = 4104
   AND LOWER(f.ScriptBlockText) LIKE "%expand-archive%"
```

Output

```
Creating Scriptblock text (1 of 1):

Expand-Archive -LiteralPath "$env:USERPROFILE\Downloads\SysinternalsSuite.zip" -De:

ScriptBlock ID: 63fc6cf4-cd9f-4134-9231-51ccb5c7d247
```