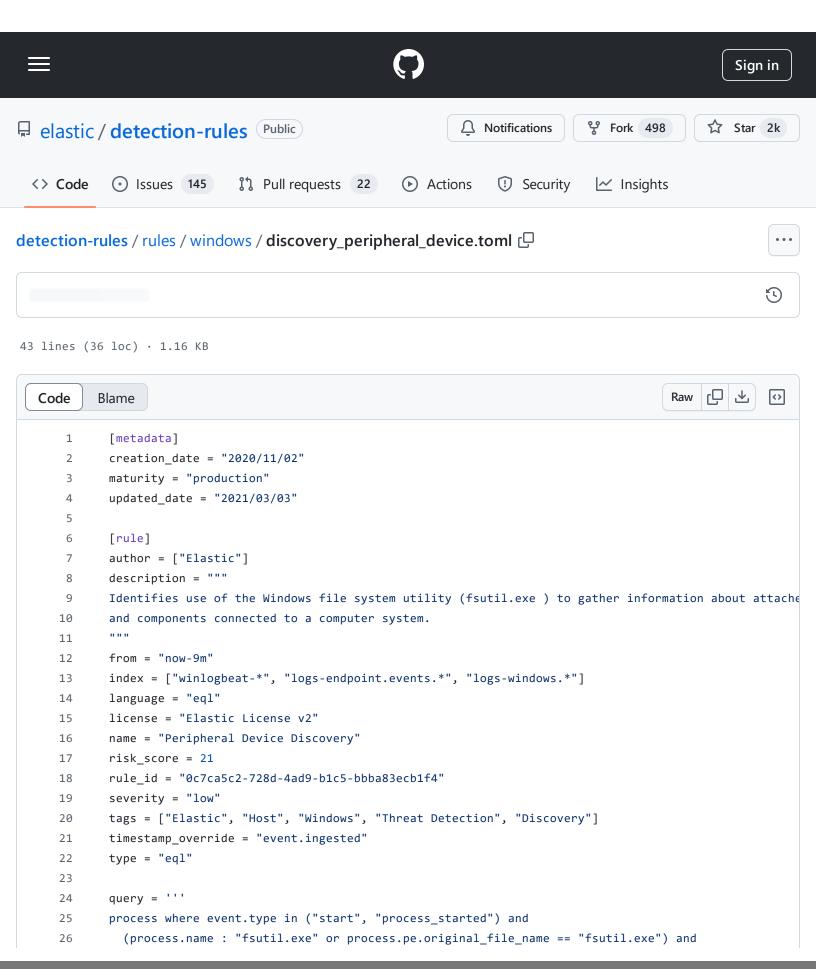
detection-rules/rules/windows/discovery_peripheral_device.toml at 414d32027632a49fb239abb8fbbb55d3fa8dd861 • elastic/detection-rules • GitHub - 31/10/2024 18:01 https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/discovery peripheral device.toml



detection-rules/rules/windows/discovery_peripheral_device.toml at 414d32027632a49fb239abb8fbbb55d3fa8dd861 · elastic/detection-rules · GitHub - 31/10/2024 18:01 https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/discovery_peripheral_device.toml

```
27
         process.args : "fsinfo" and process.args : "drives"
28
29
30
31
       [[rule.threat]]
       framework = "MITRE ATT&CK"
32
       [[rule.threat.technique]]
33
34
       id = "T1120"
35
       name = "Peripheral Device Discovery"
       reference = "https://attack.mitre.org/techniques/T1120/"
36
37
38
39
       [rule.threat.tactic]
       id = "TA0007"
40
       name = "Discovery"
41
42
       reference = "https://attack.mitre.org/tactics/TA0007/"
```